CONSEIL CONSTITUTIONNEL

Commentaire

Décision n° 2015-478 QPC du 24 juillet 2015

Association French Data Network et autres

(Accès administratif aux données de connexion)

Le Conseil d'État a renvoyé au Conseil constitutionnel le 5 juin 2015 (décision n° 388134 du même jour) une question prioritaire de constitutionnalité (QPC) posée par les associations French Data Network, la Quadrature du Net et Fédération des fournisseurs d'accès à internet associatifs portant sur les articles L. 246-1 à L. 246-5 du code de la sécurité intérieure (CSI).

Dans sa décision n° 2015-478 QPC, le Conseil constitutionnel a jugé que la QPC portait sur les articles L. 246-1 et L. 246-3 et les a déclarés conformes à la Constitution.

I – Les dispositions contestées

A. – Historique et contexte des dispositions contestées

Comme cela a été relevé lors des débats parlementaires sur le projet de loi relatif au renseignement, l'activité des services de renseignement s'est longtemps inscrite dans un environnement « ″para-légal″, ″extra-légal″ voire ″a-légal″ », la France pouvant être regardée comme « *rétive à toute intrusion du pouvoir législatif dans le champ des services de renseignement* »[1]. La loi relative au renseignement adoptée définitivement par le Parlement le 24 juin 2015, et que le Conseil constitutionnel a examiné dans sa décision n° 2015-713 DC du 23 juillet 2015, a pour objet de remédier à cette situation en créant un cadre juridique global et cohérent pour l'action de ces services.

Toutefois, avant ce texte, le législateur était déjà intervenu à plusieurs reprises afin d'encadrer l'usage de certaines techniques de renseignement. Il l'a ainsi fait pour les interceptions de sécurité avec la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques. Dans ce cadre, les services de renseignement pouvaient également

[1] Rapport n° 2697 du 2 avril 2015 fait au nom de la commission des lois de l'Assemblée nationale sur le projet de loi relatif au renseignement, p. 15

collecter des données de connexion, celles-ci étant une étape technique préalable aux interceptions de sécurité. Les évolutions technologiques ayant renforcé la « valeur informative » des données de connexion, la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers a créé une procédure dédiée pour le recueil de ces données. Par la suite, cette procédure a été substantiellement réformée par 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 dont sont issues les dispositions contestées relatives au recueil des données de connexion.

1. - La notion de « données de connexion »

La notion de « données de connexion » est décrite par l'étude d'impact du projet de loi relatif au renseignement :

« *En application du nouveau régime juridique et comme cela était déjà le cas sous l'empire du régime précédent,* ***l'accès aux données de connexion ne permet pas de connaître le contenu des échanges effectués par les personnes surveillées***.

« *Les services de renseignement peuvent accéder, en vertu de ce dispositif, aux informations et documents concernant les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communication électronique, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelant, la durée et la date des communications.*

« *Il ne s'agit donc que de la* ***collecte de toutes les "traces" d'une connexion ou d'un appel, des factures détaillées dont dispose chaque abonné. Jamais l'accès au contenu d'une connexion ou d'un appel n'est permis*** ».

Les « données de connexion » sont souvent qualifiées de « métadonnées », autrement dit de « données sur les données ».

La loi régit la conservation de ces données.

D'une part, le paragraphe II de l'article L. 34-1 du code des postes et des communications électroniques (CPCE) pose le principe de l'effacement ou l'anonymisation de « *toute donnée relative au trafic* », sous réserve des exceptions qu'il prévoit expressément, notamment pour les poursuites pénales.

D'autre part, les paragraphes I et II de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique prévoit que « *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 »* les personnes suivantes *:*

« *les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne ;*(…)

« *les personnes* (…) *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* ».

2. - L'accès aux données de connexion avant la loi de programmation militaire du 18 décembre 2013

Avant l'intervention de la loi du 18 décembre 2013, l'accès aux données de connexion reposait sur les opérateurs de services de communications électroniques.

