



# Décision n° 2021-924 QPC

## La Quadrature du Net

**Article L. 863-2 du code de la sécurité intérieure**  
*Communication d'informations entre services de  
renseignement et à destination de ces services*

## Dossier documentaire

*Source : services du Conseil constitutionnel - 2021*

### Sommaire

|            |   |           |
|------------|---|-----------|
| <b>I.</b>  | <b>Contexte de la disposition contestée .....</b>           | <b>5</b>  |
| <b>II.</b> | <b>Constitutionnalité de la disposition contestée .....</b> | <b>26</b> |

# Table des matières

|   |           |
|---|-----------|
| <b>I. Contexte de la disposition contestée .....</b>  | <b>5</b>  |
| <b>A. Dispositions contestées .....</b>   | <b>5</b>  |
| <b>Code de la sécurité intérieure .....</b>   | <b>5</b>  |
| - Article L. 863-2.....   | 5         |
| <b>B. Évolution des dispositions contestées .....</b>   | <b>5</b>  |
| <b>1. Loi n° 2015-912 du 24 juillet 2015 relative au renseignement .....</b>  | <b>5</b>  |
| - Article 8 .....   | 5         |
| <b>2. Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste .....</b> | <b>7</b>  |
| - Article 17 .....  | 7         |
| <b>C. Autres dispositions .....</b>   | <b>7</b>  |
| <b>1. Code de la sécurité intérieure.....</b>   | <b>7</b>  |
| - Article L. 801-1.....   | 7         |
| - Article L. 811-1.....   | 8         |
| - Article L. 811-2.....   | 8         |
| - Article L. 811-3.....   | 8         |
| - Article L. 811-4.....   | 8         |
| - Article L. 821-1.....   | 9         |
| - Article L. 821-4.....   | 9         |
| - Article L. 822-2.....   | 9         |
| - Article L. 822-3.....   | 10        |
| - Article L. 833-2.....   | 10        |
| - Article L. 851-1.....   | 10        |
| - Article L. 851-2.....   | 11        |
| - Article L. 851-3.....   | 11        |
| - Article L. 851-4.....   | 12        |
| - Article L. 851-5.....   | 12        |
| - Article L. 851-6.....   | 12        |
| - Article L. 851-7.....   | 13        |
| - Article L. 852-1.....   | 13        |
| - Article L. 852-2.....   | 13        |
| - Article L. 853-1.....   | 14        |
| - Article L. 853-2.....   | 14        |
| - Article L. 853-3.....   | 15        |
| - Article L. 854-1.....   | 15        |
| - Article L. 854-2.....   | 16        |
| - Article L. 854-3.....   | 17        |
| - Article L. 854-4.....   | 17        |
| - Article L. 854-5.....   | 17        |
| - Article L. 854-6.....   | 17        |
| - Article L. 854-7.....   | 18        |
| - Article L. 854-8.....   | 18        |
| - Article L. 854-9.....   | 18        |
| - Article L. 855-1 A.....   | 19        |
| - Article L. 855-1 B.....   | 19        |
| - Article L. 855-1 C.....   | 19        |
| <b>2. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés</b>  | <b>20</b> |
| - Article 2 .....   | 20        |
| - Article 4 .....   | 20        |

|   |           |
|---|-----------|
| - Article 6 .....   | 21        |
| - Article 19 .....  | 21        |
| - Article 31 .....  | 22        |
| - Article 33 .....  | 23        |
| <b>3. Décret n°2007-914 du 15 mai 2007 pris pour l'application du I de l'article 33 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés..</b>  | <b>24</b> |
| - Article 1 .....   | 24        |
| <b>4. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.</b>   | <b>25</b> |
| - Article 1 .....   | 25        |
| <b>5. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) .....</b> | <b>25</b> |
| - Article 4 Définitions .....   | 25        |
| <b>II. Constitutionnalité de la disposition contestée .....</b>   | <b>26</b> |
| <b>A. Normes de référence.....</b>  | <b>26</b> |
| <b>1. Déclaration des droits de l'homme et du citoyen de 1789 .....</b>   | <b>26</b> |
| - Article 2 .....   | 26        |
| <b>2. Constitution du 4 octobre 1958 .....</b>  | <b>26</b> |
| - Article 34 .....  | 26        |
| <b>B. Jurisprudence du Conseil constitutionnel.....</b>   | <b>27</b> |
| <b>Sur le droit au respect de la vie privée.....</b>  | <b>27</b> |
| - Décision n° 99-416 DC du 23 juillet 1999 - Loi portant création d'une couverture maladie universelle  | 27        |
| - Décision n° 2003-467 DC du 13 mars 2003 - Loi pour la sécurité intérieure.....  | 27        |
| - Décision n° 2004-492 DC du 2 mars 2004 - Loi portant adaptation de la justice aux évolutions de la criminalité.....   | 28        |
| - Décision n° 2004-499 DC du 29 juillet 2004 - Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés .....   | 28        |
| - Décision n° 2007-553 DC du 3 mars 2007 - Loi relative à la prévention de la délinquance .....   | 29        |
| - Décision n° 2010-604 DC du 25 février 2010 - Loi renforçant la lutte contre les violences de groupes et la protection des personnes chargées d'une mission de service public .....  | 29        |
| - Décision n° 2011-209 QPC du 17 janvier 2012 - M. Jean-Claude G. [Procédure de dessaisissement d'armes].....   | 30        |
| - Décision n° 2012-652 DC du 22 mars 2012 - Loi relative à la protection de l'identité .....  | 30        |
| - Décision n° 2013-684 DC du 29 décembre 2013 - Loi de finances rectificative pour 2013 .....   | 31        |
| - Décision n° 2015-713 DC du 23 juillet 2015 - Loi relative au renseignement.....   | 32        |
| - Décision n° 2015-715 DC du 5 août 2015 - Loi pour la croissance, l'activité et l'égalité des chances économiques .....  | 33        |
| - Décision n° 2015-722 DC du 26 novembre 2015 - Loi relative aux mesures de surveillance des communications électroniques internationales .....   | 35        |
| - Décision n° 2016-569 QPC du 23 septembre 2016 - Syndicat de la magistrature et autre [Transaction pénale par officier de police judiciaire - Participation des conseils départementaux de prévention de la délinquance et des zones de sécurité prioritaires à l'exécution des peines] .....  | 36        |
| - Décision n° 2016-590 QPC du 21 octobre 2016 - La Quadrature du Net et autres [Surveillance et contrôle des transmissions empruntant la voie hertzienne] .....   | 36        |
| - Décision n° 2017-637 QPC du 16 juin 2017 - Association nationale des supporters [Refus d'accès à une enceinte sportive et fichier d'exclusion].....   | 37        |
| - Décision n° 2019-789 QPC du 14 juin 2019 - Mme Hanen S. [Droit de communication des organismes de sécurité sociale] .....   | 37        |

|  |    |
|--|----|
| - 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].....         | 38 |
| - Décision n° 2020-800 DC du 11 mai 2020 - Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions .....  | 39 |
| - Décision n° 2020-841 QPC du 20 mai 2020 - La Quadrature du Net et autres [Droit de communication à la Hadopi].....   | 41 |
| - Décision n° 2020-808 DC du 13 novembre 2020 - Loi autorisant la prorogation de l'état d'urgence sanitaire et portant diverses mesures de gestion de la crise sanitaire ..... | 41 |
| - Décision n° 2021-817 DC du 20 mai 2021 - Loi pour une sécurité globale préservant les libertés .   | 42 |
| - Décision n° 2021-819 DC du 31 mai 2021 - Loi relative à la gestion de la sortie de crise sanitaire   | 43 |

# I. Contexte de la disposition contestée

## A. Dispositions contestées

### Code de la sécurité intérieure

#### LIVRE VIII : DU RENSEIGNEMENT

#### TITRE VI : DES AGENTS DES SERVICES SPECIALISES DE RENSEIGNEMENT

#### Chapitre III : De l'information des services de renseignement

- Article L. 863-2

*Modifié par LOI n°2016-987 du 21 juillet 2016 - art. 17*

Les services spécialisés de renseignement mentionnés à l'article L. 811-2 et les services désignés par le décret en Conseil d'Etat prévu à l'article L. 811-4 peuvent partager toutes les informations utiles à l'accomplissement de leurs missions définies au titre Ier du présent livre.

Les autorités administratives mentionnées à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives peuvent transmettre aux services mentionnés au premier alinéa du présent article, de leur propre initiative ou sur requête de ces derniers, des informations utiles à l'accomplissement des missions de ces derniers.

Les modalités et les conditions d'application du présent article sont déterminées par décret en Conseil d'Etat.

## B. Évolution des dispositions contestées

### 1. Loi n° 2015-912 du 24 juillet 2015 relative au renseignement

- Article 8

**I. - Après le titre V du livre VIII du code de la sécurité intérieure, tel qu'il résulte des articles 5 et 6 de la présente loi, il est inséré un titre VI intitulé : « Des agents des services spécialisés de renseignement ».**

**II. - Au même titre VI, il est inséré un chapitre Ier intitulé : « De la protection du secret de la défense nationale et de l'anonymat des agents » et comprenant les articles L. 861-1 à L. 861-3, tels qu'ils résultent des III et IV du présent article et du III de l'article 23 de la présente loi.**

**III. - Au début du même chapitre Ier, il est inséré un article L. 861-1 ainsi rédigé :**

« Art. L. 861-1. - Les actes réglementaires et individuels concernant l'organisation, la gestion et le fonctionnement des services mentionnés à l'article L. 811-2 et de ceux désignés par le décret en Conseil d'Etat prévu à l'article L. 811-4 ainsi que la situation de leurs agents sont pris dans des conditions qui garantissent la préservation de l'anonymat des agents.

« Lorsque, en application du premier alinéa du présent article, un acte ne peut être publié, son entrée en vigueur est subordonnée à son enregistrement dans un recueil spécial, dispensé de toute publication ou diffusion et tenu par le Premier ministre. Seuls les autorités publiques compétentes et les agents publics justifiant d'un intérêt ainsi que, dans les conditions et sous les réserves prévues au dernier alinéa, les juridictions administratives et judiciaires peuvent consulter un acte figurant dans ce recueil.

« Par dérogation à l'article 4 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, les décisions et les autres actes pris par les autorités administratives au sein des services mentionnés au premier alinéa du présent article peuvent comporter seulement, outre la signature, le numéro d'identification de leur auteur, attribué avec la délégation de signature et qui se substitue à la mention de ses prénom, nom et qualité. Le nombre de délégations de signature numérotées par service est fixé par arrêté du ministre compétent.

« Lorsque, dans le cadre d'une procédure engagée devant une juridiction administrative ou judiciaire, la solution du litige dépend d'une question relative à un acte non publié en application du présent article ou faisant l'objet

d'une signature numérotée, ce dernier est communiqué, à sa demande, à la juridiction ou au magistrat délégué par celle-ci, sans être versé au contradictoire. Si cet acte est protégé au titre du secret de la défense nationale, la juridiction peut demander sa déclassification et sa communication en application de l'article L. 2312-4 du code de la défense. »

IV. - Le même chapitre Ier est complété par un article L. 861-3 ainsi rédigé :

« Art. L. 861-3. - I. - Tout agent d'un service mentionné à l'article L. 811-2 ou d'un service désigné par le décret en Conseil d'Etat prévu à l'article L. 811-4 qui a connaissance, dans l'exercice de ses fonctions, de faits susceptibles de constituer une violation manifeste du présent livre peut porter ces faits à la connaissance de la seule Commission nationale de contrôle des techniques de renseignement, qui peut alors saisir le Conseil d'Etat dans les conditions prévues à l'article L. 833-8 et en informer le Premier ministre.

« Lorsque la commission estime que l'illégalité constatée est susceptible de constituer une infraction, elle saisit le procureur de la République dans le respect du secret de la défense nationale et transmet l'ensemble des éléments portés à sa connaissance à la Commission consultative du secret de la défense nationale afin que celle-ci donne au Premier ministre son avis sur la possibilité de déclassifier tout ou partie de ces éléments en vue de leur transmission au procureur de la République.

« II. - Aucun agent ne peut être sanctionné ou faire l'objet d'une mesure discriminatoire, directe ou indirecte, notamment en matière de rémunération, de recrutement, de titularisation, de notation, de discipline, de traitement, de formation, de reclassement, d'affectation, de qualification, de classification, de promotion professionnelle, de mutation, d'interruption ou de renouvellement de contrat, pour avoir porté, de bonne foi, des faits mentionnés au I à la connaissance de la Commission nationale de contrôle des techniques de renseignement. Tout acte contraire au présent alinéa est nul et non avenu.

