Décision n° 2017-648 QPC

Accès administratif en temps réel aux données de connexion

Dossier documentaire

Sommaire

Table des matières

I. Dispositions législatives

A. Dispositions contestées

1. Code de la sécurité intérieure

LIVRE VIII : DU RENSEIGNEMENT

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

Chapitre Ier : Des accès administratifs aux données de connexion

- **Article L. 851-2** *(en vigueur, applicable au litige)*

Version issue de la 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 - art. 15

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.

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

B. Évolution des dispositions contestées

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

- **Article 20**

I. — Le livre II du même code est ainsi modifié :

II. 1° L'intitulé du titre IV est complété par les mots : « et accès administratif aux données de connexion » ;

2° Il est ajouté un chapitre VI ainsi rédigé :

« Chapitre VI

« Accès administratif aux données de connexion

(...)

- **« Art. L. 246-3**

Pour les finalités énumérées à l'article L. 241-2, les informations ou documents mentionnés à l'article L. 246-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs aux agents mentionnés au I de l'article L. 246-2.

« L'autorisation de recueil de ces informations ou documents est accordée, sur demande écrite et motivée des ministres de la sécurité intérieure, de la défense, de l'économie et du budget ou des personnes que chacun d'eux a spécialement désignées, par décision écrite du Premier ministre ou des personnes spécialement désignées par lui, pour une durée maximale de trente jours. Elle peut être renouvelée, dans les mêmes conditions de forme et de durée. Elle est communiquée dans un délai de quarante-huit heures au président de la Commission nationale de contrôle des interceptions de sécurité.

« Si celui-ci estime que la légalité de cette autorisation au regard des dispositions du présent titre n'est pas certaine, il réunit la commission, qui statue dans les sept jours suivant la réception par son président de la communication mentionnée au deuxième alinéa.

« Au cas où la commission estime que le recueil d'une donnée de connexion a été autorisé en méconnaissance des dispositions du présent titre, elle adresse au Premier ministre une recommandation tendant à ce qu'il y soit mis fin.

« Elle porte également cette recommandation à la connaissance du ministre ayant proposé le recueil de ces données et du ministre chargé des communications électroniques

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

- **Article 5**

I.-Le livre VIII du code de la sécurité intérieure, tel qu'il résulte de l'article 2 de la présente loi, est complété par un titre V intitulé : « Des techniques de recueil de renseignement soumises à autorisation ».
II.-Au même titre V, il est inséré un chapitre Ier intitulé « Des accès administratifs aux données de connexion » et comprenant les articles L. 851-1 à L. 851-7, tels qu'ils résultent du III du présent article.
III.-Le même code est ainsi modifié :

(...)

- **« Art. L. 851-2.-I**

Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des informations ou documents mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée comme présentant une menace.

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

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

c. 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 15**

L'article L. 851-2 du code de la sécurité intérieure est ainsi rédigé :

« Art. L. 851-2.-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.

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

- **Art. L. 851-2 consolidé**

(En *italique*, les éléments ajoutés, en ~~barré~~, les éléments supprimés)

I.- Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des informations ou documents mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée ~~comme présentant une menace~~ **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.**

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

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

~~III. -~~[déplacé]

C. Autres dispositions législatives

1. Code de la sécurité intérieure

LIVRE VIII : DU RENSEIGNEMENT

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**

Créé par LOI n°2015-912 du 24 juillet 2015 - art. 2

La mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées au 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. 821-2**

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

L'autorisation mentionnée à l'article L. 821-1 est délivrée sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur, du ministre de la justice ou des ministres chargés de l'économie, du budget ou des douanes. Chaque ministre ne peut déléguer cette attribution individuellement qu'à des collaborateurs directs habilités au secret de la défense nationale.

La demande précise :

1° La ou les techniques à mettre en œuvre ;

2° Le service pour lequel elle est présentée ;

3° La ou les finalités poursuivies ;

4° Le ou les motifs des mesures ;

5° La durée de validité de l'autorisation ;

6° La ou les personnes, le ou les lieux ou véhicules concernés.

Pour l'application du 6°, les personnes dont l'identité n'est pas connue peuvent être désignées par leurs identifiants ou leur qualité et les lieux ou véhicules peuvent être désignés par référence aux personnes faisant l'objet de la demande.

Lorsqu'elle a pour objet le renouvellement d'une autorisation, la demande expose les raisons pour lesquelles ce renouvellement est justifié au regard de la ou des finalités poursuivies.

- **Article L. 821-3**

Créé par LOI n°2015-912 du 24 juillet 2015 - art. 2

La demande est communiquée au président ou, à défaut, à l'un des membres de la Commission nationale de contrôle des techniques de renseignement parmi ceux mentionnés aux 2° et 3° de l'article L. 831-1, qui rend un avis au Premier ministre dans un délai de vingt-quatre heures. Si la demande est examinée par la formation restreinte ou par la formation plénière de la commission, le Premier ministre en est informé sans délai et l'avis est rendu dans un délai de soixante-douze heures.

Les avis mentionnés au présent article sont communiqués sans délai au Premier ministre. En l'absence d'avis transmis dans les délais prévus au même article, celui-ci est réputé rendu.

- **Article L. 821-4**

Créé par LOI n°2015-912 du 24 juillet 2015 - art. 2

L'autorisation de mise en œuvre des techniques mentionnées au 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.

- **Article L. 821-5**

Créé par LOI n°2015-912 du 24 juillet 2015 - art. 2

En cas d'urgence absolue et pour les seules finalités mentionnées aux 1° et 4° et au a du 5° de l'article L. 811-3, le Premier ministre, ou l'une des personnes déléguées mentionnées à l'article L. 821-4, peut délivrer de manière exceptionnelle l'autorisation mentionnée au même article L. 821-4 sans avis préalable de la Commission nationale de contrôle des techniques de renseignement. Il en informe celle-ci sans délai et par tout moyen.