L'accès administratif aux données de connexion était régi par deux procédures différentes.

* En premier lieu, l'article L. 244-2 du CSI, toujours en vigueur, qui permet au Premier ministre de recueillir auprès des opérateurs de services de communications électroniques « *les informations ou documents qui leur sont nécessaires, chacun en ce qui le concerne, pour la réalisation et l'exploitation des interceptions autorisées par la loi* ».

Selon la commission nationale de contrôle des interceptions de sécurité (CNCIS), ce dispositif peut être mis en œuvre « *pour tous les motifs légaux (la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupement dissous) et par tous les services* »[2].

Les demandes de réquisition sont examinées par le groupement interministériel de contrôle (GIC), relevant du Premier ministre, le contrôle a *posteriori* étant du ressort de la CNCIS.

---

[2] CNCIS, 20 ème rapport d'activité, 2011-2012, p.64.

* En second lieu, l'article 6 de la loi du 23 janvier 2006 avait inséré à l'article 6 de la loi du 21 juin 2004 un paragraphe II *bis* prévoyant une procédure spécifique d'accès aux données de connexion en matière de prévention du terrorisme.

Elle permettait aux services de police et de gendarmerie d'exiger des opérateurs de communications électroniques la transmission des données de connexion pour la seule finalité de prévention des actes de terrorisme[3].

Le nouvel article L. 34-1-1 du code des postes et des communications électroniques (CPCE) créé par cette loi disposait ainsi : « *Afin de prévenir les actes de terrorisme, les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions peuvent exiger des opérateurs et personnes mentionnés au I de l'article L. 34-1 la communication des données conservées et traitées par ces derniers en application dudit article.*

« *Les données pouvant faire l'objet de cette demande sont limitées aux 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, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ».

Les services adressaient leurs demandes à une « personnalité qualifiée ». Celle-ci était placée auprès du ministre de l'intérieur, mais désignée et contrôlée par la CNCIS. Après avoir vérifié le bien-fondé de la demande, la personnalité qualifiée délivrait une autorisation de transmission de la demande à l'opérateur concerné. La CNCIS effectuait aussi un contrôle *a posteriori*.

L'article 6 de la loi du 23 janvier 2006 prévoyait ainsi une procédure de demande et de contrôle formalisée.

Ce texte, qui a été jugé partiellement conforme à la Constitution par le Conseil constitutionnel dans sa décision n° 2005-532 DC du 19 janvier 2006[4], ne constituait toutefois qu'une base juridique partielle[5] et temporaire[6].

---

[3] Ces actes étant limitativement définis par les articles 421-1 à 421-2-2 du code pénal.

[4] Décision n° 2005-532 DC du 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.* Dans cette décision, le Conseil constitutionnel avait censuré l'emploi du mot « réprimer » qui donnait une finalité répressive à la réquisition, ce qui aboutissait à une

3. - La loi du 18 décembre 2013 relative à la programmation militaire

L'article 20 de la loi du 18 décembre 2013 a réorganisé l'accès administratif aux données de connexion, en abrogeant l'article L. 34-1-1 du CPCE et le paragraphe II *bis* de l'article 6 de la loi du 21 juin 2004 et en insérant au sein du CSI un nouveau chapitre intitulé « *Accès administratif aux données de connexion* » qui comprend les articles L. 246-1 à L. 246-5.

L'article L. 246-1 du CSI prévoit désormais que « *Pour les finalités énumérées à l'article L. 241-2*[7]*, 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* ».

Le décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion, pris pour l'application des articles L. 246-1 et suivants du CSI, a inséré dans ce code un article R. 246-1 ainsi rédigé : « *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* ».

L'article L. 246-2 du CSI précise dans son paragraphe I que les autorités compétentes pour solliciter ces données sont les « *agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la*

---

méconnaissance du principe de séparation des pouvoirs s'agissant d'un régime conçu pour prévenir et non pour réprimer (cons. 6).