« En cas de litige relatif à l'application du premier alinéa du présent II, il incombe à la partie défenderesse de prouver que sa décision est justifiée par des éléments objectifs étrangers à la déclaration ou au témoignage de l'agent intéressé.

« Tout agent qui relate ou témoigne des faits mentionnés au I, de mauvaise foi ou avec l'intention de nuire ou avec la connaissance au moins partielle de l'inexactitude des faits, encourt les peines prévues au premier alinéa de l'article 226-10 du code pénal. »

**V. - Le même titre VI est complété par des chapitres II et III ainsi rédigés :**

« Chapitre II De la protection juridique des agents

« Art. L. 862-1. - Lorsque des faits commis hors du territoire national, à des fins strictement nécessaires à l'accomplissement d'une mission commandée par ses autorités légitimes, par un agent des services mentionnés à l'article L. 811-2, sont portés à sa connaissance et paraissent susceptibles de constituer des infractions pénales, le procureur de la République territorialement compétent en informe le ministre dont relève le service de l'agent concerné aux fins de recueillir son avis préalablement à tout acte de poursuite. Hormis le cas d'urgence, cet avis est donné dans le délai d'un mois. L'avis est demandé par tout moyen dont il est fait mention au dossier de la procédure.

« L'avis figure au dossier de la procédure, à peine de nullité, sauf s'il n'a pas été formulé dans le délai précité ou en cas d'urgence.

« Art. L. 862-2. - Les agents des services spécialisés de renseignement sont pénalement responsables de leurs actes dans les conditions définies au titre II du livre Ier du code pénal.

« **Chapitre III De l'information des services de renseignement**

« Art. L. 863-1. - Dans l'accomplissement de leurs missions définies au titre Ier du présent livre, les agents individuellement désignés et habilités des services mentionnés à l'article L. 811-2 ou des services désignés par le décret en Conseil d'Etat prévu à l'article L. 811-4 peuvent procéder aux actes suivants sans en être pénalement responsables :

« 1° Etre en contact, par le moyen d'échanges électroniques et dans les conditions prévues à l'article L. 861-2, avec des personnes susceptibles de porter atteinte aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 ;

« 2° Extraire, acquérir ou conserver par ce moyen des données sur les personnes mentionnées au 1° du présent article ;

« 3° Extraire, transmettre en réponse à une demande expresse, acquérir ou conserver des contenus provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie.

« Ces actes ne peuvent constituer une incitation à commettre des infractions, sous peine d'un an d'emprisonnement et de 30 000 € d'amende.

« Art. L. 863-2. - Les services spécialisés de renseignement mentionnés à l'article L. 811-2 et les services désignés par le décret en Conseil d'Etat prévu à l'article L. 811-4 peuvent échanger toutes les informations utiles à l'accomplissement de leurs missions définies au titre Ier du présent livre.

« Les autorités administratives mentionnées à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives peuvent transmettre aux services mentionnés au premier alinéa du présent article, de leur propre initiative ou sur requête de ces derniers, des informations utiles à l'accomplissement des missions de ces derniers.

« Les modalités et les conditions d'application du présent article sont déterminées par décret en Conseil d'Etat. »

## **2. Loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste**

### **- Article 17**

Le livre VIII du même code est ainsi modifié :

1° Au III de l'article L. 852-1, le mot : « nécessaires » est remplacé par le mot : « associés » ;

2° Au premier alinéa de l'article L. 863-2, le mot : « échanger » est remplacé par le mot : « partager ».

## **C. Autres dispositions**

### **1. Code de la sécurité intérieure**

#### **LIVRE VIII : DU RENSEIGNEMENT**

##### **- Article L. 801-1**

*Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 22*

Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte 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.

L'autorisation et la mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées aux chapitres Ier à III du titre V du présent livre ne peuvent être décidées que si :

1° Elles procèdent d'une autorité ayant légalement compétence pour le faire ;

2° Elles résultent d'une procédure conforme au titre II du même livre ;

3° Elles respectent les missions confiées aux services mentionnés à l'article L. 811-2 ou aux services désignés par le décret en Conseil d'Etat prévu à l'article L. 811-4 ;

4° Elles sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 ;

5° Les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoqués.

La Commission nationale de contrôle des techniques de renseignement s'assure, dans les conditions prévues au présent livre, du respect de ces principes. Le Conseil d'Etat statue sur les recours formés contre les décisions relatives à l'autorisation et à la mise en œuvre de ces techniques et ceux portant sur la conservation des renseignements collectés.

## **TITRE Ier : DISPOSITIONS GÉNÉRALES**

### **- Article L. 811-1**

*Création LOI n°2015-912 du 24 juillet 2015 - art. 2*

La politique publique de renseignement concourt à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation. Elle relève de la compétence exclusive de l'Etat.

### **- Article L. 811-2**

*Création LOI n°2015-912 du 24 juillet 2015 - art. 2*

Les services spécialisés de renseignement sont désignés par décret en Conseil d'Etat. Ils ont pour missions, en France et à l'étranger, la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. Ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et de ces menaces.

Ils agissent dans le respect de la loi, sous l'autorité du Gouvernement et conformément aux orientations déterminées par le Conseil national du renseignement.

La mise en œuvre sur le territoire national du chapitre II du titre II et des chapitres Ier à III du titre V du présent livre est effectuée sans préjudice du second alinéa de l'article 40 du code de procédure pénale.

### **- Article L. 811-3**

*Création LOI n°2015-912 du 24 juillet 2015 - art. 2*

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.

### **- Article L. 811-4**

*Modifié par LOI n°2016-731 du 3 juin 2016 - art. 14*

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.

## **TITRE II : DE LA PROCÉDURE APPLICABLE AUX TECHNIQUES DE RECUEIL DE RENSEIGNEMENT SOUMISES À AUTORISATION**

### **Chapitre Ier : De l'autorisation de mise en œuvre**

#### **- Article L. 821-1**

*Modifié par LOI n°2017-1510 du 30 octobre 2017 - art. 15 (V)*

La mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées aux chapitres Ier à IV du titre V du présent livre est soumise à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement.

Ces techniques ne peuvent être mises en œuvre que par des agents individuellement désignés et habilités.

#### **- Article L. 821-4**

*Modifié par LOI n°2017-1510 du 30 octobre 2017 - art. 15 (V)*

L'autorisation de mise en œuvre des techniques mentionnées aux chapitres Ier à IV du titre V du présent livre est délivrée par le Premier ministre pour une durée maximale de quatre mois. Le Premier ministre ne peut déléguer cette attribution individuellement qu'à des collaborateurs directs habilités au secret de la défense nationale.

L'autorisation comporte les motivations et mentions prévues aux 1° à 6° de l'article L. 821-2. Toute autorisation est renouvelable dans les mêmes conditions que celles prévues au présent chapitre.

Lorsque l'autorisation est délivrée après un avis défavorable de la Commission nationale de contrôle des techniques de renseignement, elle indique les motifs pour lesquels cet avis n'a pas été suivi.

L'autorisation du Premier ministre est communiquée sans délai au ministre responsable de son exécution ainsi qu'à la commission.

La demande et l'autorisation sont enregistrées par les services du Premier ministre. Les registres sont tenus à la disposition de la Commission nationale de contrôle des techniques de renseignement.

### **Chapitre II : Des renseignements collectés**

#### **- Article L. 822-2**

*Modifié par LOI n°2017-1510 du 30 octobre 2017 - art. 15 (V)*

I.- Les renseignements collectés par la mise en œuvre d'une technique de recueil de renseignement autorisée en application du chapitre Ier du présent titre sont détruits à l'issue d'une durée de :

1° Trente jours à compter de leur recueil pour les correspondances interceptées en application des articles L. 852-1 et L. 852-2 et pour les paroles captées en application de l'article L. 853-1 ;

2° Cent vingt jours à compter de leur recueil pour les renseignements collectés par la mise en œuvre des techniques mentionnées au chapitre III du titre V du présent livre, à l'exception des informations ou documents mentionnés à l'article L. 851-1 ;

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.

II.- Par dérogation au I, les renseignements qui concernent une requête dont le Conseil d'Etat a été saisi ne peuvent être détruits. A l'expiration des délais prévus au même I, ils sont conservés pour les seuls besoins de la procédure devant le Conseil d'Etat.

- **Article L. 822-3**

*Création LOI n°2015-912 du 24 juillet 2015 - art. 2*

Les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles mentionnées à l'article L. 811-3. Ces opérations sont soumises au contrôle de la Commission nationale de contrôle des techniques de renseignement.

Les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite de ces finalités.

**TITRE III : DE LA COMMISSION NATIONALE DE CONTRÔLE DES TECHNIQUES DE RENSEIGNEMENT**

**Chapitre III : Missions**

- **Article L. 833-2**

*Création LOI n°2015-912 du 24 juillet 2015 - art. 2*

Pour l'accomplissement de ses missions, la commission :

- 1° Reçoit communication de toutes demandes et autorisations mentionnées au présent livre ;
- 2° Dispose d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions et extractions mentionnés au présent livre [Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015], ainsi qu'aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements en application de l'article L. 822-1 ;
- 3° Est informée à tout moment, à sa demande, des modalités d'exécution des autorisations en cours ;
- 4° Peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de ses missions, y compris lorsque la technique de recueil de renseignement mise en œuvre n'a fait l'objet ni d'une demande, ni d'une autorisation ou ne répond pas aux conditions de traçabilité, à l'exclusion des éléments communiqués par des services étrangers ou par des organismes internationaux ou qui pourraient donner connaissance à la commission, directement ou indirectement, de l'identité des sources des services spécialisés de renseignement ;
- 5° Peut solliciter du Premier ministre tout ou partie des rapports de l'inspection des services de renseignement ainsi que des rapports des services d'inspection générale des ministères portant sur les services qui relèvent de leur compétence, en lien avec les missions de la commission.

**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**

*Modifié par LOI n°2017-1510 du 30 octobre 2017 - art. 15 (V)*

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. 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. L'article L. 821-5 n'est pas applicable à une autorisation délivrée en application du présent article.

- **Article L. 851-3**

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

I. Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste.

Ces traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1, sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent.

Dans le respect du principe de proportionnalité, l'autorisation du Premier ministre précise le champ technique de la mise en œuvre de ces traitements.

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.

La première autorisation de mise en œuvre des traitements automatisés prévue au I du présent article est délivrée pour une durée de deux mois. L'autorisation est renouvelable dans les conditions de durée prévues au chapitre Ier du titre II du présent livre. La demande de renouvellement comporte un relevé du nombre d'identifiants signalés par le traitement automatisé et une analyse de la pertinence de ces signalements.

III. Les conditions prévues à l'article L. 871-6 sont applicables aux opérations matérielles effectuées pour cette mise en œuvre par les opérateurs et les personnes mentionnés à l'article L. 851-1.

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.

V. L'article L. 821-5 n'est pas applicable à une autorisation délivrée en application du présent article.

- **Article L. 851-4**

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

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 recueillies sur sollicitation du réseau et transmis en temps réel par les opérateurs à un service du Premier ministre.

- **Article L. 851-5**

*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 autorisée l'utilisation d'un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet.

Si la mise en œuvre de cette technique nécessite l'introduction dans un véhicule ou dans un lieu privé, cette mesure s'effectue selon les modalités définies à l'article L. 853-3.

- **Article L. 851-6**

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

I. Dans les conditions prévues au chapitre Ier du titre II du présent livre, peuvent être directement recueillies, au moyen d'un appareil ou d'un dispositif technique mentionné au 1° de l'article 226-3 du code pénal, les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés.

Par dérogation à l'article L. 821-4 du présent code, l'autorisation est délivrée pour une durée de deux mois, renouvelable dans les mêmes conditions de durée.

II. Les appareils ou dispositifs techniques mentionnés au I font l'objet d'une inscription dans un registre spécial tenu à la disposition de la Commission nationale de contrôle des techniques de renseignement et ne peuvent être mis en œuvre que par des agents individuellement désignés et habilités.

III. Un service du Premier ministre centralise les informations ou documents recueillis, qui sont :

1° Conservés dans les conditions prévues à l'article L. 822-2, s'ils se rapportent à l'autorisation de mise en œuvre ;

2° Détruits dès qu'il apparaît qu'ils ne sont pas en rapport avec l'autorisation de mise en œuvre, dans un délai maximal de quatre-vingt-dix jours.

