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 :

[...]

« 3º 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 ;

« 4º 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 3º et 4º 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.