[5] Limité à la seule finalité antiterroriste, le texte ne couvrait que les services du ministère de l'intérieur, et pas de la défense.

[6] Adopté pour trois ans, le dispositif a été reconduit à deux reprises, en 2009 puis en 2012, par le législateur, pour une expiration au 31 décembre 2015. Son caractère provisoire avait ainsi tendance à se pérenniser.

[7] Les finalités pour lesquelles il peut être procédé à des réquisitions administratives de données de connexion sont ainsi identiques à celles exigées pour les interceptions de sécurité.

sécurité intérieure, de la défense, de l'économie et du budget chargés de missions prévues à l'article L. 241-2 ».

Le régime n'est cependant pas aligné sur celui des interceptions de sécurité dès lors qu'en vertu du paragraphe II de l'article L. 246-2, les demandes motivées sont « *soumises à la décision d'une personnalité qualifiée placée auprès du Premier ministre* ». Cette personnalité est désignée pour trois ans renouvelables par la CNCIS sur proposition du Premier ministre qui lui présente une liste d'au moins trois noms. Elle adresse annuellement un rapport d'activité à la CNCIS.

L'article L. 246-3 du CSI permet, pour sa part, aux services de renseignement de recueillir des données de connexion en temps réel, et non plus seulement de manière rétrospective. Il dispose ainsi que « *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* ». Cette mesure, qui permet également de géolocaliser une personne, est mise en œuvre après autorisation du Premier ministre. L'autorisation est communiquée au président de la CNCIS qui peut, s'il estime la légalité de la mesure incertaine, réunir la commission afin qu'il soit adressé au Premier ministre une recommandation tendant à ce qu'il y soit mis fin.

L'article L. 246-4 du CSI prévoit que la CNCIS dispose d'un accès permanent au dispositif de recueil des informations ou documents mis en œuvre afin de procéder à des contrôles visant à s'assurer du respect des conditions fixées aux articles L. 246-1 à L. 246-3.

Enfin, l'article L. 246-5 du CSI dispose que les surcoûts liés à ces mesures pour les opérateurs mentionnées à l'article L. 246-1 font l'objet d'une compensation financière de la part de l'État.

4. – La loi relative au renseignement définitivement adoptée par le Parlement le 24 juin 2015

La loi relative au renseignement modifie les dispositions contestées.

L'article L. 246-1 du CSI devient l'article L. 851-1 du même code. Le recueil n'est plus autorisé par une personnalité qualifiée mais par le Premier ministre, après avis de la commission nationale de contrôle des techniques de renseignement (CNCTR), à la suite d'une demande directe des agents habilités des services de renseignement des premier et second cercles visés aux articles L. 811-2 et L. 811-4 du CSI.

L'article L. 246-3 du CSI devient l'article L. 851-4 du même code.

L’autorisation est également donnée par le Premier ministre après avis de la CNCTR, cette dernière étant toutefois saisie par l’un des ministres ou collaborateurs directs de ceux-ci visés à l’article L. 821-2.

Les articles L. 246-2, L. 246-4 et L. 246-5 sont pour leur part abrogés.

Les dispositions contestées demeurent toutefois applicables jusqu’à l’adoption des mesures réglementaires prévues par l’article 26 de la loi relative au renseignement. Par conséquent, dans la décision commentée, le Conseil constitutionnel était appelé à contrôler l’état du droit actuellement en vigueur et qui le demeurera jusqu’à cette date.

B. – Origine de la QPC et question posée

Les associations French Data Network, la Quadrature du Net et Fédération des fournisseurs d’accès à internet associatifs ont saisi le Conseil d’État d’un recours en excès de pouvoir à l’encontre du décret n° 2014-1576 du 24 décembre 2014 relatif à l’accès administratif aux données de connexion.

