Statuts de l'association

Article 1
Titre de l'Association

Il est fondé entre les adhérents aux présents statuts une Association régie par la loi du premier juillet 1901 et le décret du 16 août 1901, ayant pour titre :

French Data Network
(Réseau Français de Données)

Article 2
But de l'Association

L'association a pour but : la promotion, l'utilisation et le développement des réseaux Internet et Usenet dans le respect de leur éthique en favorisant en particulier les utilisations à des fins de recherche ou d'éducation sans volonté commerciale.

Article 3
Siège social

Le siège social est fixé 16 rue de Cachy, 80090 Amiens.

Il pourra être transféré sur décision d'une Assemblée Générale.

Article 4
Membres de l'association

L'association se compose de membres d'honneur, membres bienfaiteurs et membres adhérents.

Sont membres d'honneur ceux qui ont été désignés comme tels par une Assemblée Générale Ordinaire ou Extraordinaire sur proposition du Bureau en raison des services éminents qu'ils ont rendus à l'association. Ils sont dispensés de cotisations.

Sont membres bienfaiteurs ceux qui versent la cotisation annuelle telle que fixée chaque année pour cette catégorie de membres par le Bureau.

Sont membres adhérents ceux qui versent la cotisation normale telle que fixée par le Bureau.

D'autre part, les membres adhérents peuvent être soit membres actifs, soit membres passifs. Sont dits membres actifs ceux qui assistent à l'Assemblée Générale Ordinaire annuelle, ou sont membres du Bureau, ou ont par un moyen ou par un autre participé à la vie de l'association autrement que par le paiement de la cotisation ou des divers abonnements possibles. Sont également membres actifs les membres bienfaiteurs. Sont, de facto, considérés comme actifs les membres participant à une Assemblée Générale Extraordinaire pour la durée de celle-ci.

Aux diverses cotisations est ajouté un droit d'entrée défini par le règlement intérieur.

Article 5
Admission

Pour faire partie de l'Association, il faut être agréé par le Bureau qui statue, lors de chacune de ses réunions, sur les demandes d'admission présentées.

Article 6
Radiation

La qualité de membre se perd par :

- la démission ;
- le décès de la personne physique ou la dissolution de la personne morale ;
- la radiation prononcée par le Bureau pour non-paiement de la cotisation ou pour motif grave, l'intéressé ayant été invité par lettre recommandée à se présenter devant le Bureau pour fournir des explications.

Article 7
Les ressources de l'Association

Elles comprennent :

- le montant des cotisations ;
- les subventions de l'État, des régions, des départements et des communes, ou de tout autre organisme public ;
- les sommes perçues en contrepartie des prestations fournies par l'Association ;
- toutes les autres ressources autorisées par les textes législatifs ou réglementaires.

Article 8
Le Bureau

L'Association est dirigée par un Bureau d'au moins deux membres élus pour une année par l'Assemblée Générale.

Les membres sont ré-éligibles.

En cas de vacances, le Bureau pourvoit provisoirement au remplacement des membres.

Il est procédé à leur remplacement définitif par l'Assemblée Générale suivante.

Article 9
Le Bureau, réunions

Le Bureau se réunit une fois au moins tous les six mois, sur convocation du Président ou à la demande du quart de ses membres.

Les réunions sont présidées par le Président ; le Bureau ne peut valablement délibérer que si les deux tiers de ses membres sont présents ou représentés.

En cas de partage, la voix du Président est prépondérante.

Article 10
Le Bureau, attributions

Le Bureau établit l'ordre du jour des Assemblées Générales et assure l'exécution des décisions de ces Assemblées. Il autorise toutes acquisitions, aliénations ou locations immobilières ainsi que les contrats à intervenir entre l'Association et les Collectivités ou Organismes publics qui lui apportent une aide financière. Ces autorisations sont faites uniquement à l'unanimité des membres du Bureau présents lors d'une réunion.

Il établit le budget de l'Association et il fixe le montant des cotisations.

Article 11
Le Bureau, composition

Le Bureau assure le bon fonctionnement de l'Association sous le contrôle de l'Assemblée Générale Ordinaire dont il prépare les réunions.

Le Président représente l'Association dans tous les actes de la vie civile et il conclut tout accord sous réserve des autorisations qu'il doit obtenir du Bureau dans les cas prévus aux présents statuts. Il a qualité pour présenter toute réclamation auprès de toutes administrations, notamment en matière fiscale, et pour ouvrir tout compte bancaire ou postal. Il agit en justice au nom de l'Association tant en demande (avec l'autorisation du Bureau s'il n'y a pas urgence) qu'en défense.

En cas d'empêchement, le Président est remplacé par le Trésorier qui dispose alors des mêmes pouvoirs.

Le Président peut accorder des délégations partielles de ses pouvoirs sous réserve, lorsqu'il s'agit de délégations d'une

certaine durée ou permanentes, d'en informer le Vice-Président.

Le Secrétaire est chargé en particulier de rédiger les procès-verbaux des réunions du Bureau et de l'Assemblée Générale et de tenir le registre prévu par la loi. En cas d'empêchement il est remplacé par le Président ou par un membre du Bureau désigné par le Président.

Le Trésorier est chargé de tenir ou de faire tenir sous son contrôle la comptabilité de l'Association. Il perçoit les recettes ; il effectue tout paiement sous réserve de l'autorisation du Président dans les cas éventuellement prévus par le Bureau.

En cas d'empêchement le Trésorier est remplacé par le Trésorier-adjoint, s'il y a lieu, ou par le Président, ou par un autre membre du Bureau désigné par le Président.

Vis-à-vis des organismes bancaires ou postaux, le Président, le Trésorier ou tout autre membre du Bureau désigné par le Président avec l'accord du Trésorier, ont pouvoir, chacun séparement, de signer tout moyen de paiement (chèques, virements, etc).

Article 12
Les Assemblées Générales

L'Assemblée Générale Ordinaire ou Extraordinaire comprend :

- les membres du Bureau ;
- tous les membres de l'Association, quel que soit le titre auquel ils sont affiliés, sous réserve qu'ils aient acquitté leur cotisation de l'année en cours et qu'ils soient membres de l'association depuis plus d'un an.

Les membres peuvent se faire représenter par leur conjoint ou par un autre membre.

Quinze jours au moins avant la date fixée par le Bureau, les membres de l'Association sont convoqués par les soins du Secrétaire.

L'ordre du jour est indiqué sur les convocations.

L'Assemblée est présidée par le Président.

Une Assemblée peut se tenir sous forme électronique conformément aux dispositions prévues par le règlement intérieur.

Article 13
Les Assemblées Générales Ordinaires

L'Assemblée Générale Ordinaire se réunit obligatoirement une fois par an au cours du premier trimestre.

Lors de cette réunion dite « annuelle », le Président soumet à l'Assemblée un rapport sur l'activité de l'Association.

Le Trésorier soumet le rapport financier comportant les comptes de l'exercice écoulé.

Il est ensuite procédé à l'élection des membres du Bureau et de son Président, celui-ci désignant parmi les membres du Bureau un Trésorier, un Secrétaire et un Vice-Président.

Il est ensuite procédé à l'examen des autres questions figurant à l'ordre du jour.

L'Assemblée Générale Ordinaire peut également être convoquée à tout moment à la demande du Président ou de la majorité des membres du Bureau.

Les décisions sont prises à la majorité absolue des suffrages exprimés par les membres présents ou représentés.

Les adhérents en faisant la demande par écrit, pourront se faire représenter par un membre de leur famille ou par un autre membre de l'Association, ou voter par correspondance (sous forme numérique sur le serveur de l'Association, ou par simple courrier).

Article 14
L'Assemblée Générale Extraordinaire

L'Assemblée Générale Extraordinaire se prononce sur les modifications à apporter aux Statuts et sur la dissolution de l'Association. Elle se réunit à la demande du Président ou de la majorité des membres du Bureau.

L'Assemblée Générale Extraordinaire ne peut se prononcer valablement que si les deux-tiers des membres actifs de l'Association sont présents ou représentés. Si plus de la moitié des membres à jour de leurs cotisations et membres depuis plus d'un an étaient absents, alors les décisions de l'Assemblée dont le degré d'urgence le permettraient seraient soumises à l'approbation, par vote électronique, de l'ensemble des adhérents. Ce vote, à approbation implicite, se ferait à la majorité absolue des membres de l'Association.

Les décisions sont prises à la majorité des deux-tiers des suffrages exprimés par les membres présents ou représentés.

L'Assemblée Générale Extraordinaire a également la possibilité de prendre toutes les décisions prévues pour l'Assemblée Générale Ordinaire, et ce dans les mêmes circonstances, c'est-à-dire sans minimum de représentation des membres, et à la majorité absolue des suffrages exprimés.

Si le quorum des deux-tiers des membres actifs n'était pas atteint, l'Assemblée serait, de facto, une Assemblée Générale Ordinaire, et statuerait sur les points de l'ordre du jour qui le permettent.

Article 15
Règlement intérieur

Un règlement intérieur est établi par le Bureau qui le fait approuver par l'Assemblée Générale.

Ce règlement éventuel est destiné à fixer les divers points non prévus par les Statuts, notamment ceux qui ont trait à l'administration interne de l'Association.

Article 16
Dissolution

En cas de dissolution prononcée par l'Assemblée Générale Extraordinaire, un ou plusisuers liquidateurs sont nommés par celle-ci.

L'actif, s'il y a lieu, est dévolu par cette Assemblée à une ou plusieurs Associations ayant un objet similaire ou à tout établissement à but social ou culturel de son choix.

Fait à Amiens le 31 mars 2013
en 2 exemplaires originaux.

Signatures :
Le président : Arnaud Luquin
Le trésorier : Simon Descarpentries

Chemin :

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

Chapitre III : Dispositions relatives au renseignement

Article 20

ELI: https://www.legifrance.gouv.fr/eli/loi/2013/12/18/DEFX1317084L/jo/article_20
Alias: https://www.legifrance.gouv.fr/eli/loi/2013/12/18/2013-1168/jo/article_20

I. — Le livre II du même code est ainsi modifié :
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. 246-1.-Pour les finalités énumérées à l'article L. 241-2, 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.
« Art. L. 246-2.-I. — Les informations ou documents mentionnés à l'article L. 246-1 sont sollicités par les agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget, chargés des missions prévues à l'article L. 241-2.
« II. — Les demandes des agents sont motivées et soumises à la décision d'une personnalité qualifiée placée auprès du Premier ministre. Cette personnalité est désignée pour une durée de trois ans renouvelable par la Commission nationale de contrôle des interceptions de sécurité, sur proposition du Premier ministre qui lui présente une liste d'au moins trois noms. Des adjoints pouvant la suppléer sont désignés dans les mêmes conditions. La personnalité qualifiée établit un rapport d'activité annuel adressé à la Commission nationale de contrôle des interceptions de sécurité. Ces décisions, accompagnées de leur motif, font l'objet d'un enregistrement et sont communiquées à la Commission nationale de contrôle des interceptions de sécurité.
« 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.
« Art. L. 246-4.-La Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent au dispositif de recueil des informations ou documents mis en œuvre en vertu du présent chapitre, afin de procéder à des contrôles visant à s'assurer du respect des conditions fixées aux articles L. 246-1 à L. 246-3. En cas de manquement, elle adresse une recommandation au Premier ministre. Celui-ci fait connaître à la commission, dans un délai de quinze jours, les mesures prises pour remédier au manquement constaté.
« 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 interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des informations ou documents transmis.
« Art. L. 246-5.-Les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs et personnes

mentionnées à l'article L. 246-1 pour répondre à ces demandes font l'objet d'une compensation financière de la part de l'Etat. » ;
3° Les articles L. 222-2, L. 222-3 et L. 243-12 sont abrogés ;
4° A la première phrase du premier alinéa de l'article L. 243-7, les mots : « de l'article L. 243-8 et au ministre de l'intérieur en application de l'article L. 34-1-1 du code des postes et des communications électroniques et de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique » sont remplacés par les références : « des articles L. 243-8, L. 246-3 et L. 246-4 » ;
5° A l'article L. 245-3, après le mot : « violation », sont insérées les références : « des articles L. 246-1 à L. 246-3 et ».
II. — L'article L. 34-1-1 du code des postes et des communications électroniques est abrogé.
III. — Le II bis de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est abrogé.
IV. — Le présent article entre en vigueur le 1er janvier 2015.

Liens relatifs à cet article

Cite:

Loi n° 2004-575 du 21 juin 2004 - art. 6 (M)
Code des postes et des communications électroni... - art. L34-1 (M)
Code des postes et des communications électroni... - art. L34-1-1 (Ab)

Cité par:

DÉCISION du 26 décembre 2014, v. init.
DÉCISION du 26 décembre 2014, v. init.
SAISINE du 25 juin 2015 - art., v. init.