Le Premier ministre fait parvenir à la commission, dans un délai maximal de vingt-quatre heures à compter de la délivrance de l'autorisation, tous les éléments de motivation mentionnés audit article L. 821-4 et ceux justifiant le caractère d'urgence absolue au sens du présent article.

- **Article L. 821-6**

Créé par LOI n°2015-912 du 24 juillet 2015 - art. 2

[Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015.]

- **Article L. 821-7**

Créé par LOI n°2015-912 du 24 juillet 2015 - art. 2

Un parlementaire, un magistrat, un avocat ou un journaliste ne peut être l'objet d'une demande de mise en œuvre, sur le territoire national, d'une technique de recueil de renseignement mentionnée au titre V du présent livre à raison de l'exercice de son mandat ou de sa profession. Lorsqu'une telle demande concerne l'une de ces personnes ou ses véhicules, ses bureaux ou ses domiciles, l'avis de la Commission nationale de contrôle des techniques de renseignement est examiné en formation plénière. L'article L. 821-5 n'est pas applicable. *[Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015.]*

La commission est informée des modalités d'exécution des autorisations délivrées en application du présent article.

Les transcriptions des renseignements collectés en application du présent article sont transmises à la commission, qui veille au caractère nécessaire et proportionné des atteintes, le cas échéant, portées aux garanties attachées à l'exercice de ces activités professionnelles ou mandats.

- **Article L. 821-8**

Créé par LOI n°2015-912 du 24 juillet 2015 - art. 2

La Commission nationale de contrôle des techniques de renseignement peut adresser des recommandations et saisir le Conseil d'Etat dans les conditions prévues, respectivement, aux articles L. 833-6 et L. 833-8.

Chapitre Ier : Des accès administratifs aux données de connexion

- **Article L. 841-1**

Modifié par LOI n°2015-1556 du 30 novembre 2015 - art. 1

Sous réserve des dispositions particulières prévues à l'article L. 854-9 du présent code, le Conseil d'Etat est compétent pour connaître, dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, des requêtes concernant la mise en œuvre des techniques de renseignement mentionnées au titre V du présent livre.

Il peut être saisi par :

1° Toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard et justifiant de la mise en œuvre préalable de la procédure prévue à l'article L. 833-4 ;

2° La Commission nationale de contrôle des techniques de renseignement, dans les conditions prévues à l'article L. 833-8.

Lorsqu'une juridiction administrative ou une autorité judiciaire est saisie d'une procédure ou d'un litige dont la solution dépend de l'examen de la régularité d'une ou de plusieurs techniques de recueil de renseignement, elle peut, d'office ou sur demande de l'une des parties, saisir le Conseil d'Etat à titre préjudiciel. Il statue dans le délai d'un mois à compter de sa saisine.

- **Article L. 841-2**

Créé par LOI n°2015-912 du 24 juillet 2015 - art. 2

Le Conseil d'Etat est compétent pour connaître, dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, des requêtes concernant la mise en œuvre de l'article 41 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, pour les traitements ou parties de traitements intéressant la sûreté de l'Etat dont la liste est fixée par décret en Conseil d'Etat.

- **Article L. 851-1**

Créé par 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.

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.

2. Code de justice administrative

Chapitre III bis : Le contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'Etat

- **Article L. 773-1**

Modifié par LOI n°2015-1556 du 30 novembre 2015 - art. 2

Le Conseil d'Etat examine les requêtes présentées sur le fondement des articles L. 841-1 et L. 841-2 du code de la sécurité intérieure conformément aux règles générales du présent code, sous réserve des dispositions particulières du présent chapitre *[Dispositions déclarées non conformes à la Constitution par la décision du Conseil constitutionnel n° 2015-713 DC du 23 juillet 2015] et du chapitre IV du titre V du livre VIII du code de la sécurité intérieure.*

NOTA :

Conformément à l'article 26 de la loi n° 2015-912 du 24 juillet 2015, à l'exception des articles 3, 4, 9, 16 à 20 et 22 et sous réserve des II à IV du présent article, la présente loi entre en vigueur au lendemain de la publication au Journal officiel du décret nommant le président de la Commission nationale de contrôle des techniques de renseignement.

- **Article L. 773-2**

Créé par LOI n°2015-912 du 24 juillet 2015 - art. 10

Sous réserve de l'inscription à un rôle de l'assemblée du contentieux ou de la section du contentieux qui siègent alors dans une formation restreinte, les affaires relevant du présent chapitre sont portées devant une formation spécialisée. La composition de ces formations est fixée par décret en Conseil d'Etat.

Préalablement au jugement d'une affaire, l'inscription à un rôle de l'assemblée du contentieux ou de la section du contentieux de l'examen d'une question de droit posée par cette affaire peut être demandée. L'assemblée du contentieux ou la section du contentieux siègent dans leur formation de droit commun.

Les membres des formations mentionnées au premier alinéa et leur rapporteur public sont habilités ès qualités au secret de la défense nationale. Les agents qui les assistent doivent être habilités au secret de la défense nationale aux fins d'accéder aux informations et aux documents nécessaires à l'accomplissement de leur mission. Les membres de ces formations et leur rapporteur public sont astreints, comme les agents qui les assistent, au respect des secrets protégés aux articles 413-10 et 226-13 du code pénal pour les faits, les actes et les renseignements dont ils peuvent avoir connaissance dans l'exercice de leurs fonctions.

Dans le cadre de l'instruction de la requête, les membres de la formation de jugement et le rapporteur public sont autorisés à connaître de l'ensemble des pièces en possession de la Commission nationale de contrôle des techniques de renseignement ou des services mentionnés à l'article L. 811-2 du code de la sécurité intérieure et ceux désignés par le décret en Conseil d'Etat mentionné à l'article L. 811-4 du même code et utiles à l'exercice de leur office, y compris celles protégées au titre de l'article 413-9 du code pénal.