À l’occasion de ce recours, ces associations ont soulevé une QPC portant sur les articles L. 246-1 à L. 246-5 du CSI.

Par sa décision du 5 juin 2015, le Conseil d’État a transmis au Conseil constitutionnel la question de la conformité à la Constitution de ces dispositions, en considérant que le moyen tiré de ce que celles-ci « *portent atteinte aux droits et libertés garantis par la Constitution, en particulier au droit au respect de la vie privée, au droit à un procès équitable et à la liberté de communication, soulève une question présentant un caractère sérieux* ».

Les associations requérantes formulaient uniquement des griefs tirés de la méconnaissance de l’étendue de sa compétence par le législateur, dans des conditions affectant des droits et libertés que la Constitution garantit. Leurs arguments relatifs au caractère incomplet de l’intervention du législateur portaient sur deux aspects des articles L. 246-1 à L. 246-5 du CSI :

– d’une part, l’imprécision d’un certain nombre de définitions relatives aux données pouvant faire l’objet de la procédure de recueil prévue par ces articles et à la procédure en elle-même ;

– d’autre part, l’absence de garanties particulières prévues pour certaines professions (les avocats ainsi que les journalistes) par cette procédure de recueil d’informations.

Le Conseil constitutionnel, compte tenu des griefs formulés par les associations requérantes, a considéré que la QPC portait uniquement sur les articles L. 246-1 et L. 246-3 du CSI.

II. – L'examen de la constitutionnalité des dispositions contestées

A. – La jurisprudence constitutionnelle

1. – Le droit au respect de la vie privée

Après avoir estimé que les méconnaissances graves du droit au respect de la vie privée affectent la liberté individuelle[8], le Conseil constitutionnel, à compter de 1999, a rattaché le droit au respect de la vie privée à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789. Il a jugé que la liberté proclamée par cet article « *implique le respect de la vie privée* »[9].

La notion de « vie privée » est entendue par le Conseil constitutionnel de façon classique : c'est la sphère d'intimité de chacun. Le champ d'application de cette notion est donc restrictif.

Le Conseil constitutionnel juge qu'il appartient au législateur d'assurer « *la conciliation entre le respect de la vie privée et d'autres exigences constitutionnelles, telles que la recherche des auteurs d'infractions et la prévention d'atteintes à l'ordre public* »[10].

La jurisprudence du Conseil constitutionnel sur le droit au respect de la vie privée est abondante. Celui-ci a notamment eu l'occasion de confronter ce droit constitutionnel à des procédures de recueil de données de connexion ou de recueil de données pour l'établissement de fichiers.

Dans sa décision n° 2005-532 DC du 19 janvier 2006, après avoir rappelé les termes de l'article L. 34-1-1 du CPCE et cité son considérant de principe relatif à la vie privée, le Conseil constitutionnel a jugé que le législateur avait assorti la procédure de réquisition de données techniques qu'il a instituée de limitations et précautions, propres à assurer la conciliation qui lui incombe entre, d'une part, le respect de la vie privée des personnes et la liberté d'entreprendre des opérateurs, et, d'autre part, la prévention des actes terroristes dès lors que *« cette procédure sera mise en œuvre par des " agents individuellement désignés et dûment*

---

[8] Décision n° 97-389 DC du 22 avril 1997, *Loi portant diverses dispositions relatives à l'immigration*, cons. 44.

[9] Voir notamment les décisions n[os] 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, cons. 45 ; 2004-492 DC du 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*, cons. 75 ; 2010-604 DC du 25 février 2010, *Loi renforçant la lutte contre les violences de groupes et la protection des personnes chargées d'une mission de service public*, cons. 21.