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

PREMIER MINISTRE

Décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion

NOR : *PRMD1422750D*

Publics concernés : *administrations, opérateurs de communications électroniques et personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques, 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.*

Objet : *procédure applicable à l'accès, au titre de la sécurité nationale, de la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France ou de la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous, aux données de connexion détenues par les opérateurs de télécommunications électroniques.*

Entrée en vigueur : *le texte entre en vigueur le 1er janvier 2015.*

Notice : *le décret crée un chapitre intitulé « Accès administratif aux données de connexion » au titre IV du livre II de la partie réglementaire du code de la sécurité intérieure. Il définit les données de connexion pouvant être recueillies et dresse la liste des services dont les agents individuellement désignés et dûment habilités peuvent demander à accéder aux données de connexion. Il prévoit les conditions de désignation et d'habilitation de ces agents ainsi que celles de désignation de la personnalité qualifiée placée auprès du Premier ministre à laquelle sont soumises les demandes d'accès en temps différé. Il précise également les modalités de présentation des demandes d'accès en temps différé comme en temps réel, de conservation de ces demandes ainsi que de décision. En cas de décision favorable, il prévoit les conditions de transmission et de conservation des données recueillies. Il fixe les modalités de transmission des demandes à la Commission nationale de contrôle des interceptions de sécurité ainsi que celles du suivi général et du contrôle du dispositif par la commission. Enfin, l'indemnisation des coûts supportés par les opérateurs de communications électroniques, les fournisseurs d'accès à Internet et les hébergeurs lors de la mise en œuvre de la procédure est prévue. Le décret se substitue, en s'en inspirant, aux dispositions jusqu'alors prévues aux articles R. 10-15 à R. 10-21 du code des postes et des communications électroniques et à celles du chapitre II du décret n° 2011-219 du 25 février 2011.*

Références : *le présent décret est pris pour l'application de l'article L. 246-4 du code de la sécurité intérieure. Le code de la sécurité intérieure, le code des postes et des communications électroniques et le décret n° 2011-219 du 25 février 2011, modifiés par le présent décret, peuvent être consultés, dans leur rédaction issue de cette modification, sur le site Légifrance (http://www.legifrance.gouv.fr).*

Le Premier ministre,

Sur le rapport du ministre des finances et des comptes publics, du ministre de la défense, du ministre de l'intérieur et du ministre de l'économie, de l'industrie et du numérique,

Vu le code de la sécurité intérieure, notamment ses articles L. 246-1 et suivants ;

Vu le code des postes et des communications électroniques, notamment ses articles L. 34-1 et R. 10-12 et suivants ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 26 et 34 ;

Vu la loi n° 2004-575 du 21 juin 2004 modifiée pour la confiance dans l'économie numérique, notamment son article 6 ;

Vu la 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, notamment ses articles 20 et 57 ;

Vu le 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 ;

Vu l'avis de la Commission nationale de contrôle des interceptions de sécurité en date du 23 octobre 2014 ;

Vu l'avis de l'Autorité de régulation des communications électroniques et des postes en date du 18 novembre 2014 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 4 décembre 2014 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

Art. 1er. – Le livre II de la partie réglementaire du code de la sécurité intérieure est ainsi modifié :

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

2° Au chapitre Ier du titre IV, il est créé deux articles R. 241-1 et R. 241-2 ainsi rédigés :

« *Art. R. 241-1.* – Le groupement interministériel de contrôle est un service du Premier ministre chargé des interceptions de sécurité et de l'accès administratif aux données de connexion dans les conditions fixées aux chapitres II et VI du présent titre.

« *Art. R. 241-2.* – Le directeur du groupement interministériel de contrôle est nommé par arrêté du Premier ministre. » ;

3° Au titre IV, il est ajouté un chapitre VI ainsi rédigé :

« Chapitre VI

« Accès administratif aux données de connexion

« *Art. R. 246-1.* – Pour l'application de l'article L. 246-1, les informations et les documents pouvant faire, à l'exclusion de tout autre, l'objet d'une demande de recueil sont 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.

« *Art. R. 246-2.* – I. – Pour l'application du I de l'article L. 246-2, les services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget dont les agents peuvent solliciter les informations et les documents mentionnés à l'article L. 246-1 sont :

« 1° Au ministère de l'intérieur :

« *a)* La direction générale de la sécurité intérieure ;

« *b)* A la direction générale de la police nationale :

« – l'unité de coordination de la lutte antiterroriste ;

« – la direction centrale de la police judiciaire ;

« – à la direction centrale de la sécurité publique : le service central du renseignement territorial ; les services départementaux du renseignement territorial et les sûretés départementales au sein des directions départementales de la sécurité publique ;

« – à la direction centrale de la police aux frontières : l'office central pour la répression de l'immigration irrégulière et de l'emploi d'étrangers sans titre au sein de la sous-direction de l'immigration irrégulière et des services territoriaux ;

« *c)* A la direction générale de la gendarmerie nationale :

« – à la direction des opérations et de l'emploi : la sous-direction de la police judiciaire ; la sous-direction de l'anticipation opérationnelle ;

« – au pôle judiciaire : le service technique de recherches judiciaires et de documentation ;

« – les sections de recherches ;

« *d)* A la préfecture de police :

« – la direction du renseignement ;

« – la direction régionale de la police judiciaire ;

« – à la direction de la sécurité de proximité de l'agglomération parisienne : le service transversal d'agglomération des événements au sein de la sous-direction des services spécialisés de l'agglomération ; la cellule de suivi du plan de lutte contre les bandes au sein de la sous-direction de la police d'investigation territoriale ; la sûreté régionale des transports au sein de la sous-direction régionale de la police des transports ; les sûretés territoriales au sein des directions territoriales de sécurité de proximité ;

« 2° Au ministère de la défense :

« *a)* La direction générale de la sécurité extérieure ;

« *b)* La direction de la protection et de la sécurité de la défense ;

« *c)* La direction du renseignement militaire ;

« 3° Au ministère des finances et des comptes publics :

« *a)* Le service à compétence nationale dénommé « direction nationale du renseignement et des enquêtes douanières » ;

« *b)* Le service à compétence nationale dénommé « traitement du renseignement et action contre les circuits financiers clandestins ».

« II. – Seuls peuvent solliciter ces informations et ces documents les agents individuellement désignés et dûment habilités par le directeur dont ils relèvent.

« *Art. R. 246-3.* – Afin de permettre la désignation de la personnalité qualifiée mentionnée au II de l'article L. 246-2 et de ses adjoints, le Premier ministre transmet à la Commission nationale de contrôle des interceptions de sécurité, pour chaque poste à pourvoir, une liste d'au moins trois personnes choisies en raison de leur compétence et de leur impartialité. Ces propositions sont motivées. Elles sont adressées à la commission au moins trois mois avant le terme du mandat de la personnalité qualifiée et de ses adjoints. La commission désigne, au sein des listes, la personnalité qualifiée et ses adjoints deux mois au plus tard après avoir reçu les propositions.

« Toute décision désignant la personnalité qualifiée et ses adjoints est notifiée sans délai au Premier ministre par la commission et publiée au *Journal officiel* de la République française.

« Les adjoints de la personnalité qualifiée sont au maximum au nombre de quatre.

« *Art. R. 246-4.* – Les demandes de recueil d'informations ou de documents prévues à l'article L. 246-2 comportent :

« *a)* Le nom, le prénom et la qualité du demandeur ainsi que son service d'affectation et l'adresse de celui-ci ;

« *b)* La nature précise des informations ou des documents dont le recueil est demandé et, le cas échéant, la période concernée ;

« *c)* La date de la demande et sa motivation au regard des finalités mentionnées à l'article L. 241-2.

« *Art. R. 246-5.* – Le Premier ministre enregistre et conserve pendant une durée maximale de trois ans, dans un traitement automatisé qu'il met en œuvre, les demandes des agents et les décisions de la personnalité qualifiée ou de ses adjoints.

« Ces demandes et ces 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 interceptions de sécurité un procès-verbal certifiant que l'effacement a été effectué.

« *Art. R. 246-6.* – Les demandes approuvées par la personnalité qualifiée ou par ses adjoints sont adressées par le groupement interministériel de contrôle, sans les éléments mentionnés aux *a* et *c* de l'article R. 246-4, aux opérateurs et aux personnes mentionnés à l'article L. 246-1. Ces derniers transmettent sans délai les informations ou les documents demandés au groupement interministériel de contrôle, qui les met à disposition de l'auteur de la demande pour exploitation.

« La transmission des informations ou des documents par les opérateurs et les personnes mentionnés à l'article L. 246-1 au groupement interministériel de contrôle est effectuée selon des modalités assurant leur sécurité, leur intégrité et leur suivi.

« Le Premier ministre enregistre et conserve pendant une durée maximale de trois ans, dans un traitement automatisé qu'il met en œuvre, les informations ou les documents transmis par les opérateurs et les personnes mentionnés à l'article L. 246-1. Ces informations ou ces documents sont automatiquement effacés du traitement dans les conditions prévues à l'article R. 246-5.

« *Art. R. 246-7.* – Les demandes de recueil d'informations ou de documents, impliquant sollicitation du réseau et transmission en temps réel, prévues à l'article L. 246-3 comportent, outre leur date et leur motivation au regard des finalités mentionnées à l'article L. 241-2, la nature précise des informations ou des documents dont le recueil est demandé et la durée de ce recueil.

« Les demandes des ministres ou des personnes spécialement désignées par eux et les décisions du Premier ministre ou des personnes spécialement désignées par lui sont enregistrées, conservées et effacées dans les conditions prévues à l'article R. 246-5.

« Les demandes approuvées par le Premier ministre ou par les personnes spécialement désignées par lui sont adressées par le groupement interministériel de contrôle, sans leur motivation, aux opérateurs et aux personnes mentionnés à l'article L. 246-1.

« La sollicitation du réseau prévue à l'article L. 246-3 est effectuée par l'opérateur qui exploite le réseau. Les informations ou les documents demandés sont transmis, enregistrés, conservés et effacés dans les conditions prévues à l'article R. 246-6.

« *Art. R. 246-8.* – 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.

« L'autorité ayant approuvé une demande de recueil d'informations ou de documents fournit à la commission tous éclaircissements que celle-ci sollicite sur cette demande.

« *Art. R. 246-9.* – Les coûts identifiables et spécifiques supportés par les opérateurs et les personnes mentionnés à l'article L. 246-1 pour la transmission des informations ou des documents font l'objet d'un remboursement par l'Etat par référence aux tarifs et selon des modalités fixés par un arrêté des ministres chargés de la sécurité intérieure, de la défense, de l'économie, du budget et des communications électroniques. » ;

4° La ligne :

R. 242-1 à R. 244-6	Résultant du décret n° 2013-1113 relatif aux dispositions des livres I^er^, II, IV et V de la partie réglementaire du code de la sécurité intérieure (Décrets en Conseil d'Etat et décrets simples)

figurant dans le tableau des articles R. 285-1, R. 286-1 et R. 287-1 est remplacée par les lignes suivantes :

R. 241-1 et R. 241-2	Résultant du décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion
R. 242-2, R. 242-4 à R. 242-8 et R. 244-1 à R. 244-6	Résultant du décret n° 2013-1113 relatif aux dispositions des livres Ier, II, IV et V de la partie réglementaire du code de la sécurité intérieure (Décrets en Conseil d'Etat et décrets simples)
R. 246-1 à R. 246-9	Résultant du décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion

5° La ligne :

R. 242-1 à R. 242-3	Résultant du décret n° 2013-1113 relatif aux dispositions des livres Ier, II, IV et V de la partie réglementaire du code de la sécurité intérieure (Décrets en Conseil d'Etat et décrets simples)

figurant dans le tableau de l'article R. 288-1 est remplacée par les lignes suivantes :

R. 241-1 et R. 241-2	Résultant du décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion
R. 242-2	Résultant du décret n° 2013-1113 relatif aux dispositions des livres Ier, II, IV et V de la partie réglementaire du code de la sécurité intérieure (Décrets en Conseil d'Etat et décrets simples)
R. 246-1 à R. 246-9	Résultant du décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion

Art. 2. – I. – Sont abrogés :

1° Les articles R. 242-1 et R. 242-3 du code de la sécurité intérieure ;

2° Les articles R. 10-15 à R. 10-21 du code des postes et des communications électroniques ;

3° Le chapitre II du décret du 25 février 2011 susvisé.

II. – La seconde phrase de l'article R. 10-22 du code des postes et des communications électroniques est supprimée.

III. – A l'article 12 du décret du 25 février 2011 susvisé, le mot : « 10 » est supprimé.

Art. 3. – Le présent décret s'applique sur l'ensemble du territoire de la République.

Il entre en vigueur le 1er janvier 2015.

Toutefois, les délais mentionnés à l'article R. 246-3 du code de la sécurité intérieure ne sont pas applicables à la première désignation, après l'entrée en vigueur du présent décret, de la personnalité qualifiée et de ses adjoints mentionnés au II de l'article L. 246-2 du même code.

Art. 4. – Le ministre des finances et des comptes publics, le ministre de la défense, le ministre de l'intérieur, le ministre de l'économie, de l'industrie et du numérique et la ministre des outre-mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait le 24 décembre 2014.

MANUEL VALLS

Par le Premier ministre :

Le ministre des finances et des comptes publics,
MICHEL SAPIN

Le ministre de la défense,
JEAN-YVES LE DRIAN

Le ministre de l'intérieur,
BERNARD CAZENEUVE

Le ministre de l'économie, de l'industrie et du numérique,
EMMANUEL MACRON

La ministre des outre-mer,
GEORGE PAU-LANGEVIN

Conseil d'État
Section du contentieux

Requête introductive d'instance

introduite

PAR

1. **French Data Network (Réseau de données français)**, dite FDN.
   Association régie par la loi du 1er juillet 1901 établie 16 rue de Cachy, 80090 Amiens, enregistrée en préfecture de la Somme sous le numéro W751107563, opérateur déclaré auprès de l'ARCEP sous la référence 07/1149, prise en la personne de son président M. Fabien Sirjean.
   Tel. : 06 36 18 91 00
   Mail : `president@fdn.fr` / `buro@fdn.fr`
2. **La Quadrature du Net**
   Association régie par la loi du 1er juillet 1901 établie au 60 rue des Orteaux 75019, Paris, enregistrée en préfecture de police de Paris sous le numéro W751218406, prise en la personne de son président M. Philippe Aigrain.
   Tel. 06 73 60 88 43
   Mail : `contact@laquadrature.net`
3. **Fédération des fournisseurs d'accès à Internet associatifs**, dite Fédération FDN (FFDN).
   Fédération régie par la loi du 1er juillet 1901 établie 16 rue de Cachy, 80090 Amiens, enregistrée en préfecture de la Somme sous le numéro W751210904, regroupant 27 fournisseurs d'accès associatifs français, déclarés auprès de l'ARCEP, et un fournisseur d'accès associatif belge déclaré auprès du régulateur, prise en la personne de son président M. Benjamin Bayart.
   Tel : 06 60 24 24 94
   Mail : `contact@ffdn.org`

CONTRE

Le décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion publié au Journal officiel de la République française n° 298 du 26 décembre 2014, p. 22224.