NOTA :

Conformément à l'article 26 de la loi n° 2015-912 du 24 juillet 2015, à l'exception des articles 3, 4, 9, 16 à 20 et 22 et sous réserve des II à IV dudit article, la loi susmentionnée entre en vigueur au lendemain de la publication au Journal officiel du décret nommant le président de la Commission nationale de contrôle des techniques de renseignement.

- **Article L .773-3**

Créé par LOI n°2015-912 du 24 juillet 2015 - art. 10

Les exigences de la contradiction mentionnées à l'article L. 5 du présent code sont adaptées à celles du secret de la défense nationale.

La Commission nationale de contrôle des techniques de renseignement est informée de toute requête présentée sur le fondement de l'article L. 841-1 du code de la sécurité intérieure. Elle est invitée à présenter, le cas échéant, des observations écrites ou orales. L'intégralité des pièces produites par les parties lui est communiquée.

La formation chargée de l'instruction entend les parties séparément lorsqu'est en cause le secret de la défense nationale.

D. Autres dispositions réglementaires

a. Décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement

Article 2

Le chapitre Ier du titre V du livre VIII de la partie réglementaire du code de la sécurité intérieure est ainsi complété :

1° Avant l'article R. 851-1, il est créé une section 1 intitulée : « Section 1 : Services autres que les services spécialisés de renseignement pouvant être autorisés à accéder aux données de connexion » et comprenant les articles R. 851-1 à R. 851-4 ;

2° A la section 1 résultant du 1°, après l'article R. 851-1, il est inséré un article R. 851-1-1 ainsi rédigé :

- **« Art. R. 851-1-1**

-Les services relevant de l'article L. 811-4 dont les agents individuellement désignés et habilités peuvent être autorisés à utiliser la technique mentionnée à l'article L. 851-2 au titre de la prévention du terrorisme sont les suivants :

« 1° Services placés sous l'autorité du directeur général de la police nationale :

« a) A la direction centrale de la police judiciaire :

«-la sous-direction antiterroriste ;

«-la sous-direction de la lutte contre la cybercriminalité ;

«-les unités de lutte antiterroriste des directions interrégionales et régionales de police judiciaire ;

« b) A la direction centrale de la sécurité publique :

«-l'unité nationale et les unités territoriales de recherche et d'appui des services du renseignement territorial ;

« 2° Unités placées sous l'autorité du directeur général de la gendarmerie nationale :

« a) A la direction des opérations et de l'emploi :

«-la sous-direction de l'anticipation opérationnelle ;

«-la sous-direction de la police judiciaire ;

« b) Les groupes d'appui et de renseignement des sections de recherches de la gendarmerie nationale ;

« 3° Services placés sous l'autorité du préfet de police de Paris :

« a) A la direction du renseignement :

«-la sous-direction de la sécurité intérieure ;

«-la sous-direction du renseignement territorial ;

« b) A la direction régionale de la police judiciaire de Paris :

«-la section antiterroriste de la brigade criminelle et la brigade de recherche et d'intervention de la sous-direction des brigades centrales ;

« 4° Services placés sous l'autorité d'emploi du ministre de la défense :

«-les groupes d'appui et de renseignement des sections de recherches de la gendarmerie maritime, de la gendarmerie de l'air et de la gendarmerie de l'armement. » ;

3° Après l'article R. 851-4, il est créé une section 2 et une section 3 ainsi rédigées :

« Section 2

« Données de connexion susceptibles d'être recueillies

- **« Art. R. 851-5.-I**

Les informations ou documents mentionnés à l'article L. 851-1 sont, à l'exclusion du contenu des correspondances échangées ou des informations consultées :
« 1° Ceux énumérés aux articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques et à l'article 1er du décret n° 2011-219 du 25 février 2011 modifié relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne ;

« 2° Les données techniques autres que celles mentionnées au 1° :

« a) Permettant de localiser les équipements terminaux ;

« b) Relatives à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne ;

« c) Relatives à l'acheminement des communications électroniques par les réseaux ;

« d) Relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne ;

« e) Relatives aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels.

« II.-Seuls les informations et documents mentionnés au 1° du I peuvent être recueillis en application de l'article L. 851-1. Ce recueil a lieu en temps différé.

« Les informations énumérées au 2° du I ne peuvent être recueillies qu'en application des articles L. 851-2 et L. 851-3 dans les conditions et limites prévues par ces articles et sous réserve de l'application de l'article R. 851-9.

« Section 3

« Conditions d'accès aux données de connexion

- **« Art. R. 851-6.-I**

Les demandes tendant au recueil mentionné à l'article L. 851-1 comportent, outre les éléments énumérés à l'article L. 821-2, la nature précise des informations ou documents dont le recueil est demandé et, le cas échéant, la période concernée.

« Seuls peuvent solliciter les informations et documents mentionnés au deuxième alinéa de l'article L. 851-1 les agents individuellement désignés et habilités par le directeur dont ils relèvent. La demande comporte alors également le nom, le prénom et la qualité du demandeur ainsi que son service d'affectation et l'adresse de celui-ci. A défaut, lorsque l'anonymat de l'agent concerné doit être préservé, la demande comporte toute indication permettant à la Commission nationale de contrôle des techniques de renseignement et au Premier ministre ou à ses délégués de vérifier l'identité du demandeur.

« II.-Le groupement interministériel de contrôle enregistre et conserve dans les mêmes conditions de durée que celles prévues à l'article L. 822-2 pour les renseignements collectés, dans un traitement automatisé qu'il met en œuvre, les demandes tendant au recueil mentionné à l'article L. 851-1 ainsi que les décisions du Premier ministre ou de ses délégués relatives à ces demandes.

« Les demandes et les décisions sont automatiquement effacées du traitement, sous l'autorité du Premier ministre, à l'expiration de la durée de conservation. Le directeur du groupement interministériel de contrôle adresse chaque année à la Commission nationale de contrôle des techniques de renseignement un procès-verbal certifiant que l'effacement a été effectué.