[10] Décision n° 2011-209 QPC du 17 janvier 2012, *M. Jean-Claude G. (Procédure de dessaisissement d'armes)*, cons. 3.

habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions " ; qu'elle s'appliquera à toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau ; qu'elle sera limitée " aux 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, aux données relatives à la localisation des équipements terminaux utilisés ainsi qu'aux données techniques relatives aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications " ; qu'elle sera subordonnée à un accord préalable d'une personnalité désignée par la Commission nationale de contrôle des interceptions de sécurité ; qu'elle sera soumise au contrôle de cette commission, laquelle adressera des recommandations au ministre de l'intérieur lorsqu'elle constatera " un manquement aux règles édictées par le présent article ou une atteinte aux droits et libertés " ; qu'elle ouvrira droit à une compensation financière des surcoûts consécutifs aux demandes d'information »[11].

S'agissant de l'article 8 de la loi contrôlée, relatif à la mise en œuvre de « *dispositifs fixes ou mobiles de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants, en tous points appropriés du territoire* », le Conseil constitutionnel, après avoir relevé les objectifs poursuivis et les conditions (effacement, durée de conservation, accès …) fixées par la loi, a jugé qu'« *eu égard aux finalités que s'est assignées le législateur et à l'ensemble des garanties qu'il a prévues, les dispositions contestées sont propres à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée* »[12].

Le Conseil constitutionnel a reconnu le droit au respect de la vie privée comme un droit ou liberté invocable en QPC dès sa décision n° 2010-25 QPC du 16 septembre 2010[13].

2. – La liberté d'expression et de communication

La protection constitutionnelle de la liberté d'expression et de communication se fonde sur l'article 11 de la Déclaration de 1789 : « *La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme : tout*

---

[11] Décision n° 2005-532 DC du 19 janvier 2006 préc., cons.10.
[12] Ibidem , cons. 21.
[13] Décision n° 2010-25 QPC du 16 septembre 2010, *M. Jean-Victor C (Fichier empreintes génétiques)*, cons. 6 et 16.

citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi. » Le Conseil constitutionnel ajoute qu'il s'agit là d'une liberté fondamentale « *d'autant plus précieuse que son exercice est une condition de la démocratie et l'une des garanties du respect des autres droits et libertés* ». Il en déduit que « *les atteintes portées à l'exercice de cette liberté doivent être nécessaires, adaptées et proportionnées à l'objectif poursuivi ;* »[14].

La jurisprudence du Conseil constitutionnel est abondante en la matière. Elle a toutefois principalement consisté à contrôler, en matière de médias, les dispositions législatives assurant la régulation globale de la presse ou de l'audiovisuel[15]. Le Conseil constitutionnel a eu, plus rarement, l'occasion de veiller à la protection de cette liberté d'expression dans sa dimension « active ».

Comme il l'a rappelé dans sa décision HADOPI I (n° 2009-580 DC du 10 juin 2009), le Conseil constitutionnel subordonne la conformité à la Constitution des atteintes portées à cette liberté à une triple condition de nécessité, d'adaptation et de proportion à l'objectif poursuivi, objectif qui doit relever d'une autre règle ou principe de valeur constitutionnelle.

Dans sa jurisprudence, le Conseil constitutionnel n'a pas retenu une conception de la liberté d'expression et de communication s'étendant à l'ensemble des atteintes indirectes à celles-ci.

Ainsi, il aurait été possible de considérer que les mesures de recueil de données de connexion, qui peuvent inciter des personnes à ne pas communiquer avec certains individus ou à ne pas s'exprimer afin d'éviter que ces communications ou propos ne soient connus des services de renseignement, portent atteinte à la liberté d'expression et de communication. Cependant, dans la décision n° 2005-532 DC du 19 janvier 2006 précitée, le Conseil constitutionnel a confronté expressément les dispositions relatives aux données de connexion uniquement au droit au respect de la vie privée et à la liberté d'entreprendre.

De la même manière, lorsqu'il a contrôlé, dans la décision n° 2013-679 DC du 4 décembre 2013, les dispositions de la loi relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière permettant au juge des

---

[14] Décision n° 2009-580 DC du 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet*, cons. 15.