1. FAITS

La loi nº 2013-1168 de programmation militaire du 18 novembre 2013 (LPM) établit les objectifs de la politique de défense française pour les années 2014 à 2019. Son article 20 a, d'une part, créé un chapitre VI « Accès administratif aux données de connexion » au sein du titre IV du livre II du code de la sécurité intérieure (CSI) contenant les articles L. 246-1 à 5 CSI. Il a, d'autre part, abrogé les articles L. 222-2, L. 222-3 et L. 243-12 CSI ainsi que l'article 6 II bis de la loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) et l'article L. 34-1-1 du code des postes et des communications électroniques (CPCE).

L'article L. 246-4 CSI créé par la LPM, actuellement en vigueur, dispose que :

> *« La Commission nationale de contrôle des interceptions de sécurité dispose d'un accès permanent au dispositif de recueil des informations ou documents mis en œuvre en vertu du présent chapitre, afin de procéder à des contrôles visant à s'assurer du respect des conditions fixées aux articles L. 246-1 à L. 246-3. En cas de manquement, elle adresse une recommandation au Premier ministre. Celui-ci fait connaître à la commission, dans un délai de quinze jours, les mesures prises pour remédier au manquement constaté.*
>
> *« Les modalités d'application du présent article sont fixées par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des informations ou documents transmis. »*

Le décret visé à cet article est le décret nº 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion publié au Journal officiel de la République française nº 298 du 26 décembre 2014, p. 22.224.

C'est la décision attaquée.

2. DISCUSSION — Intérêt à agir

2.1. French Data Network

FDN est une association loi 1901, et est un fournisseur d'accès à Internet. Elle existe, et exerce son activité, depuis 1992, ce qui en fait le plus ancien fournisseur d'accès à Internet encore en activité. Elle regroupe 450 adhérents et est administrée de manière entièrement bénévole. Elle ne fournit d'accès à Internet qu'à ses membres. Son intérêt à agir, en l'espèce est donc double.

D'une part, en tant qu'opérateur d'un réseau de communication ouvert au public, déclaré auprès de l'ARCEP, parce que le décret attaqué lui est applicable directement. À ce titre FDN fournit également un certain nombre de services (courrier électronique, hébergement de sites web ou de serveurs, etc) à ceux de ses membres qui en ont fait le choix.

D'autre part, en tant qu'association, représentant ses membres, y compris ceux auxquels elle fournit un accès à Internet. Ces abonnés sont concernés au premier chef par la conservation des données de connexion, et par les accès de l'administration à ces données.

L'intérêt à agir de FDN a été reconnu par le Conseil d'État dans l'affaire n° 342405, par exemple.

2.2. La Quadrature du Net

L'objet général de la Quadrature du Net est la défense des droits fondamentaux dans l'environnement numérique. À ce titre, elle intervient dans les débats réglementaires touchant au droit de l'Internet au niveaux français et européen, notamment en développant des analyses juridiques, en proposant et en évaluant des amendements au cours des procédures législatives.

Dès 2008 et 2009, LQDN s'était illustrée comme l'un « des fers de lance de l'opposition à loi » HADOPI, selon l'expression du journal Le Figaro[1]. Elle avait à cette occasion porté de nombreux arguments juridiques plus tard validés dans la décision n° 2009-580 DC du Conseil constitutionnel du 10 juin 2009. Son combat contre les excès du droit d'auteur

[1] `https://www.laquadrature.net/fr/le-figaro-bataille-politique-autour-de-la-loi-antipiratage`

l'a également conduite à mener campagne contre le projet d'accord multilatéral ACTA, rejeté par le Parlement européen à l'été 2012.

L'un des axes fort de ses positions est la défense d'une protection judiciaire des droits fondamentaux sur Internet, et notamment la liberté d'expression et de communication. À ce titre, elle s'oppose à la délégation de la répression des infractions aux acteurs privés ou administratifs. En 2009, elle avait dans ce but proposé et défendu l'amendement dit « 138 » lors de l'examen du Paquet Télécom au Parlement européen. Ces derniers mois, elle s'est également illustrée dans les débats parlementaires français sur différents projets et propositions de loi tendant à étendre les obligations des hébergeurs en matière de surveillance des contenus, pointant le risque de censure extrajudiciaire qu'emportaient de telles mesures.

Cette défense de l'État de droit l'a évidemment conduite à se mobiliser sur les questions de vie privée et de surveillance des communications sur Internet. Au niveau européen, elle mène par exemple campagne sur le projet de règlement relatif à la protection des données personnelles. Au niveau français, LQDN s'est notamment illustrée par son opposition à la loi de programmation militaire (LPM) adoptée fin 2013. Elle participe depuis à l'Observatoire des Libertés Numériques, créé suite à la mobilisation de la société civile contre l'article 20 de la LPM, aux côtés entre autres de la Ligue des Droits de l'Homme et du Syndicat de la Magistrature. Récemment, elle a encore été auditionnée par le Conseil d'État le 28 janvier 2014 en vue de l'élaboration de son étude annuelle pour l'année 2014 intitulée « Le numérique et les droits fondamentaux ».

Enfin, les statuts de l'association lui confèrent la possibilité d'ester en justice – possibilité qu'elle entend exercer pour la première fois à l'occasion de ce recours. Cela étant, elle a déjà eu l'occasion d'intervenir auprès de juridictions. En 2011, elle était intervenue auprès du Conseil constitutionnel au travers d'un mémoire en « amicus curiae » pour pointer le caractère disproportionné et dès lors inconstitutionnel des mesures de blocage administratif de sites inscrit à l'article 4 de la loi LOPPSI[2]. Actuellement, elle participe à une tierce intervention d'une coalition d'ONG européennes auprès de la Cour européenne des droits de l'Homme, à l'occasion du recours de plusieurs associations britanniques contre le programme de surveillance d'Internet TEMPORA, révélé par Edward Snowden[3].

Ainsi, La Quadrature du Net introduit la présente requête non seulement en conformité avec ses statuts, mais aussi en pleine cohérence avec ses activités.

2.3. Fédération des fournisseurs d'accès à Internet associatifs

La Fédération FDN regroupe 28 fournisseurs d'accès à Internet associatifs, 27 sont des associations de droit français (loi de 1901 ou droit spécifique d'Alsace Moselle, selon), la 28^{e} étant une association de droit belge. Toutes ces associations sont gérées de manière

[2] http://www.laquadrature.net/files/20110214_La%20Quadrature%20du%20Net_Amicus%20curiae%20LOPPSI2.pdf

[3] https://www.laquadrature.net/fr/la-quadrature-sengage-dans-la-lutte-juridictionnelle-contre-la-surveillance-de-masse

bénévole et représentent, toutes ensemble, près de 2000 adhérents. FDN est une des associations membres, et fondatrice, de la Fédération FDN. Les associations membres de la Fédération FDN sont toutes signataires d'une charte par laquelle elles prennent des engagements éthiques et techniques.

Ici encore, l'intérêt à agir de la Fédération FDN est double.

D'une part, en tant que représentant de 28 opérateurs, tous déclarés auprès du régulateur national, et presque tous de droit français, donc concernés par le décret attaqué qui leur est applicable.

D'autre part, en tant que représentant, au travers de ses membres, de l'ensemble des abonnés et adhérents de ses associations membres, concernés par la conservation des données de connexion, l'intrusion qu'elle représente dans leur vie privée, et les accès de l'administration à ces données.

3. DISCUSSION — Légalité externe

La décision attaquée est entachée de vices d'incompétence et de procédure.

3.1. Le décret attaqué est entaché d'incompétence matérielle.

Le décret est entaché d'incompétence *ratione materiae* en ce qu'il comporte des dispositions dont la substance outrepasse largement le champ de l'article L. 246-4 CSI créé par la LPM et sort du champ du pouvoir réglementaire autonome.

L'article L. 246-4 CSI précité, sur le fondement duquel le décret attaqué est adopté, ne porte que sur le rôle alloué à la Commission nationale de contrôle des interceptions de sécurité (CNCIS) dans le contrôle qu'elle opère sur le recueil d'informations opéré en vertu du chapitre VI créé par l'article 20 de la loi de programmation militaire du 18 novembre 2013. Il confie au pouvoir réglementaire le soin d'établir les conditions dans lesquelles la CNCIS peut effectuer ce contrôle.

La notice présentant le décret[1], précise que le décret « définit les données de connexion pouvant être recueillies et dresse la liste des services dont les agents individuellement désignés et dûment habilités peuvent demander à accéder aux données de connexion ». Cette notice décrit parfaitement l'objet des dispositions du décret attaqué, lesquelles excèdent le champ de l'article L. 246-4 CSI pour combler les lacunes des articles L. 246-1 à 3 et L. 246-5.

Les dispositions du décret attaqué dépassent donc très largement la compétence du pouvoir réglementaire. En cela, le décret attaqué est entaché d'incompétence matérielle et devra être annulé.

[1] `http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029958091&categorieLien=id`, texte du décret joint à la procédure.

3.2. Le décret attaqué est entaché de vices de procédure.

Le décret est vicié en ce que le pouvoir réglementaire n'a pas respecté la procédure qui s'imposait à son adoption.

3.2.1. Le décret attaqué n'a pas été notifié à la Commission européenne.

La directive 98/34/CE du 22 juin 1998 modifiée, en son article 1er 2) définit la notion de « service de la société de l'information » comme :

> *« tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services »*

L'article 1er 5) définit la « règle relative aux services » comme :

> *« une exigence de nature générale relative à l'accès aux activités de services visées au point 2 et à leur exercice, notamment les dispositions relatives au prestataire de services, aux services et au destinataire de services, à l'exclusion des règles qui ne visent pas spécifiquement les services définis au même point »*

L'article 1er 11) définit la « règle technique » comme :

> *« une spécification technique ou autre exigence ou une règle relative aux services, y compris les dispositions administratives qui s'y appliquent, dont l'observation est obligatoire de jure ou de facto, pour la commercialisation, la prestation de services, l'établissement d'un opérateur de services ou l'utilisation dans un État membre ou dans une partie importante de cet État, de même que, sous réserve de celles visées à l'article 10, les dispositions législatives, réglementaires et administratives des États membres interdisant (...) de fournir ou d'utiliser un service ou de s'établir comme prestataire de services »*

En l'espèce, les mesures créées par le décret sont bien des règles techniques au sens de la directive. En effet, il s'agit bien de dispositions administratives dont l'observation est obligatoire et s'appliquant à des services tels que définis par la directive puisque sont notamment visés les hébergeurs, tels que définis à l'article 6, I, 1° de la LCEN et prestataires de services de la société de l'information par excellence.

Dès lors, le projet de décret devait être notifié à la Commission européenne, l'article 8 de la directive 98/34/CE disposant quant à lui que :

> *« Sous réserve de l'article 10, les États membres communiquent immédiatement à la Commission tout projet de règle technique, sauf s'il s'agit d'une simple transposition intégrale d'une norme internationale ou européenne, auquel cas une simple information quant à la norme concernée suffit. »*

Ne s'agissant ni d'un cas visé à l'article 10 ni d'une transposition intégrale d'une norme internationale ou européenne, le décret devait être notifié à la Commission européenne

conformément à la procédure établie par la directive 98/34/CE. Cette interprétation de la directive 98/34/CE est d'ailleurs conforme à la solution adoptée par le Conseil d'État dans son arrêt du 10 juin 2013 rendu dans l'affaire n° 327375.

Le Gouvernement ayant manqué de le notifier à la Commission européenne, le décret attaqué n'a pas été adopté conformément aux dispositions susvisées de la directive 98/34 et doit donc être annulé.

3.2.2. Aucune étude d'impact n'a été réalisée antérieurement à l'adoption du décret attaqué.

D'après la circulaire du 17 février 2011 relative à la simplification des normes concernant les entreprises et les collectivités territoriales :

> *« L'élaboration de tout projet de loi, d'ordonnance, de décret ou d'arrêté comportant des mesures concernant les entreprises, c'est-à-dire susceptibles d'avoir une incidence sur elles, tout particulièrement sur les petites et moyennes entreprises et sur les entreprises du secteur industriel, appelle une analyse d'impact circonstanciée.*
>
> *« S'agissant des projets d'ordonnance, de décret et d'arrêté, cette évaluation préalable sera retracée dans la fiche d'impact de l'annexe III de la présente circulaire.*
>
> *« Le commissaire à la simplification **doit être saisi** du projet de texte et de l'analyse d'impact correspondante :*
>
> *[...]*
>
> *« — s'agissant des projets de décret en Conseil d'État ou d'ordonnance, au plus tard concomitamment à la saisine des instances obligatoirement consultées si le projet entre dans leur champ de compétence et préalablement à l'organisation d'une réunion interministérielle ou saisine du cabinet du Premier ministre pour arbitrage et, en toute hypothèse, à la saisine du Conseil d'État. »*

Cette circulaire, adoptée par le Premier ministre, crée une obligation pour l'ensemble des composantes du gouvernement et de l'administration non seulement d'élaborer une fiche d'impact mais de saisir le commissaire à la simplification du projet de décret, à tout le moins lors de la saisine du Conseil d'État.

Cette obligation s'applique lorsque sont en cause des mesures concernant les entreprises et tout particulièrement des petites et moyennes entreprises. Ce qui est le cas en l'espèce puisque, comme en témoigne l'existence même d'associations comme celles de la FFDN, les destinataires du décret sont pour un très grand nombre, et plus encore pour ce qui concerne les hébergeurs, des petites et moyennes entreprises.