« III.-Lorsqu'une demande tendant au recueil mentionné à l'article L. 851-1 a été approuvée par le Premier ministre ou ses délégués, le groupement interministériel de contrôle adresse aux opérateurs et aux personnes mentionnés à l'article L. 851-1 l'ordre de procéder au recueil, qui ne peut faire état des éléments prévus aux 2° à 4° de l'article L. 821-2 et au second alinéa du I du présent article.
« Les opérateurs et les personnes mentionnés à l'article L. 851-1 transmettent sans délai les informations ou documents demandés au groupement interministériel de contrôle, selon des modalités assurant leur sécurité, leur intégrité et leur suivi.

« IV.-Le groupement interministériel de contrôle enregistre et conserve dans les conditions prévues à l'article L. 822-2, dans un traitement automatisé qu'il met en œuvre, les informations ou documents transmis et les met à disposition des demandeurs pour exploitation. Ces informations ou documents sont automatiquement effacés du traitement dans les conditions prévues au second alinéa du II du présent article.

- **« Art. R. 851-7.-I**

Les demandes tendant au recueil mentionné à l'article L. 851-2 comportent, outre les éléments énumérés à l'article L. 821-2, la nature précise des informations ou documents dont le recueil est demandé.

« II.-Le groupement interministériel de contrôle enregistre, conserve et efface, dans les conditions prévues au II de l'article R. 851-6, les demandes tendant au recueil mentionné à l'article L. 851-2 ainsi que les décisions du Premier ministre ou de ses délégués relatives à ces demandes.

« III.-Lorsqu'une demande tendant au recueil mentionné à l'article L. 851-2 a été présentée par un service mentionné à l'article R. 851-1-1 et approuvée par le Premier ministre ou l'un de ses délégués, le groupement interministériel de contrôle recueille en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, les informations ou documents demandés.

« IV.-Lorsque les informations ou documents demandés ont été recueillis en application du III du présent article, le groupement interministériel de contrôle les enregistre, conserve et efface, dans les conditions prévues au IV de l'article R. 851-6, et les met à disposition des demandeurs pour exploitation.

- **« Art. R. 851-8.-I**

Le groupement interministériel de contrôle enregistre, conserve et efface, dans les conditions prévues au II de l'article R. 851-6, les demandes tendant au recueil mentionné à l'article L. 851-4 ainsi que les décisions du Premier ministre ou de ses délégués relatives à ces demandes.
« II.-Lorsqu'une demande tendant au recueil mentionné à l'article L. 851-4 a été approuvée par le Premier ministre ou ses délégués, il est procédé comme au III de l'article R. 851-6. La transmission des données techniques demandées intervient en temps réel sur sollicitation du réseau par l'opérateur qui l'exploite.
« III.-Le groupement interministériel de contrôle enregistre, conserve et efface, dans les conditions prévues au IV de l'article R. 851-6, les données techniques transmises et les met à disposition des demandeurs pour exploitation.

- **« Art. R. 851-9**

Les informations ou documents recueillis en application du présent chapitre ne peuvent, sans l'autorisation prévue à l'article L. 852-1 ou à l'article L. 853-2, être exploités aux fins d'accéder au contenu de correspondances échangées ou d'informations consultées.

- **« Art. R. 851-10**

La Commission nationale de contrôle des techniques de renseignement dispose d'un accès permanent, complet, direct et immédiat aux traitements automatisés prévus aux articles R. 851-6 à R. 851-8.
« Le Premier ministre ou ses délégués fournissent à la commission tous éclaircissements qu'elle sollicite sur les demandes qu'ils ont approuvées. »

E. Application des dispositions contestées

1. Jurisprudence administrative

- **CE, 19 octobre 2016, n° 396958**

4. Il ressort des pièces du dossier que M. B...a saisi, le 23 novembre 2015, la Commission nationale de contrôle des techniques de renseignement (CNCTR) afin de vérifier qu'aucune technique de renseignement n'était irrégulièrement mise en oeuvre à son égard. Par lettre du 8 décembre 2015, le président de la CNCTR a informé M. B...qu'il avait été procédé à l'ensemble des vérifications requises et que la procédure était terminée, sans apporter à l'intéressé d'autres informations. Dans le dernier état de son argumentation, M. B...demande au Conseil d'Etat de vérifier si des techniques de renseignement ont été mises en oeuvre à son égard et, le cas échéant, de constater qu'elles l'ont été illégalement. Il résulte de ce qui a été dit au point 2 que ces conclusions, qui se rapportent à la mise en oeuvre éventuelle de techniques de renseignement postérieurement à l'entrée en vigueur, le 3 octobre 2015, de la loi du 24 juillet 2015, sont recevables, que la décision de les mettre en oeuvre ait été prise avant comme après cette date, contrairement à ce que le Premier ministre soutient en défense.

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

6. La formation spécialisée a examiné, selon les modalités décrites au point précédent, les éléments fournis par la CNCTR, qui a précisé l'ensemble des vérifications auxquelles elle avait procédé, et par le Premier ministre. A l'issue de cet examen, il y a lieu de répondre à M. B...que la vérification qu'il a sollicitée a été effectuée et n'appelle aucune mesure de la part du Conseil d'Etat.