IV. Le nombre maximal d'appareils ou de dispositifs techniques mentionnés au II du présent article pouvant être utilisés 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 est portée à la connaissance de la commission.

- **Article L. 851-7**

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

Le présent chapitre est mis en œuvre dans le respect de l'article 226-15 du code pénal.

## **Chapitre II : Des interceptions de sécurité**

- **Article L. 852-1**

*Modifié par LOI n°2016-987 du 21 juillet 2016 - art. 17*

I.- Dans les conditions prévues au chapitre Ier du titre II du présent livre, peuvent être autorisées les interceptions de correspondances émises par la voie des communications électroniques et susceptibles de révéler des renseignements relatifs aux finalités mentionnées à l'article L. 811-3. Lorsqu'il existe des raisons sérieuses de croire qu'une ou plusieurs personnes appartenant à l'entourage d'une 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 pour ces personnes.

II.- Pour les seules finalités mentionnées aux 1° et 4° et a du 5° de l'article L. 811-3 du présent code, peut être autorisée, pour une durée de quarante-huit heures renouvelable, l'utilisation d'un appareil ou d'un dispositif technique mentionné au 1° de l'article 226-3 du code pénal afin d'intercepter des correspondances émises ou reçues par un équipement terminal. Les correspondances interceptées par cet appareil ou ce dispositif technique sont détruites dès qu'il apparaît qu'elles sont sans lien avec l'autorisation délivrée, dans la limite du délai prévu au 1° du I de l'article L. 822-2 du présent code.

III.- L'autorisation vaut autorisation de recueil des informations ou documents mentionnés à l'article L. 851-1 associés à l'exécution de l'interception et à son exploitation.

IV.- Un service du Premier ministre organise la centralisation de l'exécution des interceptions mentionnées au I. Après avis de la Commission nationale de contrôle des techniques de renseignement, le Premier ministre définit les modalités de la centralisation des correspondances interceptées en application du II.

V.- Les opérations de transcription et d'extraction des communications interceptées, auxquelles la Commission nationale de contrôle des techniques de renseignement dispose d'un accès permanent, complet, direct et immédiat, sont effectuées au sein d'un service du Premier ministre.

VI.- Le nombre maximal des autorisations d'interception 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.

- **Article L. 852-2**

*Création LOI n°2017-1510 du 30 octobre 2017 - art. 15 (V)*

Dans les conditions prévues au chapitre Ier du titre II du présent livre, peuvent être autorisées les interceptions de correspondances échangées au sein d'un réseau de communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques, lorsque ce réseau est conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs. Pour l'application du 6° de l'article L. 821-2, lorsque l'identité de la personne concernée n'est pas connue, la demande précise les éléments nécessaires à l'identification du réseau concerné.

L'autorisation mentionnée au premier alinéa du présent article vaut autorisation de recueil des informations ou documents mentionnés à l'article L. 851-1 associés à l'exécution de l'interception et à son exploitation.

### **Chapitre III : De la sonorisation de certains lieux et véhicules et de la captation d'images et de données informatiques**

#### **- Article L. 853-1**

*Création LOI n°2015-912 du 24 juillet 2015 - art. 6*

I.- Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisée, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant la captation, la fixation, la transmission et l'enregistrement de paroles prononcées à titre privé ou confidentiel, ou d'images dans un lieu privé.

II.- Par dérogation à l'article L. 821-4, l'autorisation est délivrée pour une durée maximale de deux mois, renouvelable dans les mêmes conditions de durée.

III.- Les dispositifs techniques mentionnés au I du présent article ne peuvent être utilisés que par des agents appartenant à l'un des services mentionnés aux articles L. 811-2 et L. 811-4 dont la liste est fixée par décret en Conseil d'Etat.

IV.- Le service autorisé à recourir à la technique mentionnée au I du présent article rend compte à la Commission nationale de contrôle des techniques de renseignement de sa mise en œuvre. La commission peut à tout moment adresser une recommandation tendant à ce que cette opération soit interrompue et que les renseignements collectés soient détruits.

V.- Si la mise en œuvre de cette technique nécessite l'introduction dans un véhicule ou dans un lieu privé, cette mesure s'effectue selon les modalités définies à l'article L. 853-3.

#### **- Article L. 853-2**

*Modifié par LOI n°2017-1510 du 30 octobre 2017 - art. 15 (V)*

I. - Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisée, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant :

1° D'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre ;

2° D'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques.

II. - Par dérogation à l'article L. 821-4, l'autorisation de mise en œuvre de la technique mentionnée au 1° du I du présent article est délivrée pour une durée maximale de trente jours et celle mentionnée au 2° du même I pour une durée maximale de deux mois. L'autorisation est renouvelable dans les mêmes conditions de durée.

III. - Les dispositifs techniques mentionnés au I du présent article ne peuvent être utilisés que par des agents appartenant à l'un des services mentionnés aux articles L. 811-2 et L. 811-4 dont la liste est fixée par décret en Conseil d'Etat.

IV. - Le service autorisé à recourir à la technique mentionnée au I rend compte à la Commission nationale de contrôle des techniques de renseignement de sa mise en œuvre. La commission peut à tout moment adresser une recommandation tendant à ce que cette opération soit interrompue et que les renseignements collectés soient détruits.

V. - Si la mise en œuvre de cette technique nécessite l'introduction dans un véhicule ou dans un lieu privé, cette mesure s'effectue selon les modalités définies à l'article L. 853-3.

- **Article L. 853-3**

*Création LOI n°2015-912 du 24 juillet 2015 - art. 6*

I.- Dans les conditions prévues au chapitre Ier du titre II du présent livre, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'introduction dans un véhicule ou dans un lieu privé à la seule fin de mettre en place, d'utiliser ou de retirer les dispositifs techniques mentionnés aux articles L. 851-5, L. 853-1 et L. 853-2 peut être autorisée. S'il s'agit d'un lieu d'habitation ou pour l'utilisation de la technique mentionnée au 1° du I de l'article L. 853-2, l'autorisation ne peut être donnée qu'après avis exprès de la Commission nationale de contrôle des techniques de renseignement, statuant en formation restreinte ou en formation plénière.

L'introduction dans un véhicule ou dans un lieu privé ne peut être effectuée que par des agents individuellement désignés et habilités appartenant à l'un des services mentionnés aux articles L. 811-2 et L. 811-4 dont la liste est fixée par décret en Conseil d'Etat.

II.- Lorsqu'il est fait application de l'avant-dernier alinéa de l'article L. 821-2, la demande mentionne, lorsqu'ils sont connus, toute indication permettant d'identifier le lieu, son usage, son propriétaire ou toute personne bénéficiant d'un droit, ainsi que la nature détaillée du dispositif envisagé.

III.- Par dérogation à l'article L. 821-4, l'autorisation, spécialement motivée, est délivrée pour une durée maximale de trente jours et est renouvelable dans les mêmes conditions de durée que l'autorisation initiale. Elle ne vaut que pour les actes d'installation, d'utilisation, de maintenance ou de retrait des dispositifs techniques.

Lorsque l'introduction mentionnée au I du présent article et portant sur un lieu privé à usage d'habitation est autorisée après avis défavorable de la Commission nationale de contrôle des techniques de renseignement, le Conseil d'Etat est immédiatement saisi par le président de la commission ou, à défaut, par l'un des membres de la commission parmi ceux mentionnés aux 2° et 3° de l'article L. 831-1 du présent code. La formation spécialisée mentionnée à l'article L. 773-2 du code de justice administrative, le président de la formation restreinte mentionnée au même article L. 773-2 ou le membre qu'il délègue statue dans un délai de vingt-quatre heures à compter de cette saisine. La décision d'autorisation du Premier ministre ne peut être exécutée avant que le Conseil d'Etat n'ait statué, sauf si elle a été délivrée au titre du 4° de l'article L. 811-3 du présent code et que le Premier ministre a ordonné sa mise en œuvre immédiate.

IV.- Le service autorisé à recourir à l'introduction dans un véhicule ou dans un lieu privé rend compte à la commission de sa mise en œuvre. La commission peut à tout moment adresser une recommandation tendant à ce que cette opération soit interrompue et que les renseignements collectés soient détruits.

## **Chapitre IV : Des mesures de surveillance des communications électroniques internationales**

- **Article L. 854-1**

*Modifié par LOI n°2018-607 du 13 juillet 2018 - art. 37*

Dans les conditions prévues au présent chapitre, peut être autorisée, aux seules fins de défense et de promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3, la surveillance des communications qui sont émises ou reçues à l'étranger.

Cette surveillance, qu'elle porte sur des correspondances ou sur des données de connexion, est exclusivement régie par le présent chapitre.

Les mesures prises à ce titre ne peuvent avoir pour objet d'assurer la surveillance individuelle des communications de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, à l'exception du cas où ces personnes communiquent depuis l'étranger et, soit faisaient l'objet d'une autorisation d'interception de sécurité, délivrée en application de l'article L. 852-1, à la date à laquelle elles ont quitté le territoire national, soit sont identifiées comme présentant une menace au regard des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3.

Les autorisations prévues aux articles L. 851-1, L. 851-2 et au I de l'article L. 852-1 peuvent valoir, lorsque la décision d'autorisation le prévoit, autorisation d'exploitation des communications, ou des seules données de connexion, interceptées dans le cadre de la mise en œuvre de mesures de surveillance des communications internationales, dans la limite de la portée de ces autorisations et dans le respect des garanties qui les entourent.

Sous réserve des dispositions particulières des troisième et quatrième alinéas du présent article ainsi que du V de l'article L. 854-2, lorsqu'il apparaît que des communications électroniques interceptées sont échangées entre

des personnes ou des équipements utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, y compris lorsque ces communications transitent par des équipements non rattachables à ce territoire, celles-ci sont instantanément détruites.

- **Article L. 854-2**

*Modifié par LOI n°2018-607 du 13 juillet 2018 - art. 37*

I.- Le Premier ministre désigne, par une décision motivée, les réseaux de communications électroniques sur lesquels il autorise l'interception des communications émises ou reçues à l'étranger, dans les limites fixées à l'article L. 854-1.

II.- Sur demande motivée des ministres ou de leurs délégués mentionnés au premier alinéa de l'article L. 821-2, le Premier ministre ou l'une des personnes déléguées mentionnées à l'article L. 821-4 peut autoriser l'exploitation non individualisée des données de connexion interceptées.

L'autorisation désigne :

1° La ou les finalités poursuivies parmi celles mentionnées à l'article L. 811-3 ;

2° Le ou les motifs des mesures ;

3° Le ou les services mentionnés à l'article L. 811-2 en charge de cette exploitation ;

4° Le type de traitements automatisés pouvant être mis en œuvre, en précisant leur objet.

L'autorisation, renouvelable dans les mêmes conditions que celles prévues au présent II, est délivrée pour une durée maximale d'un an.

III.- Sur demande motivée des ministres ou de leurs délégués mentionnés au premier alinéa de l'article L. 821-2, le Premier ministre ou l'un de ses délégués peut également, après avis de la Commission nationale de contrôle des techniques de renseignement, délivrer une autorisation d'exploitation de communications, ou de seules données de connexion, interceptées.

L'autorisation désigne :

1° La ou les finalités poursuivies parmi celles mentionnées à l'article L. 811-3 ;

2° Le ou les motifs des mesures ;

3° Les zones géographiques ou les organisations, groupes de personnes ou personnes concernés ;

4° Le ou les services mentionnés à l'article L. 811-2 en charge de cette exploitation.

L'autorisation, renouvelable dans les mêmes conditions que celles prévues au présent III, est délivrée pour une durée maximale de quatre mois.

IV.- L'autorisation prévue au III vaut autorisation d'effectuer au sein des données de connexion interceptées des vérifications ponctuelles aux seules fins de détecter une menace pour les intérêts fondamentaux de la Nation liée aux relations entre des numéros d'abonnement ou des identifiants techniques rattachables au territoire français et des zones géographiques, organisations ou personnes mentionnés au 3° du même III.

A la seule fin de détecter, de manière urgente, une menace terroriste, cette vérification ponctuelle peut porter sur les communications de numéros d'abonnement ou d'identifiants techniques rattachables au territoire national. Ces numéros et identifiants sont immédiatement communiqués au Premier ministre et à la Commission nationale de contrôle des techniques de renseignement, pour les besoins du contrôle prévu à l'article L. 854-9.