Le décret attaqué, en ce qu'il comporte des mesures que de nombreux hébergeurs et fournisseurs d'accès – dont un grand nombre sont des petites et moyennes entreprises, voire des associations – doivent respecter, devait être précédé d'une étude d'impact ainsi que d'une saisine du commissaire à la simplification. Or, encore une fois, il n'en a rien été.

Ainsi, le décret a été adopté en contradiction des dispositions contraignantes précitées et devra donc être annulé.

4. DISCUSSION - Légalité interne

La décision attaquée doit au surplus être annulée en ce qu'elle est contraire au droit de l'Union européenne et à la Convention européenne des droits de l'Homme, à la loi et aux principes généraux du droit.

À titre liminaire, il doit d'ores et déjà être précisé que l'application de la Charte des droits fondamentaux de l'Union européenne à la décision attaquée appelle à ce qu'une question préjudicielle soit adressée à la Cour de justice de l'Union européenne. Par ailleurs, les associations requérantes formeront une question prioritaire de constitutionnalité dans un mémoire séparé qui sera communiqué ultérieurement.

4.1. Le décret attaqué est contraire à la Charte des droits fondamentaux et à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

La Charte des droits fondamentaux de l'Union européenne dispose que :

« Article 7 — Respect de la vie privée et familiale

« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

« Article 8 — Protection des données à caractère personnel

« Toute personne a droit à la protection des données à caractère personnel la concernant.

« Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

« Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

« Article 11 — Liberté d'expression et d'information

« 1.Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.

> *« 2. La liberté des médias et leur pluralisme sont respectés.*
> *[...]*
> *« Article 52 — Portée et interprétation des droits et des principes*
> *« Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui. »*

Dans son arrêt du 8 avril 2014 (*Digital Rights Ireland*, C-293/12), la grande chambre de la Cour de justice de l'Union européenne (CJUE) a invalidé la directive 2006/24/CE relative à la conservation des données par les opérateurs de communications électroniques, la jugeant non conforme à la Charte des droits fondamentaux de l'Union européenne (la Charte).

Pour déclarer cette directive invalide, la CJUE a d'abord estimé que l'obligation généralisée de conservation des données de connexion ainsi que l'accès qui en était donné aux autorités nationales constituaient des ingérences dans les droits fondamentaux au respect de la vie privée et familiale et à la protection des données à caractère personnel reconnus aux articles 7 et 8 de la Charte. Comme l'a décidé la CJUE :

> *« (...) 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. » (§ 58)*

Suite à l'invalidation de la directive 2006/24, le droit de l'Union européenne applicable est désormais celui de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive dite « ePrivacy »). Cette directive dispose dans son article 15 que :

> *« Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue* ***une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique****, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant*

la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne. »

Ainsi, la décision attaquée doit être conforme à la Charte des droits fondamentaux, à la CEDH ainsi qu'aux principes généraux du droit de l'Union européenne.

Lue à la lumière de l'arrêt du 8 avril 2014 rendu par la CJUE, et en particulier de ses paragraphes 57 à 59, l'article 15 de la directive 2002/58/CE tend à invalider le principe même d'une obligation de conservation des données pour les 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 »*, pour privilégier des dispositifs de conservation de données ciblées, tant en termes temporels que s'agissant des personnes concernées (conservation sur injonction).

Or, le présent décret fournit à l'administration un accès à un ensemble de données collectées dans le cadre d'un dispositif de collecte généralisée des données de connexion, y compris pour les personnes pour lesquelles il n'existe aucune suspicion d'un lien direct ou indirect avec des infractions graves. **Tout comme la directive 2006/24/CE, le décret échoue à apporter les garanties requises par les articles 7, 8, 11 et 52, paragraphe 1 de la Charte des droits fondamentaux tels qu'interprétés par l'arrêt du 8 avril 2014 de la CJUE**. Dès lors, le décret attaqué est contraire au droit de l'Union européenne.

En tout état de cause, si le Conseil d'État s'interroge sur la portée qu'il convient de donner à l'arrêt de la CJUE du 8 avril 2014, la lettre et l'esprit de la procédure du renvoi préjudiciel devraient le conduire à poser à la CJUE la question de savoir si le droit de l'Union européenne doit être interprété en ce sens qu'il prohibe tout dispositif de collecte généralisée des données de connexion pour l'ensemble des utilisateurs d'Internet, y compris ceux pour lesquels il n'existe aucune suspicion d'infraction.

De plus, bien que, dans son arrêt du 8 avril 2014, la CJUE se soit contentée d'apprécier la validité de la directive au regard des articles 7 et 8 de la Charte, la Cour n'a pas exclu que les dispositions visées constituent également une ingérence dans l'exercice de la liberté d'expression, telle que reconnue à l'article 11 de la Charte.

En cela, la CJUE s'est inscrite dans le sillage d'une jurisprudence bien établie de la Cour européenne des droits de l'homme relative tant à l'article 8 qu'à l'article 10 de la Convention européenne de sauvegarde des droits de l'homme et du citoyen (Conv. EDH).

La Conv. EDH dispose en effet que :

« Article 8 — Droit au respect de la vie privée et familiale

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

« 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale,

ou à la protection des droits et libertés d'autrui.

« Article 10 — Liberté d'expression

« 1. Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontière. Le présent article n'empêche pas les États de soumettre les entreprises de radiodiffusion, de cinéma ou de télévision à un régime d'autorisations.

« 2. L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire. »

De jurisprudence constante, la Cour européenne des droits de l'homme (Cour EDH) considère que toute loi instaurant des mesures de surveillance des communications « *crée par sa simple existence, pour tous ceux auxquels on pourrait l'appliquer, une menace de surveillance entravant forcément la liberté de communication entre usagers des services des postes et télécommunications et constituant par là une ingérence d'une autorité publique dans l'exercice du droit des requérants au respect de leur vie privée et familiale ainsi que de leur correspondance* » (CEDH, *Klass et autres c. Allemagne*, Plén., 6 septembre 1978, n° 5029/71, §41 ; voir aussi CEDH *Leander c. Suède*, 26 mars 1987, n° 9248/81, §48 ; *Rotaru c. Roumanie*, 4 mai 2000, n° 28341/95, §46).

Les mesures de surveillance, lorsqu'elles constituent une ingérence dans l'exercice du droit au respect de la vie privée ou du droit à la liberté d'expression consacrés par la Conv. EDH, doivent être prévues par la loi, poursuivre un intérêt légitime et être proportionnées à cet objectif, tel que l'exige le § 2 de ce même article 8.

Or, le décret met en œuvre une ingérence extrajudiciaire disproportionnée dans les droits et libertés. Celle-ci n'est ni « prévue par la loi », ni proportionnée aux buts qu'elle poursuit, tel qu'exigé tant par l'article 52, paragraphe 1 de la Charte que par les articles 8 et 10 de la Conv. EDH.

4.1.1. L'ingérence par le décret dans les droits fondamentaux protégés en droit conventionnel n'est pas prévue par la loi.

La Cour EDH considère que, pour qu'une ingérence soit « prévue par la loi » au sens de l'article 8§2 de la Conv. EDH, « *la loi doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à opérer pareille atteinte secrète, et virtuellement dangereuse, au droit au respect de la vie privée et de la correspondance* » (CEDH, *Malone c. Royaume-Uni*, 2 août 1984, n° 8691/79, §67). La Cour EDH précise ainsi que « *les mots « prévue par la loi », au sens de l'article 8§2, veulent d'abord que la mesure incriminée ait une*

base en droit interne, mais ils ont trait aussi à la qualité de la loi en cause : ils exigent l'accessibilité de celle-ci à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle » (CEDH, *Kruslin c/ France*, 24 avril 1990, n° 11801/85, §27).

Le décret attaqué autorise l'accès par les administrations énumérées à l'article R. 246-2 du code de la sécurité intérieure (CSI) aux données visées aux articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques (CPCE) ainsi qu'à l'article 1er du décret n° 2011-219.

Or, ces données ne sont conservées qu'à la discrétion des opérateurs de communications électroniques et des hébergeurs.

En cela, le décret manque de prévoir la portée de l'ingérence constituée à la fois par la conservation des données de connexion et l'accès qui y est accordé aux administrations.

4.1.1.1. Les données énumérées aux articles R. 10-14 CPCE et 1er, 3° et 4° du décret n° 2011-219 du 25 février 2011 ne sont conservées qu'à la discrétion des opérateurs de communications électroniques et des hébergeurs

L'article R. 10-14 CPCE autorise les opérateurs de communications électroniques à conserver certaines données concernant leurs clients, sans toutefois les y contraindre. En effet, l'article R. 10-14 CPCE dispose que :

> *« I.-En application du IV de l'article L. 34-1 les opérateurs de communications électroniques* ***sont autorisés*** *à conserver pour les besoins de leurs opérations de facturation et de paiement les données à caractère technique permettant d'identifier l'utilisateur ainsi que celles mentionnées aux b, c et d du I de l'article R. 10-13.*
>
> *« II.-Pour les activités de téléphonie, les opérateurs* ***peuvent conserver****, outre les données mentionnées au I, les données à caractère technique relatives à la localisation de la communication, à l'identification du ou des destinataires de la communication et les données permettant d'établir la facturation.*
>
> *« III.-Les données mentionnées aux I et II du présent article* ***ne peuvent être conservées que si elles sont nécessaires à la facturation et au paiement des services rendus****. Leur conservation devra se limiter au temps strictement nécessaire à cette finalité sans excéder un an.*
>
> *« IV.-Pour la sécurité des réseaux et des installations, les opérateurs* ***peuvent*** *conserver pour une durée n'excédant pas trois mois :*
>
> *a) Les données permettant d'identifier l'origine de la communication ;*
>
> *b) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;*
>
> *c) Les données à caractère technique permettant d'identifier le ou les destinataires de la communication ;*
>
> *d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs. »*

De même, les points 3° et 4° de l'article 1er du décret n° 2011-219 listent des données que fournisseurs d'accès à Internet et hébergeurs peuvent conserver quant à leurs utilisateurs, sans toutefois y être contraints.

Ainsi, l'article 1er du décret no 2011-219 dispose que :

« Les données mentionnées au II de l'article 6 de la loi du 21 juin 2004 susvisée, que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes :

[...]

« 3° Pour les personnes mentionnées aux 1 et 2 du I du même article, les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte :

« a) Au moment de la création du compte, l'identifiant de cette connexion ;

b) Les nom et prénom ou la raison sociale ;

c) Les adresses postales associées ;

d) Les pseudonymes utilisés ;

e) Les adresses de courrier électronique ou de compte associées ;

f) Les numéros de téléphone ;

g) Le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour ;

« 4° Pour les personnes mentionnées aux 1 et 2 du I du même article, lorsque la souscription du contrat ou du compte est payante, les informations suivantes relatives au paiement, pour chaque opération de paiement :

a) Le type de paiement utilisé ;

b) La référence du paiement ;

c) Le montant ;

d) La date et l'heure de la transaction.

« Les données mentionnées aux 3° et 4° ne doivent être conservées que dans la mesure où les personnes les collectent habituellement. »

Le décret attaqué permet l'accès administratif aux données que les opérateurs de communications électroniques, les fournisseurs d'accès à Internet et les hébergeurs choisissent de conserver quant à leurs utilisateurs. Or, *en ce qu'ils procèdent d'une simple faculté, ces choix ne sont ni connus ni prévisibles pour ces utilisateurs*, qui ignorent si des données les concernant, et lesquelles, sont conservées par ces prestataires et donc accessibles par l'administration. À tout le moins, la détermination des données conservées et accessibles par l'administration n'est pas définie par la loi.

L'ingérence constituée par la demande d'accès aux données telle que définie par le présent décret n'est donc pas « prévue par la loi » au sens de l'article 8 § 2 de la Conv. EDH, tel qu'interprété par la Cour EDH, puisque son étendue matérielle est laissée à la discrétion des opérateurs de communications électroniques, fournisseurs d'accès à Internet et hébergeurs.

Ainsi, le présent décret viole l'ensemble des dispositions de la Charte des droits fondamentaux et de la Conv. EDH susvisées.

4.1.1.2. L'obligation de conservation des données visées aux articles 1er, 1° du décret n° 2011-219 du 25 février 2011 et R. 10-13 CPCE est imprécise.

L'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) prévoit que :

> *« I.-1. Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne [...]*
> *« 2. Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services [...]*
> *« II.- Les personnes mentionnées aux 1 et 2 du I détiennent et conservent* ***les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus*** *des services dont elles sont prestataires.*
> *[...]*
> *« Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation. »*

Le décret n° 2011-219, pris en application de cet article 6 II de la LCEN, prévoit au point 1° de son premier article l'obligation pour les fournisseurs d'accès à Internet de conserver une liste de données permettant d'identifier leurs abonnés à chacune de leur connexion :

> *« Les données mentionnées au II de l'article 6 de la loi du 21 juin 2004 susvisée, que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes :*
> *1° Pour les personnes mentionnées au 1 du I du même article et* pour chaque connexion de leurs abonnés *:*
> *a) L'identifiant de la connexion ;*
> *b) L'identifiant attribué par ces personnes à l'abonné ;*
> *c) L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;*
> *d) Les dates et heure de début et de fin de la connexion ;*
> *e) Les caractéristiques de la ligne de l'abonné ; »*

Or, le champ des données défini par ce décret dépasse largement celui défini par la loi dans l'article 6 II de la LCEN. La loi ne vise que « *les données de nature à permettre l'identification de quiconque a contribué à la création d['un] contenu* » et non pas toute donnée permettant l'identification de tout abonné, *à chacune de ses connexions*, qu'il contribue ou non à la création d'un contenu. Le point 1° de l'article premier du décret n° 2011-219 crée une obligation que n'a pas prévue le législateur dans les dispositions que le décret est censé appliquer.