- **CE, 12 février 2016, N° 388134, Association French Data Network**

5. Considérant, en premier lieu, que le décret attaqué encadre l'accès administratif aux données de connexion, pour la poursuite des finalités établies à l'article L. 241-2 du code de la sécurité intérieure dont, notamment, la sécurité nationale et la prévention du terrorisme ; **qu'il est constant que l'accès administratif aux données de connexion, tel qu'il est précisé par le décret attaqué, contribue à la réalisation de cet objectif, qui est d'intérêt général ;**

6. Considérant, en second lieu, que le décret attaqué définit, à l'article R. 246-1 qu'il insère dans le code de la sécurité intérieure, les " informations et documents " qui, à l'exclusion de tout autre, et en particulier de ceux relatifs au contenu des correspondances, peuvent faire l'objet d'une demande de recueil ; que l'obligation faite aux opérateurs et aux personnes mentionnées à l'article L. 246-1 de conserver, pour un an, ces données, est fondée sur des règles précises et contraignantes, dont la méconnaissance est sanctionnée dans les conditions fixées par les dispositions de l'article L. 39-3 du code des postes et des communications électroniques ; que, dans ces conditions, est en mesure d'être connue l'étendue maximale des données susceptibles de faire l'objet d'une collecte, pour la poursuite des finalités rappelées au point précédent et sur demande des seuls agents habilités à cette fin ;

7. Considérant que le décret attaqué énumère, au I de l'article R. 246-2 qu'il insère dans ce même code, l'ensemble des services dont les agents peuvent solliciter l'accès aux données de connexion ; que ces services ont des missions se rattachant à la poursuite des finalités précédemment rappelées ; qu'en outre, le II de ce même article précise qu'au sein des services ainsi identifiés, seuls les agents individuellement désignés et dûment habilités par le directeur dont ils relèvent peuvent solliciter ces informations et ces documents ; que ces demandes sont enregistrées et conservées dans un traitement de données mis en oeuvre par le Premier ministre, de telle sorte que la Commission nationale de contrôle des interceptions de sécurité puisse y accéder et, le cas échéant, demander des éclaircissements ; qu'il suit de là que, contrairement à ce qui est soutenu**, le décret attaqué définit, avec une précision suffisante, les conditions dans lesquelles les agents et services sont susceptibles de solliciter l'accès aux données de connexion ;**

8. Considérant qu'en vertu des articles R. 246-5 et R. 246-6 du code de la sécurité intérieure issu du décret attaqué, des traitements automatisés sont mis en oeuvre par le Premier ministre pour enregistrer et conserver, pour une durée maximale de trois ans, d'une part, " les demandes des agents et les décisions de la personnalité qualifiée ou de ses adjoints ", d'autre part " les informations ou les documents transmis par les opérateurs et les personnes mentionnées à l'article L. 246-1 " ; qu'il ressort des pièces du dossier, et notamment de la délibération de la Commission nationale de l'informatique et des libertés du 4 décembre 2014, que cette période de trois ans, qui permet aux services d'avoir accès aux données pendant toute la durée de leurs investigations relatives à la poursuite des finalités d'intérêt général listées à l'article L. 241-2 du même code, constitue une durée maximale, à l'issue de laquelle les données sont automatiquement effacées ; qu'à cet égard, l'article R. 246-5 prévoit que " le directeur du groupement interministériel de contrôle adresse chaque année à la Commission nationale de contrôle des interceptions de sécurité un procès-verbal certifiant que l'effacement a été effectué " ; que, dans ces conditions, la durée de conservation prévue par le décret attaqué, qui permet, au demeurant, à la Commission nationale de contrôle des interceptions de sécurité d'exercer son contrôle de manière plus approfondie, n'est pas excessive ;

9. Considérant qu'il ressort de l'article R. 246-6 déjà mentionné que les demandes formulées par les agents habilités des services désignés sont soumises à l'approbation d'une personnalité qualifiée, dont les modalités de

désignation sont établies à l'article R. 246-3 du même code, créé par le décret attaqué ; que cette personnalité qualifiée, ainsi que ses adjoints, sont choisis, sous le contrôle du juge, par la Commission nationale de contrôle des interceptions de sécurité en raison de leur compétence et de leur impartialité ; que, par un nouvel article R. 246-7 inséré au sein de ce même code, le décret attaqué prévoit une procédure spécifique pour les demandes de recueil d'informations ou de documents " impliquant sollicitation du réseau et transmission en temps réel ", qui requièrent l'approbation du Premier ministre ; que, par ailleurs, aux termes de l'article R. 246-8 du code de la sécurité intérieure : " la Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent aux traitements automatisés mentionnés aux articles R. 246-5, R. 246-6 et R. 246-7 " ; qu'en outre, **toute décision faisant droit, dans les conditions énoncées ci-dessus, à une demande d'accès administratif aux données de connexion est susceptible d'être contestée devant le juge administratif ; que, dans ces conditions, le moyen tiré de ce que le décret attaqué n'aurait pas apporté de garanties suffisantes de nature à permettre un contrôle effectif des demandes d'accès administratif aux données de connexion doit être écarté ;**

10. Considérant qu'il résulte de tout ce qui précède que le décret attaqué ne porte pas une atteinte disproportionnée aux droits et libertés garantis par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ; que doivent, pour les mêmes motifs et en tout état de cause, être écartés les moyens, soulevés par les associations requérantes, et tirés de la méconnaissance des articles 7, 8 et 11 de la Charte des droits fondamentaux de l'Union européenne, respectivement relatifs au respect de la vie privée et familiale, à la protection des données à caractère personnel et à la liberté d'expression et d'information ; (...)

En ce qui concerne le moyen tiré de la méconnaissance de la directive 2002/58/CE :

13. Considérant qu'aux termes de l'article 5 de la directive 2002/58/CE : " Les États membres garantissent, par la législation nationale, (...) la confidentialité des données relatives au trafic (...). En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. " ; qu'en vertu de son article 15 : " Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe " ; qu'il résulte de ces dispositions que, contrairement à ce que soutiennent les associations requérantes, **cette directive ne fait pas obstacle à ce qu'un Etat membre puisse organiser la conservation préventive des données de connexion en vue de leur réquisition administrative, dès lors que la procédure ainsi prévue respecte les conditions énoncées par l'article 15 ainsi qu'il résulte des points 6 à 10 de la présente décision ;**

2. Jurisprudence de l’Union européenne

- **CJUE, 8 avril 2014, Digital Rights aff. C-293/12 et C-594/12,**

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

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

53 À cet égard, il convient de rappeler que la protection des données à caractère personnel, résultant de

l’obligation explicite prévue à l’article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l’article 7 de celle-ci.