Des vérifications ponctuelles peuvent également être mises en œuvre pour détecter sur les communications d'identifiants techniques rattachables au territoire national, à des fins d'analyse technique, des éléments de cyberattaques susceptibles de porter atteinte aux intérêts fondamentaux de la Nation mentionnés au 1° de l'article L. 811-3.

Lorsque les vérifications ponctuelles mentionnées au présent IV font apparaître la nécessité d'une surveillance, l'exploitation des communications ou des seules données de connexion interceptées ne peut être poursuivie que sur le fondement d'une autorisation obtenue en application des chapitres Ier ou II du présent titre ou du V du présent article, dans le respect des règles qui leur sont propres.

V.- Par dérogation au troisième alinéa de l'article L. 854-1 et pour la défense ou la promotion des finalités mentionnées aux 1°, 2°, 4°, 6° et 7° de l'article L. 811-3, le Premier ministre ou l'un de ses délégués peut, dans les conditions prévues au III du présent article, délivrer une autorisation d'exploitation de communications ou de seules données de connexion interceptées, de numéros d'abonnement ou d'identifiants techniques rattachables au territoire national dont l'utilisateur communique depuis ce territoire.

Le nombre maximal des autorisations d'exploitation, en vigueur simultanément et portant sur des correspondances, 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 sont portées à la connaissance de la commission.

- **Article L. 854-3**

*Création LOI n°2015-1556 du 30 novembre 2015 - art. 1*

Les personnes qui exercent en France un mandat ou une profession mentionné à l'article L. 821-7 ne peuvent faire l'objet d'une surveillance individuelle de leurs communications à raison de l'exercice du mandat ou de la profession concerné.

- **Article L. 854-4**

*Modifié par LOI n°2018-607 du 13 juillet 2018 - art. 37*

L'interception et l'exploitation des communications en application du présent chapitre ainsi que la vérification ponctuelle mentionnée au IV de l'article L. 854-2 ainsi que la vérification ponctuelle mentionnée au IV de l'article L. 854-2 font l'objet de dispositifs de traçabilité organisés par le Premier ministre après avis de la Commission nationale de contrôle des techniques de renseignement. Le Premier ministre définit les modalités de la centralisation des renseignements collectés.

- **Article L. 854-5**

*Création LOI n°2015-1556 du 30 novembre 2015 - art. 1*

Sous réserve des dispositions particulières de l'article L. 854-8, les renseignements collectés en application du présent chapitre sont détruits à l'issue d'une durée de :

1° Douze mois à compter de leur première exploitation pour les correspondances, dans la limite d'une durée de quatre ans à compter de leur recueil ;

2° Six ans à compter de leur recueil pour les données de connexion.

Pour ceux des renseignements qui sont chiffrés, le délai court à compter de leur déchiffrement. Ils ne peuvent être conservés plus de huit 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 au titre du présent chapitre 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 article.

Par dérogation aux cinq premiers alinéas, les renseignements qui concernent une requête dont le Conseil d'Etat a été saisi ne peuvent être détruits. A l'expiration des délais prévus au présent article, ils sont conservés pour les seuls besoins de la procédure devant le Conseil d'Etat.

- **Article L. 854-6**

*Création LOI n°2015-1556 du 30 novembre 2015 - art. 1*

Sous réserve des dispositions particulières de l'article L. 854-8, les renseignements collectés en application du présent chapitre sont exploités par le ou les services mentionnés à l'article L. 811-2 désignés par l'autorisation.

Les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles mentionnées à l'article L. 811-3.

Les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite des finalités mentionnées au même article L. 811-3.

Les opérations de destruction des renseignements collectés, les transcriptions et les extractions sont effectuées par des agents individuellement désignés et habilités et font l'objet de relevés.

- **Article L. 854-7**

*Création LOI n°2015-1556 du 30 novembre 2015 - art. 1*

Les conditions prévues aux articles L. 871-6 et L. 871-7 sont applicables aux opérations matérielles effectuées par les opérateurs de communications électroniques pour la mise en œuvre des mesures prévues au I de l'article L. 854-2.

- **Article L. 854-8**

*Création LOI n°2015-1556 du 30 novembre 2015 - art. 1*

Lorsque les correspondances interceptées renvoient à des numéros d'abonnement ou à des identifiants techniques rattachables au territoire national, elles sont exploitées dans les conditions prévues aux IV et V de l'article L. 852-1 et conservées et détruites dans les conditions prévues aux articles L. 822-2 à L. 822-4, sous le contrôle de la Commission nationale de contrôle des techniques de renseignement. Le délai de conservation des correspondances court toutefois à compter de leur première exploitation, mais ne peut excéder six mois à compter de leur recueil. Les données de connexion associées à ces correspondances sont conservées et détruites dans les conditions prévues aux mêmes articles L. 822-2 à L. 822-4.

- **Article L. 854-9**

*Modifié par LOI n°2018-607 du 13 juillet 2018 - art. 37*

La Commission nationale de contrôle des techniques de renseignement émet un avis sur les demandes mentionnées aux III et V de l'article L. 854-2 dans les délais prévus à l'article L. 821-3. Elle reçoit communication de toutes les décisions et autorisations mentionnées à l'article L. 854-2. Elle dispose d'un accès permanent, complet et direct aux dispositifs de traçabilité mentionnés à l'article L. 854-4, aux renseignements collectés, aux transcriptions et extractions réalisées ainsi qu'aux relevés mentionnés à l'article L. 854-6. A sa demande, elle peut contrôler les dispositifs techniques nécessaires à l'exécution des décisions et des autorisations. Si la surveillance des personnes mentionnées au troisième alinéa de l'article L. 854-1 n'a pas déjà fait l'objet d'une autorisation spécifique, leur identité est portée sans délai à la connaissance de la commission.

La commission peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de ses missions.

L'article L. 833-3 est applicable aux contrôles effectués par la commission en application du présent article.

De sa propre initiative ou sur réclamation de toute personne souhaitant vérifier qu'aucune mesure de surveillance ou de vérification ponctuelle n'est irrégulièrement mise en œuvre à son égard, la commission s'assure que les mesures mises en œuvre au titre du présent chapitre respectent les conditions qu'il fixe ainsi que celles définies par les textes pris pour son application et par les décisions et autorisations du Premier ministre ou de ses délégués. Elle notifie à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer la mise en œuvre de mesures de surveillance ou de vérification ponctuelle.

Lorsqu'elle constate un manquement au présent chapitre, la commission adresse au Premier ministre une recommandation tendant à ce que le manquement cesse et que les renseignements collectés soient, le cas échéant, détruits. Lorsque le Premier ministre ne donne pas suite à cette recommandation ou que les suites qui y sont données sont estimées insuffisantes, le Conseil d'Etat, statuant dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, peut être saisi par le président ou par au moins trois membres de la commission. Toutefois, toute personne souhaitant vérifier qu'elle n'a pas fait l'objet d'une surveillance irrégulière au titre du V de l'article L. 854-2 du présent code peut saisir le Conseil d'Etat du recours prévu au 1° de l'article L. 841-1.

La commission peut adresser à tout moment au Premier ministre les recommandations et les observations qu'elle juge nécessaires au titre du contrôle qu'elle exerce sur l'application du présent chapitre.

## Chapitre V : Des mesures de surveillance de certaines communications hertziennes

### - **Article L. 855-1 A**

*Création LOI n°2017-1510 du 30 octobre 2017 - art. 15 (V)*

Les services de renseignement mentionnés aux articles L. 811-2 et L. 811-4 sont autorisés, aux seules fins de la défense et de la promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3, à procéder à l'interception et à l'exploitation des communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques lorsque cette interception et cette exploitation n'entrent dans le champ d'application d'aucune des techniques de renseignement prévues aux chapitres Ier à IV du présent titre. Ces mesures de surveillance sont exclusivement régies par le présent chapitre.

### - **Article L. 855-1 B**

*Création LOI n°2017-1510 du 30 octobre 2017 - art. 15 (V)*

I.- Les renseignements collectés en application de l'article L. 855-1 A sont détruits à l'issue d'une durée de six ans à compter de leur recueil.

Pour ceux des renseignements qui sont chiffrés, le délai court à compter de leur déchiffrement. Ils ne peuvent être conservés plus de huit ans à compter de leur recueil.

II.- Les renseignements mentionnés au I ne peuvent être transcrits ou extraits pour d'autres finalités que celles mentionnées à l'article L. 811-3. Les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite des finalités mentionnées au même article L. 811-3.

### - **Article L. 855-1 C**

*Création LOI n°2017-1510 du 30 octobre 2017 - art. 15 (V)*

La Commission nationale de contrôle des techniques de renseignement veille au respect des champs d'application respectifs des articles des chapitres Ier à IV du présent titre régissant les techniques de renseignement et de l'article L. 855-1 A.

A ce titre, elle est informée du champ et de la nature des mesures prises en application du même article L. 855-1 A. Elle peut, à sa demande et à la seule fin de s'assurer du respect des champs d'application mentionnés au premier alinéa du présent article, se faire présenter sur place les capacités d'interception mises en œuvre sur le fondement dudit article L. 855-1 A et se faire communiquer les renseignements collectés conservés à la date de sa demande et les transcriptions et extractions réalisées.

La commission peut, à tout moment, adresser au Premier ministre, ainsi qu'à la délégation parlementaire au renseignement, les recommandations et observations qu'elle juge nécessaires au titre du contrôle qu'elle exerce sur l'application du présent chapitre.

## **2. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**

### **- Article 2**

*Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 1*

La présente loi s'applique aux traitements automatisés en tout ou partie de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, lorsque leur responsable remplit les conditions prévues à l'article 3 de la présente loi, à l'exception des traitements mis en œuvre par des personnes physiques pour l'exercice d'activités strictement personnelles ou domestiques.

Constitue un fichier de données à caractère personnel tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

Sauf dispositions contraires, dans le cadre de la présente loi s'appliquent les définitions de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016.

*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.*

### **- Article 4**

*Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 1*

Les données à caractère personnel doivent être :

1° Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ;

2° Collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des dispositions du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, applicables à de tels traitements et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;

3° Adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives ;

4° Exactes et, si nécessaire, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder ;

5° Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Toutefois, les données à caractère personnel peuvent être conservées au-delà de cette durée dans la mesure où elles sont traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques. Le choix des données conservées à des fins archivistiques dans l'intérêt public est opéré dans les conditions prévues à l'article L. 212-3 du code du patrimoine ;

6° Traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non autorisées, à l'aide de mesures techniques ou organisationnelles appropriées.

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.

- **Article 6**

*Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 1*

I. Il est interdit de traiter des données à caractère personnel 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 physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

II. Les exceptions à l'interdiction mentionnée au I sont fixées dans les conditions prévues par le 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 et par la présente loi.

III. De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés suivant les modalités prévues au II de l'article 31 et à l'article 32.

*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.*

- **Article 19**

*Modifié par Ordonnance n°2019-964 du 18 septembre 2019 - art. 35 (VD)*

I. Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités dans les conditions définies au dernier alinéa de l'article 10 ont accès, de 6 heures à 21 heures, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement de données à caractère personnel.

Le procureur de la République territorialement compétent en est préalablement informé.

Lorsqu'un traitement de données à caractère personnel est mis en œuvre, soit dans les parties de ces lieux, locaux, enceintes, installations ou établissements affectées au domicile privé, soit dans de tels lieux, locaux, enceintes, installations ou établissements entièrement affectés au domicile privé, la visite ne peut se dérouler qu'après l'autorisation du juge des libertés et de la détention du tribunal judiciaire dans le ressort duquel sont situés les locaux à visiter, dans les conditions prévues au II du présent article.

II. Le responsable de ces lieux, locaux, enceintes, installations ou établissements est informé de son droit d'opposition à la visite. Lorsqu'il exerce ce droit, la visite ne peut se dérouler qu'après l'autorisation du juge des libertés et de la détention du tribunal judiciaire dans le ressort duquel sont situés les locaux à visiter, qui statue dans des conditions fixées par décret en Conseil d'Etat. Toutefois, lorsque l'urgence, la gravité des faits à l'origine du contrôle ou le risque de destruction ou de dissimulation de documents le justifie, la visite peut avoir lieu sans que le responsable des locaux en ait été informé, sur autorisation préalable du juge des libertés et de la détention. Dans ce cas, le responsable des lieux ne peut s'opposer à la visite.