L'étendue matérielle de l'ingérence réalisée par le décret attaqué résultant d'un excès de pouvoir, cette ingérence n'est une fois de plus pas prévue par la loi au sens des dispositions conventionnelles précitées telles qu'interprétées par la Cour EDH et la CJUE.

Il en va de même lorsque le décret attaqué renvoie à l'article R. 10-13 CPCE pour définir le champ des données qu'il couvre. L'article R. 10-13 CPCE a été pris en application de l'article L. 34-1 III CPCE. Ce dernier article autorise les opérateurs de communications électroniques à différer d'un an l'effacement de certaines données techniques relatives à leurs abonnés, par dérogation à l'obligation prévue à l'article L. 34-1 II CPCE de les effacer ou de les rendre anonymes immédiatement.

L'article L. 34-1 CPCE prévoit en effet que :

> *« II.-Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI.*
> *[...]*
> *« III.-Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, **il peut être différé** pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs. »*

L'article L. 34-1 III CPCE ne prévoit encore ici qu'une simple faculté pour les opérateurs, et non une obligation. Pourtant, l'article R. 10-13 CPCE qui l'applique, prévoit une obligation de conservation des données techniques par ces prestataires.

En effet, l'article R. 10-13 CPCE dispose :

> *« I.-En application du III de l'article L. 34-1 les opérateurs de communications électroniques **conservent** pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :*
> *a) Les informations permettant d'identifier l'utilisateur ;*
> *b) Les données relatives aux équipements terminaux de communication utilisés ;*
> *c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;*
> *d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;*
> *e) Les données permettant d'identifier le ou les destinataires de la communication.*
> *« II.-Pour les activités de téléphonie l'opérateur conserve les données mentionnées au II et, en outre, celles permettant d'identifier l'origine et la localisation de la communication. »*

Ainsi, l'obligation de conservation des données techniques mise à la charge des opérateurs de communications électroniques par l'article R. 10-13 CPCE dépasse les limites posées par l'article L. 34-1 CPCE, qui ne prévoyait qu'une simple faculté pour ces derniers. L'étendue de cette obligation étant ainsi aussi incertaine que son existence, il en va de même du champ des données conservées par ces prestataires auxquelles le décret attaqué autorise l'accès par l'administration.

L'étendue matérielle de l'ingérence réalisée par le décret n'étant donc ici pas clairement définie, cette ingérence n'est pas prévue par la loi au sens des dispositions de la Conv. EDH et de la Charte des droits fondamentaux précitées, que le présent décret viole à nouveau.

4.1.2. Les limitations aux droits et libertés fondamentaux introduites par le décret attaqué sont disproportionnées.

Les limitations aux droits et libertés fondamentaux ne sont valides que si elles respectent le principe de proportionnalité.

De jurisprudence constante, la Cour EDH considère au regard de l'article 8§2 de la Conv. EDH, que, « *caractéristique de l'État policier, le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques* » (CEDH, *Klass et autres c. Allemagne*, Plén., 6 septembre 1978, n° 5029/71, §42). Elle considère ainsi qu'« *une ingérence est considérée comme « nécessaire dans une société démocratique » pour atteindre un but légitime si elle répond à un « besoin social impérieux » et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier apparaissent « pertinents et suffisants »* » (CEDH, *S et Marper c. Royaume-Uni*, 4 décembre 2008, n° 30562/04 et 30566/04, §101).

Tant la CJUE que la Cour EDH ont, au fil de leur jurisprudence, distingué plusieurs critères leur permettant d'évaluer la proportionnalité d'une restriction. Pour s'assurer de la proportionnalité d'une ingérence dans les droits et libertés fondamentaux, les juridictions sont notamment conduites à examiner si l'ingérence est pertinente pour parvenir au but visé et si ce but peut être atteint de manière satisfaisante par d'autres moyens, moins restrictifs de droits. Dans le cadre de ce contrôle, la CJUE et la Cour EDH sont amenées à examiner la durée de l'ingérence ainsi que les contrôles pouvant être opérés.

4.1.2.1. Il existe des mesures alternatives pour atteindre les finalités poursuivies.

Confier à l'autorité administrative un accès à une somme de données telle que celles visées par le décret n'est pas nécessaire pour atteindre les finalités définies à l'article L. 241-2 auxquelles l'article L. 246-1 CSI renvoie – notamment quant à la lutte contre le terrorisme, la criminalité et la délinquance organisées et la protection de la sécurité nationale.

En témoigne le fait que d'autres mesures permettent de poursuivre ces finalités. Ainsi, plusieurs États européens, dont l'Autriche, la Belgique, l'Allemagne, la Grèce ou la Roumanie, ont renoncé à recourir à la conservation généralisée des données techniques, pré-

férant des mesures ciblées de conservation des données, parmi lesquelles l'injonction faite par les autorités à un opérateurs de conserver les données ne concernant que certains individus suspects. Dans son étude sur « le numérique et les droits fondamentaux » de 2014, le Conseil d'État expose d'ailleurs précisément comment de telles mesures reposant sur des injonctions préalables ciblées seraient aussi envisageables en droit français[1].

Ensuite, la conservation généralisée des données techniques ne permet pas d'atteindre les finalités poursuivies par le présent décret plus efficacement que ne le peuvent ces mesures ciblées, que les États précités ont adoptées sans nuire à leur capacité de lutte contre les infractions graves. Ainsi, le gouvernement allemand publiait en 2008 une étude concluant à ce que seuls 4% des demandes d'accès de données faites par les autorités n'avaient pu être satisfaites en raison de l'absence d'une obligation de conservation généralisée des données techniques[2].

Ces mesures alternatives ciblées, adoptées par ces différents États, constituent une ingérence bien plus faible dans le droit au respect de la vie privée des utilisateurs que ne constitue celle réalisée par une conservation généralisée des données techniques, telle que celle à laquelle participe le présent décret.

Qui plus est, ce régime étendu d'accès administratif aux données de connexions n'a été accompagné par aucune étude d'impact. Cela est d'autant plus regrettable que le régime qui l'inspire, institué par la loi du 23 janvier 2006, n'est encore qu'« expérimental » comme le rappelle la CNCIS dans son dernier rapport d'activité[3]. Son élargissement drastique au travers du décret attaqué intervient donc sans qu'aucune étude ne permette d'en démontrer l'efficacité et le caractère nécessaire par rapport à des mesures plus ciblées, et donc moins restrictives de libertés.

En ce que l'atteinte aux droits portée par le décret dépasse très largement celle causée par des mesures alternatives, sans même justifier ni à plus forte raison démontrer sa plus grande efficacité du point de vue de l'objectif poursuivi, le décret attaqué doit être annulé.

4.1.2.2. La réquisition administrative des données est disproportionnée au regard de l'étendue des services administratifs ayant accès aux données collectées et des finalités visées par le décret.

La disproportion est d'autant plus manifeste que, par rapport à la loi du 23 janvier 2006, la loi de programmation militaire du 18 décembre 2013 (LPM) a encore élargi les mesures de réquisition administrative.

D'une part, la LPM a augmenté le nombre de services administratifs pouvant requérir ces données conservées. Ces services sont visés à l'article L. 246-2 CSI, leur nombre s'élève désormais à plusieurs dizaines en incluant des directions territoriales.

D'autre part, la LPM a élargi les finalités pour lesquelles les données de connexion peuvent être demandées. En effet, les réquisitions administratives de données de connexion

[1] `http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541/0000.pdf`, pp. 208 et s.

[2] Max Planck Institute for Foreign and International Criminal Law, *The Right of Discovery Concerning Telecommunication Traffic Data According to §§ 100g, 100h of the German Code of Criminal Procedure*, March 2008, `http://dip21.bundestag.de/dip21/btd/16/084/1608434.pdf`, p. 150.

[3] 22e rapport d'activité 2013-2014 de la CNCIS, p. 95 ; `http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000101/0000.pdf`.

prévues par le décret attaqué pourront intervenir dans un contexte identique à celui des interceptions de sécurité, à savoir, au delà de la prévention du terrorisme, la recherche des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention de la criminalité et de la délinquance organisées ou encore de la reconstitution ou du maintien de groupements dissous.

4.1.2.3. Les données sont conservées pour une durée excessive.

La durée de conservation des réponses fournies à l'administration est disproportionnée en ce qu'il n'est pas nécessaire pour l'administration de conserver les données concernées pour une période de trois ans, tel que prévu par le décret.

En effet, l'article R. 246-6, alinéa 3 dispose que :

> *« Le Premier ministre enregistre et conserve pendant une durée maximale de trois ans, dans un traitement automatisé qu'il met en œuvre, les informations ou les documents transmis par les opérateurs et les personnes mentionnés à l'article L. 246-1. »*

Comme l'observe la CNIL dans son avis, le Gouvernement, à l'occasion des formalités préalables effectuées pour les traitements actuellement mis en œuvre, a retenu une durée de conservation d'un an. La CNIL avait en effet relevé que cette durée était suffisante au regard des obligations légales et réglementaires imposées aux opérateurs, tout en permettant à la CNCIS de réaliser ses missions de contrôle a posteriori.

Rien ne justifie une durée de conservation de trois ans. Cette conservation centralisée de données extrêmement sensible est à la fois inutile pour parvenir au but recherché, elle est aussi dangereuse.

Tout d'abord, une durée unique de conservation des données établie à trois ans n'a aucun fondement pratique. Soit la personne dont les données sont demandées est considérée comme étant une personne à risque et dans ce cas, le service administratif à l'origine de la demande pourra assurer une copie des données et les conserver dans ses fichiers propres (typiquement un dossier d'enquête, une fiche S, etc.), soit il ne s'agit pas d'une personne à risque, et les données n'ont aucune raison d'être conservées sans être exploitées par ailleurs par les services administratifs.

Concrètement, le décret instaure un sas dans lequel les données sont conservées plus longtemps que chez les opérateurs ou hébergeurs sans qu'aucune raison ne le justifie.

Par ailleurs, aucun système informatique ne pouvant être parfaitement sécurisé, qu'il soit public ou privé, la conservation de données devrait se faire dans des conditions draconiennes pour limiter les atteintes aux droits des personnes en cas d'intrusion frauduleuse dans les systèmes informatiques concernés. Une durée de conservation de trois ans est d'autant plus inutile et dangereuse que nulle part ne sont prévues dans la loi ou le décret les mesures qui devront assurer la protection technique de ces données vis-à-vis notamment d'accès frauduleux.

4.1.2.4. Le contrôle sur les demandes de communications de données est lacunaire.

De jurisprudence constante, la Cour EDH considère qu'une société démocratique « *implique, entre autres, qu'une ingérence de l'exécutif dans les droits d'un individu soit soumise à un contrôle efficace* » (CEDH, *Klass et autres c. Allemagne*, Plén., 6 septembre 1978, n° 5029/71, §55).

De même, dans son arrêt du 8 avril 2014 déclarant l'invalidité de la directive 2006/24/CE, la CJUE se fondait notamment sur le fait que la directive n'imposait aucun contrôle préalable opéré par une autorité administrative indépendante ou judiciaire sur les demandes faites :

> « ***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.* »
> *(§62 de l'arrêt du 8 avril 2014 précité)*

Tout d'abord, le décret attaqué contrevient aux articles 8 et 10 de la Conv. EDH, ainsi qu'aux articles 7, 8, 11 et 52 de la Charte des droits fondamentaux en ce qu'il instaure des modalités de communications des données de connexion conservées sans instituer un contrôle préalable indépendant sur les demandes de transmission. Le régime d'autorisation par la « personnalité qualifiée » institué par la loi du 23 janvier 2006 en matière anti-terroriste et étendue par la LPM, n'apporte par les garanties suffisantes au regard du droit européen.

Ensuite, pour ce qui est du contrôle *a posteriori*, il s'avère lui aussi insuffisant pour assurer la conventionnalité du dispositif.

En effet, le décret attaqué ne fait que confier à la CNCIS l'accès aux traitements mentionnés aux articles R. 246-5 à 7 sans lui donner les moyens matériels lui permettant de réaliser un contrôle efficace de ces traitements. Dans son étude annuelle pour l'année 2014, le Conseil d'État observait lui-même que les moyens conférés à la CNCIS, qui « *n'ont pas évolué depuis la loi du 10 juillet 1991, alors que son champ de compétence a été considérablement étendu par la création d'une procédure d'accès aux métadonnées* », « *ne sont manifestement pas suffisants pour assurer un contrôle effectif de la surveillance des communications* », la CNCIS n'étant composée que de trois membres, assistés de cinq collaborateurs, et devant traiter près de 600 demandes par semaine. (pp. 211 et 212)

Ainsi, le décret échoue à remplir ce qui était pourtant le seul objectif qui lui était fixé par la loi à l'article L. 246-4 CSI et, en échouant à soumettre l'accès administratif aux données de connexion à un contrôle efficace, autorise une ingérence disproportionnée dans les droits reconnus par les articles 8 et 10 de la Conv. EDH.

4.2. Le décret attaqué est contraire à l'article L. 246-4 CSI en ce qu'il manque d'encadrer les procédures de suivi des demandes et de conservation des documents transmis à l'administration.

Le décret ne précise pas, comme l'y oblige l'article L. 246-4 CSI, les procédures de suivi des demandes par la CNCIS et les conditions de conservation des informations ou documents transmis.

L'article L. 246-4 du CSI prévoit que :

> *« Les modalités d'application [...] sont fixées par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des interceptions de sécurité, qui précise notamment la procédure de suivi des demandes et les conditions et durée de conservation des informations ou documents transmis »*

Comme le résume très clairement la notice de présentation du décret attaqué, celui-ci « *fixe les modalités de transmission des demandes à la Commission nationale de contrôle des interceptions de sécurité ainsi que celles du suivi général et du contrôle du dispositif par la commission* ». Cette notice précise aussi que « *le présent décret est pris pour l'application de l'article L. 246-4 du code de la sécurité intérieure* » (et de ce seul article).