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

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

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

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

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

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

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

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

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

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

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

- **CJUE, 21 décembre 2016, Tele2 Sverige AB/Post- och telestyrelsen (C-203/15), Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15)**

http://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1497262317054&uri=CELEX:62015CJ0203

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

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

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

100 L'ingérence que comporte une telle réglementation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de

communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 37).

101 Même si une telle réglementation n'autorise pas la conservation du contenu d'une communication et, partant, n'est pas de nature à porter atteinte au contenu essentiel desdits droits (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 39), la conservation des données relatives au trafic et des données de localisation pourrait toutefois avoir une incidence sur l'utilisation des moyens de communication électronique et, en conséquence, sur l'exercice par les utilisateurs de ces moyens de leur liberté d'expression, garantie à l'article 11 de la Charte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 28).

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

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

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

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

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

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

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

109 Pour satisfaire aux exigences énoncées au point précédent du présent arrêt, cette réglementation nationale doit, en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences, de telle sorte que les personnes

dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire (voir, par analogie, à propos de la directive 2006/24, arrêt Digital Rights, point 54 et jurisprudence citée).

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

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

F. Délibération de la CNCTR n° 1/2016 du 14 janvier 2016

Saisie pour avis par le Premier ministre (1) d'un projet de décret relatif aux techniques de renseignement, la Commission nationale de contrôle des techniques de renseignement (CNCTR), réunie en formation plénière, a formulé les observations suivantes : **(...)**

I. - Remarques de portée générale

La CNCTR observe en outre que le titre V du livre VIII du code de la sécurité intérieure présente les techniques de renseignement selon l'atteinte qu'elles peuvent porter à la vie privée, en partant de la technique réputée la moins intrusive, en l'espèce le recueil administratif des données de connexion. Si la CNCTR considère qu'un tel recueil est effectivement moins attentatoire à la vie privée que d'autres techniques, elle rappelle que les données de connexion sont des données sensibles et que le degré d'intrusion doit être apprécié au regard du mode de recueil mis en oeuvre et, partant, de la nature et de la quantité des données collectées.

Les flux de communications électroniques sont aujourd'hui tels que le recueil des données de connexion permet de connaître ou de déduire de très nombreuses informations sur les personnes visées. Prises dans leur ensemble, ces données peuvent fournir des indications sur la vie privée, comme les habitudes de la vie quotidienne, les lieux de séjours ou les déplacements.

À cet égard, un recueil en temps réel augmente l'atteinte portée à la vie privée, ce pourquoi le législateur a expressément décidé, sous le contrôle du Conseil constitutionnel, de limiter, en fonction du motif invoqué, de la durée de surveillance ou de la nature des données recueillies, la possibilité d'un tel recueil, qui n'est prévu qu'aux articles L. 851-2 et L. 851-4 du code de la sécurité intérieure.

2. Sur le mode de recueil des données de connexion

a) S'agissant de l'accès administratif aux données de connexion prévu à l'article L. 851-1 du code de la sécurité intérieure, la CNCTR considère que la loi, eu égard tant à sa rédaction qu'aux travaux parlementaires qui ont précédé son adoption, n'a ni pour objet ni pour effet de permettre le recueil en temps réel des données, qui doit être expressément prévu, comme il l'est aux articles L. 851-2 et L. 851-4 du code. Le recueil autorisé sur le fondement de l'article L. 851-1 du code ne peut donc intervenir qu'en temps différé.

A cet égard, dans sa décision n° 2015-713 DC du 23 juillet 2015, le Conseil constitutionnel, après avoir analysé les dispositions des articles L. 851-1 et L. 851-2 du code de la sécurité intérieure, a jugé « qu'en outre, lorsque le recueil des données a lieu en temps réel, il ne pourra être autorisé que pour les besoins de la prévention du terrorisme, pour une durée de deux mois renouvelable, uniquement à l'égard d'une personne préalablement identifiée comme présentant une menace et sans le recours à la procédure d'urgence absolue prévue à l'article L. 821-5 du même code » (considérant 56), c'est-à-dire dans les conditions prévues à l'article L. 851-2. En conséquence, les données de connexion susceptibles d'être recueillies en application de l'article L. 851-1 du code de la sécurité intérieure ne peuvent être que des données préalablement conservées par les opérateurs de

communications électroniques, les hébergeurs et les fournisseurs de services sur internet. Il s'agit, par définition, des données mentionnées au 1° du I du nouvel article R. 851-5 du code.

La CNCTR souhaite que le cadre juridique exposé ci-dessus ressorte clairement des dispositions du projet de décret. Elle note que, dans sa saisine rectificative, le Premier ministre indique garantir que « les données de connexion traitées par les réseaux mais non conservées ne peuvent pas être recueillies dans le cadre de l'article L. 851-1 » du code de la sécurité intérieure. Cette garantie est censée être apportée par le II du nouvel article R. 851-5 du code, aux termes duquel : « Les informations énumérées aux 2° à 6° du I ne peuvent être recueillies qu'en application des articles L. 851-2 à L. 851-6, dans les conditions et limites prévues par ces articles ». La CNCTR préconise une rédaction plus directe, plus complète et, partant, plus sûre. Elle propose que le II du nouvel article R. 851-5 du code de la sécurité intérieure soit ainsi rédigé :

« II. - Seuls les informations et documents mentionnés au 1° du I peuvent être recueillis en application de l'article L. 851-1. Ce recueil a lieu en temps différé. »