La visite s'effectue sous l'autorité et le contrôle du juge des libertés et de la détention qui l'a autorisée, en présence de l'occupant des lieux ou de son représentant qui peut se faire assister d'un conseil de son choix ou, à défaut, en présence de deux témoins qui ne sont pas placés sous l'autorité des personnes chargées de procéder au contrôle.

L'ordonnance ayant autorisé la visite est exécutoire au seul vu de la minute. Elle mentionne que le juge ayant autorisé la visite peut être saisi à tout moment d'une demande de suspension ou d'arrêt de cette visite. Elle indique le délai et la voie de recours. Elle peut faire l'objet, suivant les règles prévues par le code de procédure civile, d'un appel devant le premier président de la cour d'appel. Celui-ci connaît également des recours contre le déroulement des opérations de visite dont la finalité est l'exercice effectif des missions prévues au III.

III. Pour l'exercice des missions relevant de la Commission nationale de l'informatique et des libertés en application du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, les membres et agents mentionnés au premier alinéa du I du présent article peuvent demander communication de tous documents nécessaires à

l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie. Ils peuvent recueillir, notamment sur place ou sur convocation, tout renseignement et toute justification utiles et nécessaires à l'accomplissement de leur mission. Ils peuvent accéder, dans des conditions préservant la confidentialité à l'égard des tiers, aux programmes informatiques et aux données ainsi qu'en demander la transcription par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle. Le secret ne peut leur être opposé sauf concernant les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou, sous réserve du deuxième alinéa du présent III, par le secret médical.

Le secret médical est opposable s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé. La communication des données médicales individuelles incluses dans cette catégorie de traitement ne peut alors se faire que sous l'autorité et en présence d'un médecin.

En dehors des contrôles sur place et sur convocation, ils peuvent procéder à toute constatation utile. Ils peuvent notamment, à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations. Ils peuvent retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle.

Pour le contrôle de services de communication au public en ligne, les membres et agents mentionnés au premier alinéa du I peuvent réaliser toute opération en ligne nécessaire à leur mission sous une identité d'emprunt. A peine de nullité, leurs actes ne peuvent constituer une incitation à commettre une infraction. L'utilisation d'une identité d'emprunt est sans incidence sur la régularité des constatations effectuées conformément au troisième alinéa du présent III. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, précise les conditions dans lesquelles ces membres et agents procèdent dans ces cas à leurs constatations.

Les membres et agents mentionnés au premier alinéa du I peuvent, à la demande du président de la commission, être assistés par des experts.

Il est dressé procès-verbal des vérifications et visites menées en application du présent article. Ce procès-verbal est dressé contradictoirement lorsque les vérifications et visites sont effectuées sur place ou sur convocation.

IV. Pour les traitements intéressant la sûreté de l'Etat et qui sont dispensés de la publication de l'acte réglementaire qui les autorise en application du III de l'article 31, le décret en Conseil d'Etat qui prévoit cette dispense peut également prévoir que le traitement n'est pas soumis aux dispositions du présent article.

V. Dans l'exercice de son pouvoir de contrôle portant sur les traitements relevant du règlement (UE) 2016/679 du 27 avril 2016 et de la présente loi, la Commission nationale de l'informatique et des libertés n'est pas compétente pour contrôler les opérations de traitement effectuées, dans l'exercice de leur fonction juridictionnelle, par les juridictions.

*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.*

## - **Article 31**

*Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 1*

I.- Sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et :

1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;

2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

L'avis de la commission est publié avec l'arrêté autorisant le traitement.

II.- Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 6 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission. Cet avis est publié avec le décret autorisant le traitement.

III.- Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise. Pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission.

IV.- Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

*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.*

- **Article 33**

*Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 1*

I. Les demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu de la présente loi précisent :

1° L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de l'Union européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ;

2° La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 31 et 32, la description générale de ses fonctions ;

3° Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;

4° Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;

5° La durée de conservation des informations traitées ;

6° Le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 31 et 32, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;

7° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;

8° La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu aux articles 49,105 et 119, ainsi que les mesures relatives à l'exercice de ce droit ;

9° Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ;

10° Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de l'Union européenne, sous quelque forme que ce soit.

Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum.

II. Le responsable d'un traitement déjà autorisé et susceptible de faire l'objet d'une mise à jour rendue publique dans les conditions prévues à l'article 36 informe sans délai la commission :

1° De tout changement affectant les informations mentionnées au I ;

2° De toute suppression du traitement.

*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.*

### **3. Décret n°2007-914 du 15 mai 2007 pris pour l'application du I de l'article 33 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**

#### **- Article 1**

*Modifié par Décret n°2021-697 du 31 mai 2021 - art. 2*

Relèvent des dispositions du dernier alinéa du I de l'article 33 de la loi du 6 janvier 1978 susvisée les traitements automatisés de données à caractère personnel intéressant la sûreté de l'Etat, la défense ou la sécurité publique autorisés par les actes réglementaires suivants :

1. Décret portant création au profit de la direction générale de la sécurité intérieure d'un traitement automatisé de données à caractère personnel dénommé CRISTINA ;
2. Décret portant application des dispositions de l'article 31 de la loi n° 78-17 du 6 janvier 1978 aux fichiers d'informations nominatives mis en œuvre par la direction générale de la sécurité extérieure ;
3. Décret autorisant la mise en œuvre par la direction du renseignement et de la sécurité de la défense d'un traitement automatisé de données à caractère personnel dénommé SIREX ;
4. Décret autorisant la mise en œuvre par la direction du renseignement militaire d'un traitement automatisé de données à caractère personnel dénommé " DOREMI " ;
5. Décret portant création au profit de la direction nationale du renseignement et des enquêtes douanières d'un traitement automatisé de données à caractère personnel dénommé BCR-DNRED ;
6. Arrêté relatif au traitement automatisé d'informations nominatives " fichier de la DGSE " mis en œuvre par la direction générale de la sécurité extérieure ;
7. Arrêté relatif au traitement automatisé d'informations nominatives " fichier du personnel de la DGSE " mis en œuvre par la direction générale de la sécurité extérieure ;
8. (Abrogé) ;
9. Décret portant création de l'application relative à la prévention des atteintes à la sécurité publique ;
10. Décret autorisant la mise en œuvre par le service à compétence nationale TRACFIN d'un traitement automatisé de données à caractère personnel dénommé " STARTRAC " ;
11. Décret autorisant la création d'un traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique ;
12. Décret portant création d'un traitement automatisé de données à caractère personnel dénommé FSPRT ;
13. Décret portant création d'un traitement automatisé de données à caractère personnel relatif au suivi des personnes placées sous-main de justice et destiné à la prévention des atteintes à la sécurité pénitentiaire et à la sécurité publique dénommé " CAR " mis en œuvre par la direction de l'administration pénitentiaire ;
14. Décret portant création d'un traitement automatisé de données à caractère personnel dénommé ASTREE mis en œuvre par la direction de la protection judiciaire de la jeunesse ;
15. Décret portant création d'un traitement automatisé de données à caractère personnel dénommé GESTEREXT ;
16. Décret autorisant la mise en œuvre par la direction du renseignement militaire d'un traitement automatisé de données à caractère personnel dénommé " BIOPEX " ;
17. Décret autorisant la mise en œuvre par le commandement de la Légion étrangère d'un traitement automatisé de données à caractère personnel dénommé " LEGATO ".

Les demandes d'avis portant sur les traitements énumérés au présent article comportent les mentions figurant à l'article 16 du décret du 20 octobre 2005 susvisé.

#### **4. Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.**

##### **- Article 1**

*Modifié par LOI n°2017-86 du 27 janvier 2017 - art. 152 (V)*

I. - Sont considérés comme autorités administratives au sens de la présente ordonnance les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du code du travail et les autres organismes chargés de la gestion d'un service public administratif ainsi que les commissions de coordination des actions de prévention des expulsions locatives prévues à l'article 7-2 de la loi n° 90-449 du 31 mai 1990 visant à la mise en œuvre du droit au logement.

II. - Sont considérés, au sens de la présente ordonnance :

1° Comme système d'information, tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives ;

2° Comme prestataire de services de confiance, toute personne offrant des services tendant à la mise en oeuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique ;

3° Comme produit de sécurité, tout dispositif, matériel ou logiciel, mettant en oeuvre des fonctions qui contribuent à la sécurité des informations échangées par voie électronique ;

4° Comme téléservice, tout système d'information permettant aux usagers de procéder par voie électronique à des démarches ou formalités administratives.

#### **5. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)**

##### **- Article 4 Définitions**

Aux fins du présent règlement, on entend par :

[...]

2) «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

[...]

## 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 fixe également les règles concernant :

- le régime électoral des assemblées parlementaires, des assemblées locales et des instances représentatives des Français établis hors de France ainsi que les conditions d'exercice des mandats électoraux et des fonctions électives des membres des assemblées délibérantes des collectivités territoriales ;
- la création de catégories d'établissements publics ;
- les garanties fondamentales accordées aux fonctionnaires civils et militaires de l'État ;
- les nationalisations d'entreprises et les transferts de propriété d'entreprises du secteur public au secteur privé.

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.

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.

Les lois de financement de la sécurité sociale déterminent les conditions générales de son équilibre financier et, compte tenu de leurs prévisions de recettes, fixent ses objectifs de dépenses, dans les conditions et sous les réserves prévues par une loi organique.

Des lois de programmation déterminent les objectifs de l'action de l'État.

Les orientations pluriannuelles des finances publiques sont définies par des lois de programmation. Elles s'inscrivent dans l'objectif d'équilibre des comptes des administrations publiques.

Les dispositions du présent article pourront être précisées et complétées par une loi organique.

## **B. Jurisprudence du Conseil constitutionnel**

### **Sur le droit au respect de la vie privée**

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

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**

39. Considérant qu'aux termes de l'article 9 de la Déclaration de 1789 : « Tout homme étant présumé innocent, jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimée par la loi » ;

40. Considérant, en premier lieu, que l'enregistrement de données nominatives dans des traitements de la nature de ceux auxquels fait référence l'article 21 de la loi déferée ne porte par lui-même aucune atteinte au principe de la présomption d'innocence ;

41. Considérant, en deuxième lieu, qu'en cas de décision de relaxe ou d'acquiescement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées ; que, si le procureur de la République peut en prescrire le maintien « pour des raisons liées à la finalité du fichier », cette exception à la règle générale d'effacement ne peut être justifiée que par des nécessités d'ordre public appréciées par l'autorité judiciaire ; qu'il est alors fait mention de la décision de relaxe ou d'acquiescement dans le fichier ;

42. Considérant, en troisième lieu, qu'en cas de décision de non lieu ou de classement sans suite, les données personnelles concernant les personnes mises en cause sont conservées sauf si le procureur de la République en ordonne l'effacement ; que, s'il ne le fait pas, les décisions de non lieu et, lorsqu'ils sont motivés par une insuffisance de charges, les classements sans suite font l'objet d'une mention dans le fichier ; qu'il appartiendra ainsi à l'autorité judiciaire d'apprécier dans chaque cas, compte tenu des motifs de la décision prise, si les nécessités de l'ordre public justifient ou non le maintien des données en cause ;

43. Considérant, enfin, ainsi qu'il a été dit ci-dessus, que toute personne inscrite dans le fichier devra pouvoir exercer son droit d'accès et de rectification des données la concernant dans les conditions prévues par l'article 39 de la loi du 6 janvier 1978 susvisée ;

- Quant au principe d'égalité :

44. Considérant qu'en vertu du II de l'article 21, la victime peut s'opposer au maintien dans le fichier des informations nominatives la concernant dès lors que l'auteur des faits a été définitivement condamné ; que les sénateurs requérants ne sauraient invoquer utilement, à l'encontre de cette disposition, une quelconque rupture du principe d'égalité ;

- Quant à la compétence du législateur :

45. Considérant que, loin d'avoir méconnu l'étendue de sa compétence, le législateur a assorti les dispositions critiquées de précisions dont certaines relèvent du pouvoir réglementaire et qui, au demeurant, avaient jusqu'ici été traitées comme telles ;

- **Décision n° 2004-492 DC du 2 mars 2004 - Loi portant adaptation de la justice aux évolutions de la criminalité**