Or, le décret n'apporte aucune information en la matière. À l'article R. 246-6, il se borne à rappeler « *que la transmission des informations ou des documents par les opérateurs et les personnes mentionnés à l'article L. 246-1 au groupement interministériel de contrôle est effectuée selon des modalités assurant leur sécurité, leur intégrité et leur suivi.* ».

Cette absence de définition des modalités de contrôles de la CNCIS exigée par l'article L. 246-4 CSI a d'ailleurs pu être observée par la CNIL dans son avis sur le projet de décret, lorsqu'elle remarque que « *le dossier qui lui a été soumis ne contient aucune information technique sur les modalités de mises en œuvre des réquisitions administratives de données de connexion ou d'informations relatives à l'accès de la CNCIS aux traitements automatisés prévus dans le cadre des articles L. 246-1 à L. 246-3 du CSI.* ».

Ainsi, le pouvoir réglementaire parvient tout à la fois à excéder le pouvoir qui lui est conféré au titre de l'article L. 246-4 CSI (*voir supra sur la légalité externe et l'incompétence du pouvoir réglementaire*, au point 3.1 page 5), et à manquer d'accomplir l'office qui lui est confié au titre du même article.

4.3. Le décret attaqué est contraire aux principes de sécurité juridique et de confiance légitime.

Pour les raisons déjà invoquées tenant notamment à l'imprécision des données auxquelles l'administration peut avoir accès, le décret porte atteinte aux principes de sécurité juridique et de confiance légitime (CE, Ass., Arrêt du 24 mars 2006, KPMG, n° 288460).

Par ces motifs, les exposants concluent à ce que le Conseil d'État :

1. Annule le décret attaqué avec toutes conséquences de droit ;

2. Mette à la charge de l'État le versement de la somme de 1024 € sur le fondement de l'article L. 761-1 du code de justice administrative.

Le 18 février 2015, à Paris

Pour l'association
French Data Network,
le Président,
Fabien Sirjean

Pour l'association
La Quadrature du Net,
le Président,
Philippe Aigrain

Pour la
Fédération des fournisseurs d'accès à Internet associatif,
le Président,
Benjamin Bayart

Pièces produites

1. Décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion.
2. Statuts de l'association French Data Network.
3. Extrait du compte rendu de la réunion du bureau de FDN du 10 janvier 2015 donnant pouvoir au président.
4. Statuts de l'association La Quadrature du Net.
5. Statuts de la Fédération des fournisseurs d'accès à Internet associatifs, dite Fédération FDN.
6. Charte de la Fédération FDN.
7. Compte rendu de la réunion du bureau de la Fédération FDN du 3 février 2015 donnant pouvoir au président.
8. La présente requête.

L'ensemble étant produit en 6 exemplaires.

SPINOSI & SUREAU
SCP d'Avocat au Conseil d'Etat
et à la Cour de cassation
16 Boulevard Raspail
75007 PARIS

CONSEIL D'ÉTAT

SECTION DU CONTENTIEUX

MEMOIRE EN REPLIQUE

POUR : **French Data Network (Réseau de données français), dite FDN**

La Quadrature du Net

Fédération des fournisseurs d'accès à Internet associatifs, dite Fédération FDN (FFDN)

SCP SPINOSI & SUREAU, avocat au conseil d'État

Sur la requête n° 388.134

DISCUSSION

I. En réponse au mémoire en défense en date du 6 octobre 2015 déposé par le Premier ministre, les associations French Data Network (FDN) et La Quadrature du Net ainsi que la Fédération des fournisseurs d'accès à Internet associatifs (FFDN) entendent verser aux débats les observations suivantes.

Persistant dans l'ensemble des moyens et des conclusions qu'elles ont développés dans leurs précédentes écritures, les exposantes entendent plus particulièrement stigmatiser la lecture partielle et erronée faite par la partie défenderesse du droit applicable en l'espèce.

Sur l'absence de compétence du pouvoir réglementaire

II. En premier lieu, le Premier ministre tente de faire valoir que le pouvoir réglementaire était bien compétent pour édicter le décret attaqué (cf. le mémoire en défense, p. 2).

Mais le raisonnement développé par le Premier ministre lui-même confirme qu'il n'en est strictement rien.

II-1 En effet, pour justifier de la nécessité de définir par le décret visé à l'article L. 246-4 du code de la sécurité intérieure les données pouvant être recueillies ainsi que les services de l'Etat bénéficiaires, le Premier ministre soutient tout d'abord que, dès lors qu'il lui appartenait de préciser les conditions de fonctionnement de la Commission nationale de contrôle des interception de sécurité (CNCIS), il lui fallait également définir les données auxquels pourraient avoir accès des services, lesquels devant aussi être déterminés.

Un tel raisonnement revient, implicitement mais nécessairement, à considérer que lorsqu'une procédure de contrôle doit être définie par décret, il doit *ipso facto* en être déduit qu'il revient aussi au pouvoir réglementaire de déterminer les atteintes aux libertés fondamentales sur laquelle la procédure de contrôle est censée porter.

Or, il convient de rappeler qu'aux termes de l'article 34 de la Constitution, c'est à « *la loi* » qu'il revient de fixer « *les règles concernant […] les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » (sur l'exigence européenne d'encadrement légal, v. également CJUE, Grande Chambre, 8 avril 2014, Aff. C-293/12 et C-594/12).

II-2 En outre, l'argumentation développée par le Premier ministre, en particulier pour préciser la mission de la CNCIS, témoigne de ce que le pouvoir règlementaire a manqué à son office en ne désignant ni les données, ni les services concernés.

Plus encore, les dispositions règlementaires litigieuses n'ont pas davantage défini les procédures de suivi des demandes et de conservation des documents transmis à l'administration (cf. le point 4.2. de la requête introductive), ce que ne conteste aucunement le Premier ministre.

Pourtant, ainsi que l'a récemment rappelé le Conseil constitutionnel, c'est à la loi qu'il appartient de déterminer « *les conditions d'exploitation, de conservation et de destruction des renseignements collectés* » (Cons. constit. Déc. n° 2015-713 DC du 23 juillet 2015, cons. 78).

Il résulte ainsi de ce qui précède que, contrairement à ce que soutient le Premier ministre, le pouvoir réglementaire a clairement excédé sa compétence en édictant les dispositions du décret attaqué.

Sur l'absence de notification du projet de décret à la Commission européenne

III. En deuxième lieu, dans l'espoir de justifier la méconnaissance de l'obligation de notification du projet de décret contestée à la Commission européenne en vertu de l'article 10 de la directive 98/34/CE du 22 juin 1998, le Premier ministre tente de faire valoir que le décret litigieux n'entrerait pas dans le champ d'application de cette directive (cf. le mémoire en défense, p. 3).

Or, une telle tentative ne peut qu'être vaine.

III-1 D'une part, et de manière pour le moins aventureuse, le Premier ministre prétend que « *les obligations fixées par la directive [...] ne peuvent s'appliquer à des normes décidées par les Etats membres pour des motifs de sécurité nationale* » en arguant de ce que l'article 4 du traité sur l'Union européenne stipule que « *la sécurité nationale reste de la seule responsabilité de l'Etat membre* » (cf. le mémoire en défense du Premier ministre, page 3).

Or, **d'emblée**, il importe de relever qu'admettre un tel raisonnement reviendrait à tolérer qu'un Etat membre de l'Union puisse se soustraire à ses obligations issues du droit de l'Union européenne au seul motif qu'il a spontanément décidé de placer l'un de ses dispositifs sous le sceau de la sécurité nationale.

Surtout, une telle lecture du Premier ministre ne résiste pas à l'analyse des textes pertinents et de la jurisprudence européenne.

Ainsi, l'obligation de communication de tout projet de règle technique prévue par l'article 8 de la directive 98/34/CE du 22 juin 1998 n'est écartée que dans les situations limitativement énumérées au sein de l'article 10 du même texte et l'enjeu de la sécurité nationale n'y figure absolument pas.

En outre, le champ d'application de la directive 98/34/CE du 22 juin 1998 n'est lui-même aucunement restreint par les impératifs tenant à la sécurité nationale.

Plus généralement encore, il y a lieu de rappeler que le droit de l'Union européenne peut parfaitement régir des domaines affectant la sécurité nationale sans que le principe prévu à l'article 4.2 du traité sur l'Union européenne ne soit méconnu.

Pour s'en convaincre, et parmi de multiples autres exemples, il suffit de rappeler le récent arrêt rendu par la Cour de justice de l'Union européenne dans l'affaire *Digital Rights Ireland et Seitlinger e.a* (CJUE, Grande Chambre, 8 avril 2014, Aff. C-293/12 et C-594/12).

A cette occasion, la Cour de justice était appelée à apprécier de la validité de la directive 2006/24/CE du 15 mars 2006 sur la

conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, laquelle fut notamment adoptée pour agir face « *aux affaires graves telles que celles liées à la criminalité organisée et au terrorisme* » et prévenir de nouveaux attentats terroristes à l'instar de ceux de Londres en 2005 (considérants 9 et 10 de la directive).

Ainsi, il est manifeste que le droit dérivé de l'Union européenne est intervenu dans le domaine de la sécurité nationale sans méconnaître le champ de compétence de l'Union. Au demeurant, si la Cour de justice n'a pas hésité à invalider ce texte, c'est uniquement en raison de la méconnaissance par cette directive des exigences du droit originaire de l'Union, au premier rang desquels figure la Charte des droits fondamentaux de l'Union européenne (v. *Digital Rights Ireland et Seitlinger e.a*, précité, § 32-71).

Enfin, à supposer même qu'il soit possible – pour les seuls besoins de la discussion – d'admettre un seul instant la lecture du Premier ministre selon lequel les obligations de la directive 98/34/CE ne s'appliqueraient pas aux dispositifs nationaux relatifs à la sécurité nationale, il convient de relever le dispositif d'accès administratif aux données de connexion mis en œuvre par le décret contestées ne concerne pas ce seul impératif.

En effet, aux termes des dispositions de l'article L. 241-2 du code de la sécurité intérieure en vigueur au jour de l'introduction du présent recours en annulation, les techniques d'accès administratif aux données de connexion pouvaient être mise en œuvre pour « *rechercher des renseignements intéressant la sécurité nationale* » mais aussi « *la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1* » du même code.

III-2 D'autre part, le Premier ministre ne saurait pas davantage écarter l'applicabilité de la directive du 22 juin 1998 en affirmant que « *le décret ne constitue pas une règle technique ni une règle technique*

ni une règle relative aux services au sens de l'article 1er de la directive » (Mémoire en défense, page 3).

En effet, à rebours de ce qu'affirme le Premier ministre, le décret litigieux affecte bien les conditions dans lesquelles les opérateurs peuvent s'installer ou exercer leur activité sur le territoire national, dès lors qu'il définit les conditions dans lesquelles les opérateurs de communications électroniques, les fournisseurs d'accès à Internet et les hébergeurs doivent déférer à un ensemble d'obligations destinées à offrir aux services compétents un accès aux données de connexion au sens des articles L. 246-1 et suivants du code de la sécurité intérieure.

Cette seule circonstance suffit à caractériser une « *règle technique* » au sens de l'article 1er 11) de la directive 98/34/CE modifiée, en ce que ces dispositions précisent qu'une telle règle est « *une spécification technique ou autre exigence ou une règle relative aux services, y compris les dispositions administratives qui s'y appliquent, dont l'observation est obligatoire de jure ou de facto, pour la commercialisation, la prestation de services, l'établissement d'un opérateur de services ou l'utilisation dans un État membre ou dans une partie importante de cet État […]* ».

Puisqu'en vertu de l'article 1er de la directive 98/48/CE portant modification de l'article 1er de la directive 98/34/CE, les services ainsi visés renvoient à « *tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de services* », il ne fait guère de doute que sont concernés l'ensemble des prestations offertes par les opérateurs de communications électroniques, les fournisseurs d'accès à Internet et les hébergeurs.

IV. Partant, la seule absence de notification du décret litigieux à la Commission européenne caractérise un vice de procédure qui en justifie la censure (v. not. CE, 10 juin 2013, n° 327.375).

Sur l'applicabilité de la Charte des droits fondamentaux de l'Union européenne

V. En troisième lieu, le Premier ministre n'hésite pas à soutenir que le moyen tiré de la violation de Charte des droits fondamentaux serait

inopérant dès lors que le décret attaqué ne mettrait pas en œuvre le droit de l'Union européenne (cf. le mémoire en défense, p. 4).

Là encore, une telle affirmation pourra être aisément écartée.

V-1 En effet, et en droit, la seule circonstance que les mesures litigieuses relèvent de la sécurité nationale ne saurait avoir pour conséquence de les soustraire du droit de l'Union européenne, dès lors que ces mesures constituent une limitation des droits et obligations résultant de la mise en œuvre du droit de l'Union.

Or, il appartient bien au Conseil d'État d'examiner si le décret attaqué constitue effectivement une telle mesure de limitation de la mise en œuvre du droit de l'Union.

Toute autre interprétation reviendrait à priver l'article 51-1 de la Charte des droits fondamentaux de tout effet utile, puisqu'il suffirait à chaque Etat membre de revendiquer la poursuite d'un objectif de sécurité nationale pour soustraire n'importe quelle mesure du contrôle de conventionnalité.

V-2 En outre, et toujours en droit, le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques font incontestablement partie du champ matériel du droit de l'Union européenne, qu'il s'agisse des articles 7 et 8 de la Charte ou de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

V-2.1 En particulier, l'objet de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 (directive dite « ePrivacy ») vise « *à garantir le plein respect des droits exposés aux articles 7 et 8* » de la Charte des droits fondamentaux (considérant 2).

Cette volonté du législateur européen apparaît notamment à l'article 15 de la directive, lequel établit les conditions dans lesquelles les États membres peuvent, dans la mise en œuvre du droit de l'Union,

prendre des mesures législatives ayant pour objectif notamment la sauvegarde de la sécurité nationale :

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

L'application de cet article à des mesures pour la sauvegarde de la sécurité nationale appelle deux remarques.