Si le Gouvernement souhaitait conserver au surplus l'alinéa du II figurant dans la saisine rectificative, la CNCTR recommanderait de modifier les références qu'il contient. Seuls les articles L. 851-2 et L. 851-3 du code de la sécurité intérieure se réfèrent en effet à l'ensemble des données de connexion mentionnées à l'article L. 851-1 du même code, dont la nature doit être précisée par décret en Conseil d'Etat. En revanche, les articles L. 851-4 à L. 851-6 du code définissent chacun de façon autonome les données susceptibles d'être recueillies sur leur fondement : il s'agit des « données techniques relatives à la localisation des équipements terminaux utilisés » à l'article L. 851-4, des données permettant « la localisation en temps réel d'une personne, d'un véhicule ou d'un objet » à l'article L. 851-5 et des « données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que [d]es données relatives à la localisation des équipements terminaux utilisés » à l'article L. 851-6. La CNCTR propose dès lors que la référence aux articles L. 851-4 à L. 851-6 soit supprimée et que l'alinéa soit ainsi rédigé : « Les informations énumérées aux 2° à 6° du I ne peuvent être recueillies qu'en application des articles L. 851-2 et L. 851-3, dans les conditions et limites prévues par ces articles. » ;

b) En ce qui concerne l'accès administratif aux données de connexion en temps réel prévu à l'article L. 851-2 du code de la sécurité intérieure, la CNCTR observe que ce recueil s'effectue, aux termes de la loi, « sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1 » du code.

Au nouvel article R. 851-7 du code de la sécurité intérieure, le projet de décret dispose que lorsque le recueil en temps réel est demandé par des services de renseignement dits « du second cercle », il est effectué par le groupement interministériel de contrôle (GIC). La CNCTR estime cette procédure conforme à la loi. Par ailleurs, pour le bon déroulement des contrôles a posteriori dont la loi l'a chargée, la CNCTR demande qu'un accès permanent, complet, direct et immédiat à l'ensemble des données de connexion recueillies en application de l'article L. 851-2 du code de la sécurité intérieure, quel que soit le service demandeur, lui soit garanti dans les locaux du GIC.

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.

B. Jurisprudence du Conseil constitutionnel

a. Respect de la vie privée et prévention des atteintes à l'ordre public

- **Décision n° 2015-478 QPC du 24 juillet 2015, Association French Data Network et autres [Accès administratif aux données de connexion]**

- SUR LE GRIEF TIRÉ DE L'INCOMPÉTENCE NÉGATIVE RÉSULTANT DE LA DÉFINITION INSUFFISANTE DES DONNÉES DE CONNEXION ET DES CONDITIONS DE LEUR COLLECTE EN CAS DE TRANSMISSION EN TEMPS RÉEL :

8. Considérant que les associations requérantes soutiennent, d'une part, qu'en employant les termes d' « informations ou documents » et ceux d' « opérateur de communications électroniques » à l'article L. 246-1 du code de la sécurité intérieure, le législateur n'a pas défini de façon suffisamment précise les données de connexion pouvant être collectées par l'autorité administrative sur réquisition et, d'autre part, qu'en employant les termes de « sollicitation du réseau » à l'article L. 246-3 du même code, il n'a pas exclu la possibilité pour cette autorité d'accéder directement aux données de connexion détenues par les opérateurs de communications électroniques dans le cadre de cette même procédure ; qu'il en résulterait une méconnaissance par le législateur de l'étendue de sa compétence dans des conditions portant atteinte au droit au respect de la vie privée ;

9. Considérant que la méconnaissance par le législateur de sa propre compétence ne peut être invoquée à l'appui d'une question prioritaire de constitutionnalité que dans le cas où cette méconnaissance affecte par elle-même un droit ou une liberté que la Constitution garantit ;

10. Considérant qu'aux termes de l'article 34 de la Constitution : « La loi fixe les règles concernant... les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques » ; que la méconnaissance par le législateur de sa compétence, dans la détermination de ces garanties dans le cadre d'une procédure de réquisition administrative de données de connexion, affecte par elle-même le droit au respect de la vie privée ;

11. Considérant, en premier lieu, d'une part, qu'en vertu de l'article L. 246-1 du code de la sécurité intérieure, la procédure de recueil des données de connexion sur réquisition administrative peut s'exercer auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du paragraphe I de l'article 6 de la loi du 21 juin 2004 susvisée ; que l'article L. 32 du code des postes et des communications électroniques définit dans son 1° les communications électroniques comme « les émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique » et dans son 15° l'opérateur comme « toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques » ; que le paragraphe II de l'article L. 34-1 du même code prévoit son application aux opérateurs de communications électroniques, et notamment aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, et aux personnes qui fournissent au public des services de communications électroniques, ainsi qu'aux personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau ; que les personnes mentionnées aux 1 et 2 du paragraphe I de l'article 6 de la loi du 21 juin 2004 sont celles dont l'activité est d'offrir un accès à des services de communication au public en ligne et celles qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ;

12. Considérant, d'autre part, qu'en vertu du même article L. 246-1, peuvent être recueillis par l'autorité administrative les informations ou documents traités ou conservés par les réseaux ou services de communications électroniques des personnes susmentionnées ; que, selon les dispositions du VI de l'article L. 34-1 du code des postes et des communications électroniques, les données conservées et traitées portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux et ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ; que selon le paragraphe II de l'article 6 de la loi du 21 juin 2004, les données conservées sont celles de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires ; qu'ainsi, le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées ;

13. Considérant, en second lieu, qu'il résulte **de l'article L. 246-1 que les données de connexion requises sont transmises par les opérateurs aux autorités administratives compétentes ; que selon l'article L. 246-3, lorsque les données de connexion sont transmises en temps réel à l'autorité administrative, celles-ci ne peuvent être recueillies qu'après « sollicitation » de son réseau par l'opérateur ; que, par suite, les**

autorités administratives ne peuvent accéder directement au réseau des opérateurs dans le cadre de la procédure prévue aux articles L. 246-1 et L. 246-3 ;

14. Considérant qu'il résulte de ce qui précède que le grief tiré de ce que le législateur, en ne définissant pas précisément la procédure de réquisition administrative des données de connexion détenues et traitées par les opérateurs de communications électroniques, a méconnu l'étendue de sa compétence dans des conditions affectant le droit au respect de la vie privée, doit être écarté ;