74. Considérant que l'inscription de l'identité d'une personne dans le fichier judiciaire national automatisé des auteurs des infractions sexuelles mentionnées à l'article 706-47 rétabli dans le code de procédure pénale par l'article 47 de la loi déferée a pour objet, aux termes de l'article 706-53-1 inséré dans le même code par l'article 48 de la même loi, de prévenir le renouvellement de ces infractions et de faciliter l'identification de leurs auteurs ; qu'il en résulte que cette inscription ne constitue pas une sanction mais une mesure de police ; que les auteurs des saisines ne sauraient dès lors utilement soutenir qu'elle méconnaîtrait le principe de nécessité des peines qui résulte de l'article 8 de la Déclaration de 1789 ; qu'il convient toutefois de vérifier si cette inscription constitue une rigueur non nécessaire au sens de l'article 9 de la Déclaration ;

75. Considérant que la liberté proclamée par l'article 2 de la Déclaration de 1789 implique le respect de la vie privée ;

76. Considérant qu'il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il lui appartient notamment 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 ;

- **Décision n° 2004-499 DC du 29 juillet 2004 - Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés**

11. Considérant que le 3° de l'article 9 de la loi du 6 janvier 1978, dans la rédaction que lui donne l'article 2 de la loi déferée, permettrait à une personne morale de droit privé, mandatée par plusieurs autres personnes morales estimant avoir été victimes ou être susceptibles d'être victimes d'agissements passibles de sanctions pénales, de rassembler un grand nombre d'informations nominatives portant sur des infractions, condamnations et mesures de sûreté ; qu'en raison de l'ampleur que pourraient revêtir les traitements de données personnelles ainsi mis en oeuvre et de la nature des informations traitées, le 3° du nouvel article 9 de la loi du 6 janvier 1978 pourrait affecter, par ses conséquences, le droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour

l'exercice des libertés publiques ; que la disposition critiquée doit dès lors comporter les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution ;

12. Considérant que, s'agissant de l'objet et des conditions du mandat en cause, la disposition critiquée n'apporte pas ces précisions ; qu'elle est ambiguë quant aux infractions auxquelles s'applique le terme de « fraude » ; qu'elle laisse indéterminée la question de savoir dans quelle mesure les données traitées pourraient être partagées ou cédées, ou encore si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles soient capables de commettre une infraction ; qu'elle ne dit rien sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux condamnations ; qu'au regard de l'article 34 de la Constitution, toutes ces précisions ne sauraient être apportées par les seules autorisations délivrées par la Commission nationale de l'informatique et des libertés ; qu'en l'espèce et eu égard à la matière concernée, le législateur ne pouvait pas non plus se contenter, ainsi que le prévoit la disposition critiquée éclairée par les débats parlementaires, de poser une règle de principe et d'en renvoyer intégralement les modalités d'application à des lois futures ; que, par suite, le 3<sup>o</sup> du nouvel article 9 de la loi du 6 janvier 1978 est entaché d'incompétence négative ;

- **Décision n° 2007-553 DC du 3 mars 2007 - Loi relative à la prévention de la délinquance**

3. Considérant que, selon les requérants, ces dispositions méconnaissent le droit à la vie privée et sont entachées d'incompétence négative ;

4. Considérant 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 ; qu'aux termes des dixième et onzième alinéas du Préambule de la Constitution de 1946 : « La Nation assure à l'individu et à la famille les conditions nécessaires à leur développement. - Elle garantit à tous, notamment à l'enfant, à la mère et aux vieux travailleurs, la protection de la santé, la sécurité matérielle, le repos et les loisirs. Tout être humain qui, en raison de son âge, de son état physique ou mental, de la situation économique, se trouve dans l'incapacité de travailler a le droit d'obtenir de la collectivité des moyens convenables d'existence » ;

5. Considérant qu'il appartient au législateur d'assurer la conciliation entre, d'une part, l'exercice des libertés constitutionnellement garanties, au nombre desquelles figure le droit au respect de la vie privée et, d'autre part, les exigences de solidarité découlant des dixième et onzième alinéas du Préambule de 1946 ;

6. Considérant que c'est afin de mieux prendre en compte l'ensemble des difficultés sociales, éducatives ou matérielles d'une personne ou d'une famille et de renforcer l'efficacité de l'action sociale, à laquelle concourt une coordination accrue des différents intervenants, que le législateur a prévu, dans certaines hypothèses, de délier ces derniers du secret professionnel ; qu'il a précisé que, si l'un d'eux agit seul auprès d'une personne ou d'une famille, il ne doit donner d'informations au maire de la commune ou au président du conseil général que « lorsque l'aggravation des difficultés sociales, éducatives ou matérielles » de cette personne ou de cette famille « appelle l'intervention de plusieurs professionnels » ; qu'il n'a autorisé les professionnels qui agissent auprès d'une personne ou d'une même famille, ainsi que le coordonnateur éventuellement désigné parmi eux par le maire, « à partager entre eux des informations à caractère secret » qu'« afin d'évaluer leur situation, de déterminer les mesures d'action sociale nécessaires et de les mettre en oeuvre » et seulement dans la mesure « strictement nécessaire à l'accomplissement de la mission d'action sociale » ; qu'il n'a permis à un professionnel, agissant seul ou en tant que coordonnateur, de délivrer ces informations confidentielles au maire ou au président du conseil général, qui disposent déjà, à d'autres titres, d'informations de cette nature, que si elles sont strictement nécessaires à l'exercice des compétences de ceux-ci ; qu'il a, enfin, précisé que la communication de telles informations à des tiers est passible des peines prévues à l'article 226-13 du code pénal ;

7. Considérant que le législateur a ainsi assorti les échanges d'informations qu'il a autorisés de limitations et précautions propres à assurer la conciliation qui lui incombe entre, d'une part, le droit au respect de la vie privée et, d'autre part, les exigences de solidarité découlant des dixième et onzième alinéas du Préambule de 1946 ; que, ce faisant, il n'a, en outre, pas méconnu l'étendue de sa compétence ;

- **Décision n° 2010-604 DC du 25 février 2010 - Loi renforçant la lutte contre les violences de groupes et la protection des personnes chargées d'une mission de service public**

19. Considérant que l'article 5 de la loi déferée insère dans le code de la construction et de l'habitation un article L. 126-1-1 qui dispose : « Lorsque des événements ou des situations susceptibles de nécessiter l'intervention des services de la police ou de la gendarmerie nationales ou, le cas échéant, des agents de la police municipale se produisent dans les parties communes des immeubles collectifs à usage d'habitation, les propriétaires ou exploitants de ces immeubles ou leurs représentants peuvent rendre ces services ou ces agents destinataires des

images des systèmes de vidéosurveillance qu'ils mettent en œuvre dans ces parties communes. » La transmission de ces images relève de la seule initiative des propriétaires ou exploitants d'immeubles collectifs d'habitation ou de leurs représentants. Elle s'effectue en temps réel et est strictement limitée au temps nécessaire à l'intervention des services de police ou de gendarmerie nationales ou, le cas échéant, des agents de la police municipale. « Un décret en Conseil d'État précise les modalités d'application du présent article » ;

20. Considérant que, selon les sénateurs requérants, en permettant en des circonstances imprécises la mise à disposition de services de police et de gendarmerie de l'enregistrement d'images effectué dans des lieux privés, le législateur est resté en deçà de sa compétence ; que, de ce fait, il aurait porté une atteinte disproportionnée et non justifiée par la nécessité de sauvegarde de l'ordre public aux exigences dues au respect de la vie privée ; qu'ils ajoutent que le législateur a manqué aux mêmes exigences en conférant à la police municipale la possibilité d'être destinataire d'images se rapportant à des faits n'entrant pas dans ses compétences ;

21. Considérant, en premier lieu, qu'aux termes de l'article 2 de la Déclaration 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 » ; que la liberté proclamée par cet article implique le respect de la vie privée ;

22. Considérant, en second lieu, qu'il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il doit, en particulier, assurer la conciliation entre le respect de la vie privée et d'autres exigences constitutionnelles, telles que la recherche des auteurs d'infractions et la prévention d'atteintes à l'ordre public, nécessaires, l'une et l'autre, à la sauvegarde de droits et principes de valeur constitutionnelle ;

23. Considérant que le législateur a permis la transmission aux services de police et de gendarmerie nationales ainsi qu'à la police municipale d'images captées par des systèmes de vidéosurveillance dans des parties non ouvertes au public d'immeubles d'habitation sans prévoir les garanties nécessaires à la protection de la vie privée des personnes qui résident ou se rendent dans ces immeubles ; qu'à l'égard de cette situation, qui n'entre pas dans le champ d'application de l'article 10 de la loi du 21 janvier 1995 susvisée, il a omis d'opérer entre les exigences constitutionnelles précitées la conciliation qui lui incombe ; que, dès lors, il a méconnu l'étendue de sa compétence ; qu'en conséquence, l'article 5 de la loi déferée doit être déclaré contraire à la Constitution ;

- **Décision n° 2011-209 QPC du 17 janvier 2012 - M. Jean-Claude G. [Procédure de dessaisissement d'armes]**

3. Considérant qu'il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il doit, en particulier, assurer la conciliation entre le respect de la vie privée et d'autres exigences constitutionnelles, telles que la recherche des auteurs d'infractions et la prévention d'atteintes à l'ordre public, nécessaires, l'une et l'autre, à la sauvegarde de droits et principes de valeur constitutionnelle ;

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

2. Considérant que l'article 5 de la loi déferée prévoit la création, dans les conditions prévues par la loi du 6 janvier 1978 susvisée, d'un traitement de données à caractère personnel facilitant le recueil et la conservation des données requises pour la délivrance du passeport français et de la carte nationale d'identité, destiné à préserver l'intégrité de ces données ; que, parmi celles-ci, figurent les données contenues dans le composant électronique sécurisé de la carte nationale d'identité et du passeport dont la liste est fixée à l'article 2 de la loi, qui sont, outre l'état civil et le domicile du titulaire, sa taille, la couleur de ses yeux, deux empreintes digitales et sa photographie ;

3. Considérant que cet article 5 permet que l'identification du demandeur d'un titre d'identité ou de voyage s'effectue en interrogeant le traitement de données à caractère personnel au moyen des données dont la liste est fixée à l'article 2, à l'exception de la photographie ; qu'il prévoit également que ce traitement de données à caractère personnel peut être interrogé au moyen des deux empreintes digitales recueillies dans le traitement, en premier lieu, lors de l'établissement des titres d'identité et de voyage, en deuxième lieu, pour les besoins de l'enquête relative à certaines infractions, sur autorisation du procureur de la République ou du juge d'instruction, et, en troisième lieu, sur réquisition du procureur de la République aux fins d'établir, lorsqu'elle est inconnue, l'identité d'une personne décédée, victime d'une catastrophe naturelle ou d'un accident collectif ;

4. Considérant que l'article 6 de la loi déferée permet de vérifier l'identité du possesseur de la carte d'identité ou du passeport à partir des données inscrites sur le document d'identité ou de voyage ou sur le composant électronique sécurisé ; qu'il permet également que cette vérification soit effectuée en consultant les données

conservées dans le traitement prévu à l'article 5 « en cas de doute sérieux sur l'identité de la personne ou lorsque le titre présenté est défectueux ou paraît endommagé ou altéré » ;

5. Considérant que l'article 10 permet aux agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales d'avoir accès au traitement de données à caractère personnel créé en application de l'article 5, pour les besoins de la prévention et de la répression des atteintes à l'indépendance de la Nation, à l'intégrité de son territoire, à sa sécurité, à la forme républicaine de ses institutions, aux moyens de sa défense et de sa diplomatie, à la sauvegarde de sa population en France et à l'étranger et aux éléments essentiels de son potentiel scientifique et économique et des actes de terrorisme ;

6. Considérant que, selon les requérants, la création d'un fichier d'identité biométrique portant sur la quasi-totalité de la population française et dont les caractéristiques rendent possible l'identification d'une personne à partir de ses empreintes digitales porte une atteinte inconstitutionnelle au droit au respect de la vie privée ; qu'en outre, en permettant que les données enregistrées dans ce fichier soient consultées à des fins de police administrative ou judiciaire, le législateur aurait omis d'adopter les garanties légales contre le risque d'arbitraire ;

7. Considérant, en premier lieu, que l'article 34 de la Constitution dispose que la loi fixe les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ainsi que la procédure pénale ; qu'il appartient au législateur, dans le cadre de sa compétence, 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 des autres droits et libertés constitutionnellement protégés ; qu'il lui est à tout moment loisible d'adopter des dispositions nouvelles dont il lui appartient d'apprécier l'opportunité et de modifier des textes antérieurs ou d'abroger ceux-ci en leur substituant, le cas échéant, d'autres dispositions, dès lors que, dans l'exercice de ce pouvoir, il ne prive pas de garanties légales des exigences constitutionnelles ;