Tout d'abord, et contrairement à ce que soutient le Premier Ministre, le fait que les mesures litigieuses soient motivées par la sauvegarde de la sécurité nationale ne saurait avoir pour conséquence de les soustraire au respect du droit de l'Union européenne.

En effet, les mesures poursuivant un objectif de sauvegarde de la sécurité nationale sont explicitement visées par l'article 15 précité.

Ensuite, l'article 15 de la directive 2002/58 prévoit que de telles mesures visant à sauvegarder la sécurité nationale comprennent « *entre autres* » des mesures législatives prévoyant la conservation de données. La directive n'exclut donc pas de son champ d'application les mesures prévoyant l'accès aux données conservées ainsi que les modalités du contrôle de cet accès aux données conservées et leur utilisation subséquente.

Au contraire, de telles mesures s'inscrivent dans un ensemble

juridique cohérant relatif à la conservation des données dans l'objectif de sauvegarder la sécurité nationale.

Partant, toute mesure nationale ayant pour objectif la sauvegarde de la sécurité nationale doit être adoptée dans le respect de la Charte des droits fondamentaux de l'Union européenne, dès lors qu'une telle mesure constitue une limitation des droits et des obligations qui sont une mise en œuvre du droit de l'Union.

V-2.2 Plus particulièrement encore, l'article 15 de la directive précitée mentionne explicitement les droits et obligations en matière de confidentialité des communications et d'anonymisation des données définis par les articles 5, 6, 8, paragraphes 1, 2, 3 et 4, et par l'article 9 de la directive 2002/58.

Ces dispositions créent à la charge des États membres une obligation de garantir le respect de la vie privée ou du secret des correspondances en matière de communications électroniques et des données personnelles afférentes.

L'article 5, intitulé « Confidentialité des communications », prévoit ainsi que :

« *1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité. [...]* »

L'article 6 portant sur les « Données relatives au trafic » précise pour sa part que :

« 1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1. [...] »

Enfin, aux termes de l'article 9 relatif aux « Données de localisation autres que les données relatives au trafic »

« *1. Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. Les utilisateurs ou les abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données de localisation autres que les données relatives au trafic. [...] »*

VI. Or, **en l'espèce**, il ne fait aucun doute que les mesures litigieuses, lesquelles devraient être nécessaires, appropriées et proportionnées dans une société démocratique, constituent bien une limitation des droits et obligations précités.

En effet, l'article L. 246-1 (entretemps modifié et prévu désormais à l' article L. 851-1) du code de la sécurité intérieure porte notamment sur le recueil par l'administration, auprès des opérateurs de communications électroniques et des hébergeurs, des « *données techniques [...] de connexion à des services de communications électroniques* », des données relatives « *à la localisation des équipements terminaux utilisés* » et, plus généralement le recueil des

données conservées en application de l'article L. 34-1 du code des postes et des communications électroniques (CPCE) ainsi que du II de l'article 6 de la loi n° 2004-575 dite LCEN (v. Cons. const., juillet 2015, décision QPC n° 2015-478, cons. 12).

Or, les données ainsi visées par les dispositions litigieuses recouvrent totalement les données visées par les articles 5, 6, 8, paragraphes 1, 2, 3 et 4, et par l'article 9 de la directive 2002/58 précités, à savoir notamment les données relatives au trafic et les données de localisation.

Il ne saurait donc être sérieusement contesté que les dispositions litigieuses, en permettant à l'administration le recueil des données visées, constituent une limitation aux principes de confidentialité, d'effacement et d'anonymisation de ces données tels que prévus par le droit de l'Union.

VII. Ainsi, et contrairement à ce que tente vainement de démontrer le Premier Ministre, dès lors qu'elles constituent bien une limitation aux droits ou obligations résultant de la mise en œuvre du droit de l'Union, les mesures litigieuses doivent respecter la Charte des droits fondamentaux de l'Union européenne.

Toute autre appréciation révèlerait nécessairement l'existence d'une difficulté réelle et sérieuse d'interprétation des stipulations des traités de l'Union européenne – parmi lesquels figure la Charte des droits fondamentaux – mais aussi des dispositions des actes de droit dérivé – dont en particulier les directives 95/46/CE du 24 octobre 1995 et 2002/58/CE du 12 juillet 2002.

Or, **une telle situation exigerait nécessairement qu'une question préjudicielle soit adressée à la Cour de justice de l'Union européenne** en application de l'article 267 du Traité sur l'Union européenne, et plus précisément encore de son alinéa 5 qui prévoit une obligation de renvoi préjudiciel pour les juridictions nationales qui, à l'instar du Conseil d'Etat, rendent des « *décisions [qui] ne sont pas susceptibles d'un recours juridictionnel de droit interne* ».

Sur la méconnaissance de la Charte des droits fondamentaux de l'Union européenne

VIII. En quatrième lieu, le Premier ministre avance que le dispositif d'accès administratif aux données de la connexion n'est pas contraire aux stipulations de la Charte des droits fondamentaux de l'Union européenne, telle qu'interprétée par la Cour de justice de l'Union européenne dans son arrêt du 8 avril 2014 (cf. le mémoire en défense, p. 4).

Une fois encore, l'argumentation du Premier ministre ne saurait convaincre.

VIII-1 En effet, il importe à nouveau de souligner que la directive 2006/24/CE a été invalidée par la Cour de justice en ce qu'elle ne prévoyait « *pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte* » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 65) et manquait ainsi « *de garantir qu'elle [était] effectivement limitée au strict nécessaire* ».

Cette exigence de nécessité à laquelle doit se conformer toute ingérence dans les droits fondamentaux est fondée aussi bien sur l'article 52, paragraphe 1 de la Charte des droits fondamentaux que sur une jurisprudence constante de la Cour européenne des droits de l'homme et de la Cour de justice de l'Union européenne.

Venant préciser les critères de stricte nécessité qu'elle avait alors dégagés dans l'arrêt *Digital Rights,* la Cour de justice de l'Union européenne a clairement établi, dans son arrêt *Schrems* du 6 octobre 2015 (point 93), que « *n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes* » sans,

- D'une part, « *qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi* » (section 1.2.1) ;

- D'autre part, sans « *que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur*

utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence » (section 1.2.2) (CJUE, 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner,* Aff. C-362/14).

Or, le régime français en matière de conservation généralisée des données et d'accès à ces données présente précisément ces deux défauts.

Plus particulièrement, le décret attaqué en matière d'accès administratif aux données de connexion ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence d'accéder à ces données conservées.

VIII-2 Par ailleurs, en rappelant la nécessité de limiter le champ des données conservées, le récent arrêt *Schrems* s'inscrit dans une ligne jurisprudentielle déjà définie par la Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne.

Ainsi, par stricte application de l'article 8 de la Convention européenne des droits de l'homme, la Cour de Strasbourg encadre le champ des données à caractère personnel pouvant être collectées et conservées à des fins d'intérêt général en considérant que :

« *La protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article [...] La nécessité de disposer de telles garanties se fait d'au- tant plus sentir lorsqu'il s'agit de protéger les données à caractère personnel soumises à un traitement automatique, en particulier lorsque ces données sont utilisées à des fins policières.* ***Le droit interne doit notamment assurer que ces données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées*** » (Cour EDH*,* Grande Chambre, 4 décembre 2008, *Marper c. Royaume-Uni*, n° 30562/04 et 30566/04, §103*)*

Lors de l'examen de la directive 2006/24/CE, la Cour de justice de l'Union européenne a dénoncé avec une particulière insistance la gravité de l'ingérence dans la vie privée des personnes que constitue la simple conservation de leurs données de connexion :

« *Ces données, prises dans leur ensemble, 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. [...]*

Force est de constater que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère, ainsi que l'a également relevé M. l'avocat général notamment aux points 77 et 80 de ses conclusions, d'une vaste ampleur et qu'elle doit être considérée comme ***particulièrement grave.*** *En outre, la circonstance que la conservation des données* ***et l'utilisation ultérieure de celles-ci*** *sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, ainsi que l'a relevé M. l'avocat général aux points 52 et 72 de ses conclusions, le sentiment que leur vie privée fait l'objet d'une surveillance constante.* » *Digital Rights Ireland et Seitlinger e.a*, précité, § 27 et 37).

A fortiori, les données conservées auxquelles l'administration a la faculté d'accéder révèlent donc des informations particulièrement personnelles, une telle faculté constituant par conséquent une grave ingérence.

VIII-3 En outre, la Cour de justice de l'Union européenne conditionne la validité des régimes d'accès aux données issues d'une obligation de conservation généralisée à la présence de critères objectifs limitant l'accès et l'utilisation subséquente à des finalités poursuivies suffisamment sérieuses, c'est-à-dire des finalités « *précises, strictement restreintes et susceptibles de justifier l'ingérence* ».

Dans son arrêt *Digital Rights* précité, elle constatait ainsi 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.* » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 60)

En 2015, la Cour de justice a repris et précisé ce critère dans son arrêt *Schrems* en l'érigeant en critère de validité de tout régime d'utilisation des données relatives au trafic.

Ainsi, emporterait nécessairement violation de la Charte un régime qui ne prévoirait pas « *un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence* » (*Maximillian Schrems contre Data Protection Commissioner,* précité, § 93).

IX. Or**, en l'espèce** et **premièrement**, il est manifeste que le décret attaqué ne prévoit aucun critère objectif permettant de limiter l'accès aux données de connexion.

Dans sa version en vigueur au jour de l'introduction du présent recours, l'article L. 246-1 du code de la sécurité intérieure disposait que :

« *Pour les finalités énumérées à l'article L. 241-2, 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. »

Ces dispositions ont depuis été transférées, après modification, à l'article L. 851-1 du code de la sécurité intérieure.

Or, à aucun moment les dispositions réglementaires attaquées ou les dispositions législatives sur lesquelles elles se fondent n'établissent de critères objectifs venant limiter ou à tout le moins définir l'accès des services administratifs aux données que tant les hébergeurs que les fournisseurs de services de communications électroniques doivent conserver.

X. Par ailleurs, et **deuxièmement**, le décret attaqué renvoie à des finalités imprécises et peu restreintes.

La disposition contestée renvoie en effet aux finalités de l'article L. 241-2 de code de la sécurité intérieure, à savoir :

« rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de l'article L. 212-1. »

Or, de tels objectifs sont si largement définis et d'une telle diversité qu'ils ne peuvent en aucun cas être considérés comme « *des fins précises, strictement restreintes et susceptibles de justifier l'ingérence* ».

En effet, il peut être difficilement soutenu que « *la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France* » constitue une finalité précise, dès lors que les « *éléments essentiels* » visés ne sont définis par aucune disposition légale ou règlementaire. Au contraire, elles sont unilatéralement déterminées par les seules autorités administratives lorsqu'elles recourent à des

mesures de surveillance, sans même que les critères définissant ces « *éléments essentiels* » ne soient connus du public.

Dans ces conditions, il ne saurait être sérieusement soutenu qu'une telle finalité soit strictement restreinte.

De plus, la « *criminalité et la délinquance organisées* » recouvrent les nombreuses infractions listées à l'article 706-73 du code de procédure pénale (voir Conseil constitutionnel, décision n° 2015-713 DC du 23 juillet 2015).

Au titre de celles-ci se trouvent par exemple les infraction définies aux articles 222-34 à 222-40 du code pénal dont, notamment, la détention, l'acquisition ou l'emploi illicites de stupéfiants à titre personnel.

Or, la prévention de telles infractions ne serait nullement susceptible de justifier l'ingérence permise.

XI. En outre, et **troisièmement,** les dispositions règlementaires attaquées définissent un champ particulièrement large des personnes ayant accès aux données de connexions.

Alors que la liste des services pouvant accéder aux données conservées par les opérateurs et hébergeurs était déjà particulièrement large, celle-ci a en effet encore été considérablement allongée par le décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure.

Cette extension n'a néanmoins pas été associée à une partition des services administratifs selon les données auxquelles ils pouvaient avoir accès et les finalités pour lesquelles ils pouvaient y avoir accès.

Au contraire aux finalités déjà énoncées, dont la particulière imprécision a déjà été amplement soulignée, sont venues s'ajouter celles énoncées à l'article L. 811-3 du code de la sécurité intérieure.

Pourtant, la Cour de justice de l'Union européenne a considéré que la

limitation au strict nécessaire n'était pas garantie par la directive en ce qu'elle ne prévoyait « *aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi* » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 60).

L'importance de la définition précise et limitée du nombre d'administrations pouvant avoir accès aux données recueillies a encore récemment été mise en exergue par l'arrêt de la High Court britannique annulant la loi nationale adoptée l'an passé (High Court of Justice, 17 juillet 2015, [2015] EWHC 2092).

En effet, selon la Cour britannique, la loi nationale ne circonscrivait pas suffisamment le champ des autorités administratives pouvant accéder aux données que les opérateurs étaient tenus de conserver.

C'est d'ailleurs sur cette seule exigence que la *High Court* du Royaume-Uni a annulé une loi nationale établissant une obligation de conservation de données sans circonscrire suffisamment le champ des autorités administratives pouvant y accéder, considérant ainsi, dans un arrêt *Open Rights Group and others v. Secretary of State for the Home Department,* rendu le 17 juillet 2015, que :

« *La solution à ce problème et l'idée sous-jacente à l'arrêt Digital Rights Ireland est, selon nous, qu'une loi établissant un régime général de conservation de données de connexion viole les droits reconnus aux articles 7 et 8 de la Charte de l'UE à moins d'être accompagné par un régime d'accès (établi au niveau national) offrant des garanties adéquates de ces droits* » (§ 89 – Trad. libre de : « *The solution to the conundrum, in our view, and the ratio of Digital Rights Ireland, is that legislation establishing a general retention regime for communications data infringes rights under Articles 7 and 8 of the EU Charter unless it is accompanied by an access regime (laid down at national level) which provides adequate safeguards for those rights* »)

XII. Enfin, et **en quatrième et dernier lieu,** le décret attaqué n'a mis en place aucun contrôle préalable effectif.

Pourtant, dans son arrêt *Digital Rights*, la Cour de justice a clairement

énoncé que :

« *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*. » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 62)

Or, en l'espèce, les dispositions contestées ne prévoient que l'intervention d'une personnalité qualifiée placée auprès du Premier ministre en guise de contrôle préalable (article L. 246-2 du code de la sécurité intérieure).