- **Décision n° 2015-713 DC du 23 juillet 2015, Loi relative au renseignement**

. En ce qui concerne les articles L. 851-1 et L. 851-2 du code de la sécurité intérieure :

52. Considérant que l'article L. 851-1 du code de la sécurité intérieure reprend la procédure de réquisition administrative de données techniques de connexion prévue auparavant à l'article L. 246-1 du même code autorisant l'autorité administrative à recueillir des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, auprès des opérateurs de communications électroniques, auprès des personnes offrant, au titre d'une activité professionnelle principale ou accessoire, au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau et auprès de celles qui assurent, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ; que, par exception aux dispositions de l'article L. 821-2 du même code, lorsque la demande sera relative 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, elle sera directement transmise à la commission nationale de contrôle des techniques de renseignement par les agents individuellement désignés et habilités des services de renseignement ;

53. Considérant que **l'article L. 851-2 du code de la sécurité intérieure permet à l'administration, pour les seuls besoins de la prévention du terrorisme, de recueillir en temps réel, sur les réseaux des opérateurs et personnes mentionnés à l'article L. 851-1**, les informations ou documents mentionnés à ce même article relatifs à une personne préalablement identifiée comme présentant une menace ;

54. Considérant que les députés requérants font valoir que le législateur a méconnu l'étendue de sa compétence en ne définissant pas suffisamment les données de connexion pouvant faire l'objet d'un recueil par les autorités administratives et que la procédure porte une atteinte disproportionnée au droit au respect de la vie privée compte tenu de la nature des données pouvant être recueillies, de l'ampleur des techniques pouvant être utilisées et des finalités poursuivies ;

55. Considérant, en premier lieu, que l'autorisation de recueil de renseignement prévue par les articles L. 851-1 et L. 851-**2 porte uniquement sur les informations ou documents traités ou conservés par les réseaux ou services de communications électroniques des personnes mentionnées au considérant 52** ; que selon les dispositions du paragraphe VI de l'article L. 34-1 du code des postes et des communications électroniques, **les données conservées et traitées par les opérateurs de communications électroniques et les personnes offrant au public une connexion permettant une telle communication portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux et ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications** ; que selon le paragraphe II de l'article 6 de la loi du 21 juin 2004, **les données conservées par les personnes offrant un accès à des services de communication en ligne et celles assurant le stockage de diverses informations pour mise à disposition du public par ces services sont celles de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires** ; qu'ainsi, le législateur a suffisamment défini les données de connexion, qui ne peuvent porter sur le contenu de correspondances ou les informations consultées ;

56. Considérant, en second lieu, que cette technique de recueil de renseignement est mise en œuvre dans les conditions et avec les garanties rappelées au considérant 51 ; qu'elle ne pourra être mise en œuvre que pour les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure ; qu'elle est autorisée pour une durée de quatre mois renouvelable conformément à l'article L. 821-4 du même code ; qu'en outre, lorsque le recueil des données a lieu en temps réel, il ne pourra être autorisé que pour les besoins de la prévention du terrorisme, pour une durée de deux mois renouvelable, uniquement à l'égard d'une personne préalablement identifiée comme présentant une menace et sans le recours à la procédure d'urgence absolue prévue à l'article L. 821-5 du même code ; que, par suite, le législateur a assorti la procédure de réquisition de données techniques de garanties

propres à assurer entre, d'une part, le respect de la vie privée des personnes et, d'autre part, la prévention des atteintes à l'ordre public et celle des infractions, une conciliation qui n'est pas manifestement déséquilibrée ;

57. Considérant qu'il résulte de tout ce qui précède que les articles L. 851-1 et L. 851-2 du code de la sécurité intérieure doivent être déclarés conformes à la Constitution ;

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

- SUR CERTAINES DISPOSITIONS DE L'ARTICLE 216 :

134. Considérant que le 2° de l'article 216 permet à l'Autorité de la concurrence d'obtenir la communication de données de connexion ;

135. Considérant que le 2° de l'article 216 insère, avant le dernier alinéa de l'article L. 450-3 du code de commerce, un nouvel alinéa permettant aux agents mentionnés à l'article L. 450-1 du même code de « se faire communiquer les données conservées et traitées par les opérateurs de communications électroniques en application de l'article L. 34-1 du code des postes et des communications électroniques et par les prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et en obtenir la copie » ;

136. Considérant que les députés requérants soutiennent que les dispositions contestées portent une atteinte manifestement disproportionnée au droit au respect de la vie privée dès lors, d'une part, que les agents de l'Autorité de la concurrence pourront obtenir des données de connexion pour les besoins d'une simple enquête et, d'autre part, que ces agents n'encourent aucune sanction en cas de divulgation des informations obtenues ; que, selon eux, en ne prévoyant pas l'intervention de l'autorité judiciaire pour autoriser la communication des données, le législateur a également porté atteinte à la garantie des droits et à l'article 66 de la Constitution ;

137. Considérant que la communication des données de connexion est de nature à porter atteinte au droit au respect de la vie privée de la personne intéressée ; que, si le législateur a réservé à des agents habilités et soumis au respect du secret professionnel le pouvoir d'obtenir ces données et ne leur a pas conféré un pouvoir d'exécution forcée, il n'a assorti la procédure prévue par le 2° de l'article 216 d'aucune autre garantie ; qu'en particulier, le fait que les opérateurs et prestataires ne sont pas tenus de communiquer les données de connexion de leurs clients ne saurait constituer une garantie pour ces derniers ; que, dans ces conditions, le législateur n'a pas assorti la procédure prévue par le 2° de l'article 216 de garanties propres à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions ;

138. Considérant que le 2° de l'article 216 est contraire à la Constitution ;

- **Décision n° 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 Ier du titre III du livre Ier 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.