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 déferée 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'en 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**

10. Considérant, en premier lieu, que l'article 34 de la Constitution dispose que la loi fixe les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; qu'il incombe au législateur, dans le cadre de sa compétence, d'assurer la conciliation entre, d'une part, la lutte contre la fraude fiscale, qui constitue un objectif de valeur constitutionnelle, et, d'autre part, le respect des autres droits et libertés constitutionnellement protégés, au nombre desquels figure le droit au respect de la vie privée qui découle de l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 ; que, dans l'exercice de son pouvoir, le législateur ne saurait priver de garanties légales des exigences constitutionnelles ;

11. Considérant qu'il ressort des débats parlementaires qu'en renforçant les obligations déclaratives en matière d'assurance-vie et en permettant que soit mis en place un fichier national des contrats d'assurance-vie, le législateur

a entendu favoriser la connaissance par l'administration de ces contrats afin de mieux prendre en compte la matière imposable et de faciliter la lutte contre la fraude fiscale ; qu'il a poursuivi un but d'intérêt général ;

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 1<sup>er</sup> 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 œuvre 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 œuvre 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° 2015-713 DC du 23 juillet 2015 - Loi relative au renseignement**

7. Considérant que l'article L. 811-3 du code de la sécurité intérieure énumère les finalités pour lesquelles les services spécialisés de renseignement peuvent recourir aux techniques définies aux articles L. 851-1 à L. 854-1 du même code tels qu'ils résultent des articles 5 et 6 de la loi déferée, pour le seul exercice de leurs missions respectives, afin de recueillir des renseignements ; que ces finalités correspondent à « la défense et 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 » ;

8. Considérant que les députés requérants font valoir que les finalités énumérées par le législateur sont trop larges, au regard des techniques de recueil de renseignement prévues par la loi déferée, et insuffisamment définies ; qu'il en résulterait une atteinte disproportionnée au droit au respect de la vie privée ainsi qu'à la liberté d'expression ;

9. Considérant que le recueil de renseignement au moyen des techniques définies au titre V du livre VIII du code de la sécurité intérieure par les services spécialisés de renseignement pour l'exercice de leurs missions respectives relève de la seule police administrative ; qu'il ne peut donc avoir d'autre but que de préserver l'ordre public et de prévenir les infractions ; qu'il ne peut être mis en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs ;

10. Considérant qu'en retenant, pour déterminer les finalités énumérées aux 1 ° à 4 °, des définitions faisant référence à certains des intérêts mentionnés à l'article 410-1 du code pénal, le législateur a précisément circonscrit les finalités ainsi poursuivies et n'a pas retenu des critères en inadéquation avec l'objectif poursuivi par ces mesures de police administrative ; qu'il en va de même pour les finalités définies au a) du 5 °, faisant référence aux incriminations pénales du chapitre II du titre I<sup>er</sup> du livre IV du code pénal, de celles définies au b) du 5 °, faisant

référence aux dispositions de l'article L. 212-1 du code de la sécurité intérieure, de celles définies au c) du 5 °, faisant référence aux incriminations pénales définies aux articles 431-1 à 431-10 du code pénal, de celles définies au 6 °, faisant référence aux incriminations pénales énumérées à l'article 706-73 du code de procédure pénale et aux délits punis par l'article 414 du code des douanes commis en bande organisée et de celles définies au 7 °, faisant référence aux incriminations pénales définies aux articles L. 2339-14 à L. 2339-18 du code de la défense ;

11. Considérant que les dispositions de l'article L. 811-3 doivent être combinées avec celles de l'article L. 801-1, dans sa rédaction résultant de l'article 1<sup>er</sup> de la loi déferée, aux termes desquelles la décision de recourir aux techniques de renseignement et les techniques choisies devront être proportionnées à la finalité poursuivie et aux motifs invoqués ; qu'il en résulte que les atteintes au droit au respect de la vie privée doivent être proportionnées à l'objectif poursuivi ; que la commission nationale de contrôle des techniques de renseignement et le Conseil d'État sont chargés de s'assurer du respect de cette exigence de proportionnalité ;

12. Considérant qu'il résulte de ce qui précède que les dispositions de l'article L. 811-3 du code de la sécurité intérieure doivent être déclarées conformes à la Constitution ;

[...]

76. Considérant que le paragraphe I de l'article L. 854-1 du code de la sécurité intérieure autorise, aux seules fins de protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code, la surveillance des communications émises ou reçues à l'étranger ; que le deuxième alinéa de ce paragraphe prévoit les mentions que les autorisations de surveillance délivrées en application de cet article devront comporter ; que le troisième alinéa de ce paragraphe indique que ces autorisations seront délivrées sur demande motivée des ministres mentionnés au premier alinéa de l'article L. 821-2 du même code pour une durée de quatre mois renouvelable ; que le quatrième alinéa de ce paragraphe dispose qu'un décret en Conseil d'État, pris après avis de la commission nationale de contrôle des techniques de renseignement, définit les conditions d'exploitation, de conservation et de destruction des renseignements collectés, ainsi que les conditions de traçabilité et de contrôle par la commission de la mise en œuvre des mesures de surveillance ; que le cinquième alinéa prévoit qu'un décret en Conseil d'État non publié pris après avis de ladite commission et porté à la connaissance de la délégation parlementaire au renseignement précise, en tant que de besoin, les modalités de mise en œuvre de ces mesures de surveillance ;

77. Considérant que les députés requérants soutiennent que ces dispositions méconnaissent le droit au respect de la vie privée ;

78. Considérant qu'en ne définissant dans la loi ni les conditions d'exploitation, de conservation et de destruction des renseignements collectés en application de l'article L. 854-1, ni celles du contrôle par la commission nationale de contrôle des techniques de renseignement de la légalité des autorisations délivrées en application de ce même article et de leurs conditions de mise en œuvre, le législateur n'a pas déterminé les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; que, par suite, les dispositions du paragraphe I de l'article L. 854-1, qui méconnaissent l'article 34 de la Constitution, doivent être déclarés contraires à la Constitution ;

79. Considérant qu'il en va de même, par voie de conséquence, des paragraphes II et III du même article L. 854-1, qui en sont inséparables ; qu'il y a également lieu, par voie de conséquence, de déclarer contraires à la Constitution les mots : « , à l'exception de ceux mentionnés à l'article L. 854-1 » figurant au troisième alinéa de l'article L. 833-2 du code de la sécurité intérieure dans sa rédaction résultant de l'article 2 de la loi, les mots : « Sous réserve des dispositions particulières prévues à l'article L. 854-1 du présent code, » figurant au premier alinéa de l'article L. 841-1 du code de la sécurité intérieure dans sa rédaction résultant de l'article 2 de la loi, les mots : « et de l'article L. 854-1 du code de la sécurité intérieure » figurant à l'article L. 773-1 du code de justice administrative dans sa rédaction résultant de l'article 10 de la loi ainsi que le paragraphe IV de l'article 26 de la loi ;

- **Décision n° 2015-715 DC du 5 août 2015 - Loi pour la croissance, l'activité et l'égalité des chances économiques**

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<sup>o</sup> 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<sup>o</sup> 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<sup>o</sup> de l'article 216 est contraire à la Constitution ;

- **Décision n° 2015-722 DC du 26 novembre 2015 - Loi relative aux mesures de surveillance des communications électroniques internationales**

6. Considérant que l'article L. 854-1 autorise la surveillance des communications qui sont émises ou reçues à l'étranger et délimite le champ de celles de ces communications qui sont susceptibles de faire l'objet de mesures de surveillance dans les conditions prévues par les autres dispositions du chapitre IV du titre V du livre VIII du code de la sécurité intérieure ; que cet article prévoit que les mesures prises à ce titre ne peuvent avoir pour objet d'assurer la surveillance individuelle des communications de personnes utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, à l'exception du cas où ces personnes communiquent depuis l'étranger et, soit faisaient l'objet d'une autorisation d'interception de sécurité délivrée en application de l'article L. 852-1, soit sont identifiées comme présentant une menace au regard des intérêts fondamentaux de la Nation ; qu'hormis ces hypothèses, les communications électroniques qui sont échangées entre des personnes ou des équipements utilisant des numéros d'abonnement ou des identifiants techniques rattachables au territoire national, lorsqu'elles sont interceptées au moyen des mesures de surveillance prévues par le chapitre IV susmentionné, sont instantanément détruites ;

7. Considérant que l'article L. 854-2 détermine la procédure d'autorisation de mise en œuvre des mesures de surveillance des communications électroniques internationales ; que son paragraphe I fixe les conditions dans lesquelles l'interception des communications émises ou reçues à l'étranger est autorisée ; que son paragraphe II prévoit les conditions dans lesquelles les données de connexion ainsi interceptées peuvent faire l'objet d'une exploitation non individualisée ; que son paragraphe III détermine les conditions dans lesquelles les communications et les données de connexion ainsi interceptées peuvent être exploitées, y compris de manière individualisée ;

8. Considérant que l'article L. 854-5 fixe les durées maximales de conservation des renseignements collectés par la mise en œuvre des mesures de surveillance des communications électroniques internationales, exception faite des correspondances interceptées qui renvoient à des numéros d'abonnement ou à des identifiants techniques rattachables au territoire national ; que ces durées sont d'un an à compter de leur première exploitation, dans la limite de quatre ans à compter de leur recueil pour les correspondances interceptées, de six ans à compter de leur recueil pour les données de connexion et de huit ans à compter de leur recueil pour les renseignements chiffrés ;

9. Considérant que les premier à troisième et le sixième alinéas de l'article L. 854-9 sont relatifs aux pouvoirs dont dispose la commission nationale de contrôle des techniques de renseignement pour vérifier si les mesures de surveillance internationale sont régulièrement mises en œuvre ;

10. Considérant, en premier lieu, que le recueil de renseignement au moyen des mesures de surveillance prévues au chapitre IV du titre V du livre VIII du code de la sécurité intérieure par les services spécialisés de renseignement pour l'exercice de leurs missions respectives relève de la seule police administrative ; qu'il ne peut donc avoir d'autre but que de préserver l'ordre public et de prévenir les infractions ; qu'il ne peut être mis en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs ;

11. Considérant, en deuxième lieu, que l'article L. 854-1 permet la surveillance « aux seules fins de défense et de promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 » ; qu'ainsi, le législateur a précisément circonscrit les finalités permettant de recourir au régime d'autorisation des mesures de surveillance des communications émises ou reçues à l'étranger prévu par l'article L. 854-1 et n'a pas retenu des critères en inadéquation avec l'objectif poursuivi par ces mesures de police administrative ;

12. Considérant, en troisième lieu, que l'autorisation d'intercepter des communications électroniques émises ou reçues à l'étranger est délivrée par le Premier ministre et désigne les réseaux de communication sur lesquels les interceptions sont admises ; que l'autorisation d'exploiter ces interceptions est délivrée par le Premier ministre ou par l'un de ses délégués sur demande motivée des ministres de la défense, de l'intérieur ou chargés de l'économie, du budget ou des douanes ou de leurs délégués ; que cette exploitation est réalisée par un service spécialisé de renseignement ; que les autorisations d'interception ou d'exploitation sont délivrées pour une durée limitée ; que l'autorisation d'exploiter de manière non individualisée les données de connexion interceptées précise le type de traitements automatisés pouvant être mis en œuvre ;

13. Considérant, en quatrième lieu, que le législateur a prévu des durées de conservation en fonction des caractéristiques des renseignements collectés ainsi qu'une durée maximale de conservation de huit ans à compter du recueil des renseignements chiffrés, au-delà desquelles les renseignements collectés doivent être détruits ; qu'en outre, en vertu de l'article L. 854-6, les transcriptions ou extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite des finalités mentionnées à l'article L. 811-3 ;

14. Considérant, en cinquième lieu, que le législateur a prévu que la commission nationale de contrôle des techniques de renseignement reçoit communication de toutes les décisions et autorisations du Premier ministre mentionnées à l'article L. 854-2 et qu'elle dispose d'un accès permanent, complet et direct aux dispositifs de

traçabilité, aux renseignements collectés, aux transcriptions et extractions réalisées ainsi qu'aux relevés mentionnés au quatrième alinéa de l'article L. 854-6 retraçant les opérations de destruction, de transcription et d'extraction ; que la commission peut solliciter du Premier ministre tous les éléments nécessaires à l'accomplissement de sa mission ; que sont applicables aux contrôles pratiqués par la commission sur les mesures de surveillance internationale les dispositions de l'article L. 833-3 qui réprime de peines délictuelles les actes d'entrave à l'action de la commission ;

15. Considérant qu'il résulte de tout ce qui précède que les dispositions des articles L. 854-1, L. 854-2, L. 854-5 et des premier à troisième et sixième alinéas de l'article L. 854-9 ne portent pas d'atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances ; que le législateur a précisément défini les conditions de mise en œuvre de mesures de surveillance des communications électroniques internationales, celles d'exploitation, de conservation et de destruction des renseignements collectés ainsi que celles du contrôle exercé par la commission nationale de contrôle des techniques de renseignement ; que ces dispositions doivent être déclarées conformes à la Constitution ;

- **Décision n° 2016-569 QPC du 23 septembre 2016 - Syndicat de la magistrature et autre [Transaction pénale par officier de police judiciaire - Participation des conseils départementaux de prévention de la délinquance et des zones de sécurité prioritaires à l'exécution des peines]**

24. En second lieu, selon l'article 2 de la Déclaration 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. Les échanges d'informations entre, d'une part, l'état-major de sécurité et la cellule de coordination opérationnelle des forces de sécurité intérieure et, d'autre part, les juridictions de l'application des peines et le service pénitentiaire d'insertion et de probation, sont susceptibles de porter atteinte à ce droit. Pour être conformes à la Constitution, ces atteintes doivent être justifiées par un motif d'intérêt général et mises en œuvre de manière adéquate et proportionnée à cet objectif.