Le seul contrôle préalable est donc celui d'une autorité qui n'est ni une autorité administrative indépendante, ni une juridiction et dont les critères d'appréciation ne sont pas clairement définis.

L'encadrement du rôle de la personnalité qualifiée et son positionnement auprès du Premier ministre ne permettent ainsi en aucune mesure de « *limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire* » (point précité).

XIII. Il résulte ainsi de l'ensemble de ce qui précède qu'à l'inverse de ce qu'affirme le Premier ministre, le décret attaqué méconnait clairement les stipulations de la Charte des droits fondamentaux de l'Union européenne, telle qu'interprété par la Cour de Justice dans son arrêt du 8 avril 2014.

Là encore, toute autre issue révèlerait une difficulté réelle et sérieuse d'interprétation des stipulations des traités de l'Union européenne et des dispositions des actes de droit dérivé, ce qui justifierait impérativement le renvoi par le Conseil d'Etat d'une **question préjudicielle** en application de l'article 267 du Traité sur l'Union européenne.

Sur la méconnaissance des dispositions de l'article L. 246-4 du code de la sécurité intérieure

XIV. En cinquième lieu, le Premier ministre tente de faire valoir que l'accès permanent de la CNCIS « *aux traitements automatisés mentionnés aux articles R. 246-5, R. 246-6 et R. 246-7* » suffirait à répondre à l'obligation de définir « *la procédure de suivi des demandes et les conditions et durée de conservation des informations ou documents transmis* » que le Premier ministre déduit des dispositions de l'article L. 246-4 du code de la sécurité intérieure alors en vigueur.

XIV-1 Pourtant, une simple comparaison des articles L. 246-4 et R. 246-8 du code de la sécurité intérieure suffit à montrer l'absence de tout rapport entre les deux dispositions.

La première concerne en effet le suivi des demandes et les conditions de conservation des informations et documents transmis, quand la seconde porte sur l'accès à ces informations et documents par la CNCIS.

Dans ces conditions, le seul accès de la CNCIS ne saurait pallier les insuffisances flagrantes d'encadrement de « *la procédure de suivi des demandes et des conditions et durée de conservation des informations ou documents transmis* ».

XIV-2 A cet égard, il y a lieu de rappeler que la Cour de justice de l'Union européenne a érigé les modalités de conservation des données par les services en l'une des conditions de validité d'un système de conservation des données avec la Charte des droits fondamentaux de l'Union européenne.

Ainsi, dans son arrêt *Digital Rights*, la Cour de justice a jugé à propos des données conservées par les opérateurs que :

« *De surcroît, en ce qui concerne les règles visant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, il convient de constater que la directive*

2006/24 ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. En effet, en premier lieu, l'article 7 de la directive 2006/24 ne prévoit pas de règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité. En outre, il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles règles. » (*Digital Rights Ireland et Seitlinger e.a*, précité, § 66).

A fortiori, une telle conclusion s'impose également aux administrations qui traitent ces données.

XIV-3 Or, en l'espèce, il est manifeste que rien n'est prévu dans le décret attaqué ou dans une quelconque autre disposition pour assurer la sécurité des données conservées une fois celles-ci transmises à l'administration.

XV. A tous égards, donc, la censure du décret attaqué est certaine.

PAR CES MOTIFS, et tous autres à produire, déduire, suppléer, au besoin même d'office, les exposantes persistent dans les conclusions de leurs précédentes écritures.

Avec toutes conséquences de droit.

SPINOSI & SUREAU
SCP d'Avocat au Conseil d'État

CONSEIL D'ETAT LL
statuant
au contentieux

N^os^ 388134,388255 **REPUBLIQUE FRANÇAISE**

_____

AU NOM DU PEUPLE FRANÇAIS

ASSOCIATION FRENCH DATA NETWORK (RESEAU DE DONNEES FRANÇAIS) et autres

REPORTERS SANS FRONTIERES

_____

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

M. Vincent Villette
Rapporteur

_____

Sur le rapport de la 10ème sous-section
de la Section du contentieux

M. Edouard Crépey
Rapporteur public

_____

Séance du 27 janvier 2016
Lecture du 12 février 2016

_____

Vu la procédure suivante :

1° Sous le n° 388134, par une requête, un mémoire complémentaire et un mémoire en réplique, enregistrés le 19 février et le 15 avril 2015 et le 22 janvier 2016, au secrétariat du contentieux du Conseil d'Etat, l'association French Data Network (Réseau Français de Données), l'association La Quadrature du Net et la Fédération des fournisseurs d'accès à internet associatifs demandent au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir le décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion ;

2°) de mettre à la charge de l'Etat la somme de 1 024 euros au titre des dispositions de l'article L. 761-1 du code de justice administrative.

……

2° Sous le n° 388255, par une requête et un mémoire en réplique, enregistrés le 24 février et le 6 novembre 2015, l'association Reporters sans frontières demande au Conseil d'Etat :

1°) d'annuler pour excès de pouvoir le décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion ;

2°) de mettre à la charge de l'Etat la somme de 512 euros au titre des dispositions de l'article L. 761-1 du code de justice administrative.

……

Vu les autres pièces des dossiers ;

Vu :

- la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales ;
- la Charte des droits fondamentaux de l'Union européenne ;
- la directive 98/34/CE du parlement européen et du conseil du 22 juin 1998 ;
- la directive 2002/58/CE du parlement européen et du conseil du 12 juillet 2002 ;
- le code de la sécurité intérieure, notamment ses articles L. 246-1 à L. 246-5 ;
- la loi du 29 juillet 1881 sur la liberté de la presse ;
- la décision du 5 juin 2015 par laquelle le Conseil d'Etat statuant au contentieux a renvoyé au Conseil constitutionnel la question prioritaire de constitutionnalité soulevée par les associations French Date Network, la Quadrature du Net et la Fédération des fournisseurs d'accès à internet associatifs ;
- la décision n° 2015-478 QPC du 24 juillet 2015 statuant sur la question prioritaire de constitutionnalité ainsi soulevée ;
- le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de M. Vincent Villette, auditeur,

- les conclusions de M. Edouard Crépey, rapporteur public ;

La parole ayant été donnée, avant et après les conclusions, à la SCP Spinosi, Sureau, avocat de l'association French Data Network (Réseau Français de Données), de l'association La Quadrature du Net et de la Fédération des fournisseurs d'accès à internet associatifs ;

1. Considérant que la requête commune de l'association French Data Network (Réseau Français de Données), de l'association La Quadrature du Net et de la Fédération des fournisseurs d'accès à internet associatifs ainsi que celle de l'association Reporters sans frontières sont dirigées contre le même décret du 24 décembre 2014 relatif à l'accès administratif aux données de connexion ; qu'il y a lieu de les joindre pour statuer par une seule décision ;

Sur la légalité externe :

2. Considérant, en premier lieu, que la circonstance que seul l'article L. 246-4 du code de la sécurité intérieure prévoit expressément l'intervention d'un décret en Conseil d'Etat pour définir ses modalités d'application ne prive pas le pouvoir réglementaire de l'étendue de la compétence qu'il détient pour prendre les mesures nécessaires à l'application des lois ; qu'ainsi, contrairement à ce qui est soutenu, le décret attaqué pouvait compétemment préciser, pour la mise en œuvre de l'ensemble des articles L. 246-1 à L. 246-4 du code de la sécurité intérieure, la procédure de suivi des demandes d'accès administratif aux données de connexion ainsi que les conditions et durée de conservation des informations ou documents transmis dans ce cadre ;

3. Considérant, en deuxième lieu, que dès lors que les dispositions du décret attaqué, qui portent sur l'accès administratif aux données de connexion, n'édictent pas de « règles techniques » relatives aux prestations de service assurées par les opérateurs au profit de leurs clients au sens de la directive du 22 juin 1998, les associations requérantes ne sauraient utilement invoquer à son encontre le moyen tiré de la méconnaissance de l'obligation de notification préalable du projet de décret à la Commission européenne instituée par l'article 8 de cette directive ;

4. Considérant, en troisième lieu, que les associations requérantes ne sauraient utilement invoquer à l'encontre du décret attaqué la méconnaissance de la circulaire du 17 février 2011 relative à la simplification des normes concernant les entreprises et les collectivités territoriales, adressée par le Premier ministre aux ministres, qui se borne à fixer des orientations pour l'organisation du travail gouvernemental ;

Sur la légalité interne :

En ce qui concerne les moyens tirés de l'atteinte disproportionnée portée par le décret attaqué au droit au respect de la vie privée et familiale, au droit à la protection des données à caractère personnel et à la liberté d'expression, tels qu'ils sont garantis par les articles 8 et 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et par les articles 7, 8 et 11 de la Charte des droits fondamentaux :

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 œuvre 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 œuvre 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 du droit au secret des sources des journalistes :

11. Considérant, d'une part, qu'aucune disposition constitutionnelle ne consacre un droit au secret des sources des journalistes ;

12. Considérant, d'autre part, qu'en l'absence de dispositions contraires dans la loi qui constitue le fondement du décret attaqué, ce dernier ne peut recevoir application que dans le respect de l'article 2 de la loi du 29 juillet 1881, aux termes duquel : « *(...) Il ne peut être porté atteinte directement ou indirectement au secret des sources que si un impératif prépondérant d'intérêt public le justifie et si les mesures envisagées sont strictement nécessaires et proportionnées au but légitime poursuivi. Cette atteinte ne peut en aucun cas consister en une obligation pour le journaliste de révéler ses sources (...)* », qu'il ne porte en lui-même aucune atteinte excessive au droit à la liberté d'expression, garanti notamment par l'article 10 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, dès lors que la procédure de réquisition administrative des données de connexion qu'il définit n'est autorisée qu'en vue de la poursuite des seules finalités mentionnées à l'article L. 241-2 du code de la sécurité intérieure, selon les modalités rappelées aux points précédents ;

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 ;

En ce qui concerne les autres moyens des requêtes :

14. Considérant qu'aucune disposition ni aucun principe n'imposait au pouvoir réglementaire d'épuiser, par le décret attaqué, l'habilitation qu'il tenait des dispositions législatives ; qu'ainsi, le moyen des associations requérantes tiré de l'erreur de droit dont serait entaché le décret attaqué, faute d'épuiser les modalités d'application pour la fixation desquelles l'article L. 246-4 du code de la sécurité intérieure a renvoyé à un décret en Conseil d'Etat, ne peut qu'être écarté ;

15. Considérant que le moyen tiré de ce que le décret attaqué porterait atteinte au principe de sécurité juridique n'est pas assorti des précisions permettant d'en apprécier le bien-fondé et ne peut, par suite, qu'être écarté ; qu'il en va de même, en tout état de cause, du moyen tiré d'une méconnaissance du principe de confiance légitime ;

16. Considérant, enfin, que par sa décision n° 2015-478 QPC du 24 juillet 2015, le Conseil constitutionnel a déclaré conforme à la Constitution les dispositions des articles L. 246-1 et L. 246-3 du code de la sécurité intérieure ; que, par suite, le moyen tiré de ce que le décret aurait été pris en application de dispositions législatives inconstitutionnelles doit être écarté ;

17. Considérant qu'il résulte de tout ce qui précède les associations requérantes ne sont pas fondées à demander l'annulation du décret qu'elles attaquent ; que leurs conclusions présentées au titre des dispositions de l'article L. 761-1 du code de justice administrative ne peuvent, par suite, qu'être rejetées ;

D E C I D E :

Article 1er : Les requêtes de l'association French Data Network (Réseau Français de Données), de l'association La Quadrature du Net, de la Fédération des fournisseurs d'accès à internet associatifs, ainsi que de l'association Reporters sans frontières sont rejetées.

Article 2 : La présente décision sera notifiée à l'association French Data Network (Réseau Français de Données), à l'association La Quadrature du Net, à la Fédération des fournisseurs d'accès à internet associatifs, à l'association Reporters sans frontières, au Premier ministre, au ministre de la défense, au ministre de l'intérieur, à la ministre des outre-mer et au ministre de l'économie, de l'industrie et du numérique.

Extrait du compte rendu de la réunion du bureau FDN
du 13 juin 2016

Le bureau ayant été convoqué en réunion extraordinaire par correspondance, l'ordre du jour appelait, au point 1, un vote concernant la motion suivante :

« *Le bureau de l'association FDN donne mandat à son président pour poursuivre devant toute juridiction compétente le refus du Conseil d'État de transmettre les questions préjudicielles posées dans le cadre du recours 388.134 devant le Conseil d'État contre le décret 2014-1576.* »

Se sont exprimé·e·s :
— Fabien Sirjean, président – par correspondance, le 14/06/2016 : [POUR]
— Hugo Roy, vice-président – par correspondance, le 14/06/2016 : [POUR]
— Rosemonde Letricot, trésorière – par correspondance, le 13/06/2016 : [POUR]
— Nicolas Grandjean, secrétaire – par correspondance, le 14/06/2016 : [POUR]

Les 4 membres du bureau s'étant exprimé·e·s, le vote est clos le 14 juin 2016.

La motion est adoptée à l'unanimité.

Fait à Grenoble, le 15 juin 2016

Le président,
Fabien Sirjean