25. En prévoyant ces échanges d'informations, le législateur a entendu, en améliorant le suivi et le contrôle des personnes condamnées, favoriser l'exécution des peines et prévenir la récidive. Il a ainsi poursuivi un objectif d'intérêt général.

26. Toutefois, le législateur a prévu que puisse être transmise à l'état-major de sécurité et à la cellule de coordination opérationnelle des forces de sécurité intérieure « toute information » que les juridictions de l'application des peines et le service pénitentiaire d'insertion et de probation « jugent utile » au bon déroulement du suivi et du contrôle des personnes condamnées, sans définir la nature des informations concernées, ni limiter leur champ. Ce faisant, même s'il s'agissait d'améliorer le suivi et le contrôle des personnes condamnées, de favoriser l'exécution des peines et de prévenir la récidive, le législateur a porté une atteinte disproportionnée au droit au respect de la vie privée.

- **Décision n° 2016-590 QPC du 21 octobre 2016 - La Quadrature du Net et autres [Surveillance et contrôle des transmissions empruntant la voie hertzienne]**

3. Selon 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 et le secret des correspondances. Pour être conformes à la Constitution, les atteintes à ce droit doivent être justifiées par un motif d'intérêt général et mises en œuvre de manière adéquate et proportionnée à cet objectif.

4. Les dispositions contestées permettent aux pouvoirs publics de prendre, à des fins de défense des intérêts nationaux, des mesures de surveillance et de contrôle des transmissions empruntant la voie hertzienne. Selon l'article L. 871-2 du code de la sécurité intérieure, pour l'exécution de ces mesures, le ministre de la défense ou le ministre de l'intérieur peuvent requérir, auprès des personnes physiques ou morales exploitant des réseaux de communications électroniques ou fournisseurs de services de communications électroniques, les informations ou documents qui leur sont nécessaires pour la réalisation et l'exploitation des interceptions autorisées par la loi.

5. Les mesures de surveillance et de contrôle autorisées par les dispositions contestées ne sont pas soumises aux dispositions relatives au renseignement figurant au livre VIII du code de la sécurité intérieure, qui définit les techniques de recueil de renseignement soumises à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement, et qui détermine les voies de recours

relatives à la mise en œuvre de ces techniques. Ces mesures ne sont pas non plus soumises aux dispositions de la sous-section 2 de la section 3 du chapitre I<sup>er</sup> du titre III du livre I<sup>er</sup> du code de procédure pénale, qui encadrent les interceptions de correspondances émises par la voie de communications électroniques prescrites par un juge d'instruction.

6. En premier lieu, dès lors qu'elles permettent aux pouvoirs publics de prendre des mesures de surveillance et de contrôle de toute transmission empruntant la voie hertzienne, sans exclure que puissent être interceptées des communications ou recueillies des données individualisables, les dispositions contestées portent atteinte au droit au respect de la vie privée et au secret des correspondances.

7. En deuxième lieu, en prévoyant que les mesures de surveillance et de contrôle peuvent être prises aux seules fins de défense des intérêts nationaux, les dispositions contestées mettent en œuvre les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation. Toutefois, elles n'interdisent pas que ces mesures puissent être utilisées à des fins plus larges que la seule mise en œuvre de ces exigences.

8. En dernier lieu, les dispositions contestées ne définissent pas la nature des mesures de surveillance et de contrôle que les pouvoirs publics sont autorisés à prendre. Elles ne soumettent le recours à ces mesures à aucune condition de fond ni de procédure et n'encadrent leur mise en œuvre d'aucune garantie.

9. Il résulte de ce qui précède que, faute de garanties appropriées, les dispositions contestées portent une atteinte manifestement disproportionnée au droit au respect de la vie privée et au secret des correspondances résultant de l'article 2 de la Déclaration de 1789. Par conséquent et sans qu'il soit besoin d'examiner les autres griefs, l'article L. 811-5 du code de la sécurité intérieure doit être déclaré 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° 2019-789 QPC du 14 juin 2019 - Mme Hanen S. [Droit de communication des organismes de 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° 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 répétition 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.

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

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.

- **Décision n° 2020-841 QPC du 20 mai 2020 - La Quadrature du Net et autres [Droit de communication à la Hadopi]**

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° 2020-808 DC du 13 novembre 2020 - Loi autorisant la prorogation de l'état d'urgence sanitaire et portant diverses mesures de gestion de la crise sanitaire**

16. L'article 5 modifie l'article 11 de la loi du 11 mai 2020 mentionnée ci-dessus qui organise les conditions dans lesquelles les données relatives à la santé des personnes atteintes par le virus responsable de la covid-19 et des personnes en contact avec elles sont, le cas échéant sans leur consentement, traitées et partagées à travers un système d'information ad hoc.

17. Les députés requérants font valoir que cet article 5 méconnaîtrait le droit au respect de la vie privée au motif qu'il prolonge le traitement et le partage de ces données jusqu'au 1<sup>er</sup> avril 2021 et qu'il élargit le champ des personnes y ayant accès.

18. 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. 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.

19. L'article 5 modifie le paragraphe I de l'article 11 de la loi du 11 mai 2020 afin de prévoir que le traitement et le partage des données à caractère personnel prévus par cet article 11 ne peuvent être mis en œuvre au plus tard que jusqu'au 1<sup>er</sup> avril 2021. Il modifie également le paragraphe III du même article 11 afin de donner accès à ces données à certains professionnels de santé et de prévoir qu'elles peuvent être communiquées aux organismes qui assurent l'accompagnement social des personnes infectées ou susceptibles de l'être pendant et après la fin des prescriptions médicales et d'isolement prophylactiques.

20. En premier lieu, par la décision du 11 mai 2020 mentionnée ci-dessus, le Conseil constitutionnel a, pour les motifs énoncés aux paragraphes 63 à 78 et sous les réserves énoncées aux paragraphes 67, 73 et 74 de cette décision, jugé conforme à la Constitution le système d'information prévu par l'article 11 de la loi du 11 mai 2020. En particulier, comme le Conseil constitutionnel l'a jugé au paragraphe 63 de sa décision, en adoptant l'article 11 de la loi du 11 mai 2020, le législateur a entendu renforcer les moyens de 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. Comme il ressort des paragraphes 66 à 67 de cette même décision, les données à caractère personnel qui font l'objet du système de traitement et de partage prévu par cet article 11 sont les seules données strictement nécessaires à la poursuite des finalités propres à ce système.

21. En deuxième lieu, d'une part, en ouvrant l'accès à ces données aux professionnels de santé figurant sur une liste prévue par décret et habilités à la réalisation des examens de dépistage virologique ou sérologique, le législateur a visé les personnels qui participent à l'établissement du diagnostic et à l'identification des chaînes de contamination. De plus, il résulte des dispositions du paragraphe III de l'article 11 que ces professionnels ne peuvent avoir accès qu'aux seules données nécessaires à leur intervention et dans la stricte mesure où leur intervention sert les finalités poursuivies par le système d'information.

22. D'autre part, si les dispositions contestées prévoient que les organismes qui assurent l'accompagnement social des personnes infectées ou susceptibles de l'être peuvent recevoir les données contenues dans ce système, cette communication est subordonnée au recueil préalable du consentement des intéressés. En outre, cette communication ne peut porter que sur les données strictement nécessaires à l'exercice de la mission de ces organismes.

23. Enfin, le législateur, qui a estimé qu'un risque important de propagation de l'épidémie persistait jusqu'au 1<sup>er</sup> avril 2021, a prévu que le dispositif instauré à l'article 11 de la loi du 11 mai 2020 pourra être appliqué au plus tard jusqu'à cette date. Pour les motifs précédemment mentionnés, cette appréciation n'est pas, en l'état des connaissances, manifestement inadéquate au regard de la situation présente.

24. Il résulte de tout ce qui précède que, sous les mêmes réserves que celles énoncées aux paragraphes 73 et 74 de la décision du 11 mai 2020, les dispositions contestées ne méconnaissent pas le droit au respect de la vie privée.

- **Décision n° 2021-817 DC du 20 mai 2021 - Loi pour une sécurité globale préservant les libertés**

83. L'article 41 autorise le placement sous vidéosurveillance des personnes retenues dans les chambres d'isolement des centres de rétention administrative et des personnes en garde à vue, sous certaines conditions et pour certaines finalités.

84. Selon les députés requérants, ces dispositions méconnaîtraient le droit au respect de la vie privée au motif qu'elles ne sont ni nécessaires ni proportionnées aux risques d'évasion ou d'atteinte aux personnes qu'elles sont censées prévenir.

85. Les sénateurs requérants soutiennent que, outre le droit au respect de la vie privée, ces dispositions méconnaîtraient également l'exigence de protection de la liberté individuelle par l'autorité judiciaire. Ils critiquent, d'une part, le caractère permanent du contrôle par vidéosurveillance auquel pourront être soumises les personnes retenues à l'isolement ou placées en garde à vue, l'absence de prise en compte de la gravité des faits reprochés à ces dernières et la portée générale des finalités poursuivies. D'autre part, ils considèrent que cette surveillance constituerait une mesure privative de la liberté individuelle qui ne pourrait donc être prise par le chef de service responsable de la sécurité des lieux.

86. En premier lieu, les dispositions contestées permettent au chef du service responsable de la sécurité des lieux de décider du placement sous vidéosurveillance d'une personne retenue ou placée en garde à vue dès lors qu'il existe des motifs raisonnables de penser qu'elle pourrait tenter de s'évader ou qu'elle représenterait une menace pour elle-même ou pour autrui. Par ailleurs, le traitement des images ainsi recueillies peut avoir pour finalité la collecte de preuves.

87. En second lieu, cette décision de placement sous vidéosurveillance est prise pour une durée de quarante-huit heures. Elle peut être renouvelée sur la seule décision du chef de service responsable de la sécurité des lieux, et sous l'unique condition d'en informer le procureur de la République, aussi longtemps que dure la garde à vue ou

le placement en chambre d'isolement dans un centre de rétention administrative. Or, la durée d'une garde à vue peut atteindre six jours et la durée du placement d'une personne en chambre d'isolement dans un centre de rétention administrative n'est pas limitée dans le temps.

88. Il résulte de ce qui précède que, par les dispositions contestées, le législateur n'a pas assuré une conciliation équilibrée entre, d'une part, les objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions, et d'autre part, le droit au respect de la vie privée. Dès lors, l'article 41 méconnaît le droit au respect de la vie privée. Sans qu'il soit besoin d'examiner les autres griefs, il est donc contraire à la Constitution.

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

22. Le 1<sup>o</sup> du paragraphe I de l'article 7 de la loi déferée 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 I<sup>er</sup> 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<sup>o</sup> 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<sup>o</sup> 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 déferée 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 déferée.

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.