[15] Décisions n^{os} 82-141 DC du 27 juillet 1982, *Loi sur la communication audiovisuelle ;* 84-181 DC du 11 octobre 1984, *Loi visant à limiter la concentration et à assurer la transparence financière et le pluralisme des entreprises de presse ;* 86-217 DC du 18 septembre 1986, *Loi relative à la liberté de communication ;* 2009-577 DC du 3 mars 2009, *Loi relative à la communication audiovisuelle et au nouveau service public de la télévision* et 2009-580 DC du 10 juin 2009 *Loi favorisant la diffusion et la protection de la création sur internet*..

libertés et de la détention d'autoriser des interceptions de correspondances, il l'a fait au regard du droit au respect de la vie privée, sans confronter dans le même temps ces dispositions à la liberté d'expression ou de communication[16].

B. – La jurisprudence européenne relative au secret professionnel des avocats et des journalistes

* Selon l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ». Les communications par téléphone, télécopie et email sont comprises dans les notions de vie privée et de correspondance au sens de cet article.

La Cour européenne des droits de l'homme (CEDH) rattache à l'article 8 de la convention le secret des correspondances ou communications entre un avocat et son client. Elle considère que cette correspondance jouit d'un statut privilégié quant à sa confidentialité et elle accorde un poids singulier au risque d'atteinte au secret professionnel des avocats car il peut avoir des répercussions sur la bonne administration de la justice. Elle admet une ingérence dans ce droit dès lors qu'elle est prévue par la loi, motivée par un ou des buts légitimes et nécessaire dans une société démocratique pour atteindre ceux-ci. C'est sous le bénéfice de cette analyse que la Cour a admis, dans sa décision *Michaud c/ France* du 6 décembre 2012[17], que l'obligation de déclaration de soupçon imposée aux avocats ne porte pas une atteinte disproportionnée à leur secret professionnel.

* Si la CEDH reconnaît un statut particulier au secret professionnel des journalistes, et plus spécifiquement le secret de leurs sources, c'est sur le fondement de l'article 10 de la convention, relatif à la liberté d'expression, et non sur celui de l'article 8.

La CEDH a rappelé dans plusieurs décisions que « *le droit des journalistes de taire leurs sources ne saurait être considéré comme un simple privilège, qui leur serait accordé ou retiré en fonction de la licéité ou de l'illicéité des sources, mais qu'il doit être considéré comme un attribut du droit à l'information, à traiter avec la plus grande circonspection* »[18] . Il revient aux autorités publiques de mettre en balance correctement l'intérêt des enquêtes à l'obtention d'éléments de preuve et l'intérêt public à la protection de la liberté d'expression

---

[16] Décision n° 2013-679 DC du 4 décembre 2013, *Loi relative à la lutte contre la fraude fiscale et la grande délinquance économique et financière*, cons. 75

[17] Décision n° 12323/11 du 6 décembre 2012, *Michaud c/ France*

[18] Voir par exemple les décisions *Tillack c. Belgique* (n° 20477/05) du 27 novembre 2007 ; *Nagla c. Lettonie* (n° 73469/10) du 16 juillet 2013.

des journalistes.

Examinant la législation allemande, la CEDH s'est prononcée de la manière suivante dans son arrêt *Weber et Saravia* du 29 juin 2006[19]. La Cour était saisie d'une argumentation selon laquelle les pouvoirs de surveillance confiés aux autorités allemandes « *portent atteinte au travail des journalistes enquêtant sur des questions visées par les mesures de surveillance* » et qu'il serait « *impossible de garantir que la confidentialité des informations* » reçues des journalistes soit préservée.

Pour statuer, la Cour s'est d'abord référée au contrôle exercé par la Cour constitutionnelle allemande, puis a jugé :

« *151. La Cour observe qu'en l'espèce les autorités procèdent à une surveillance stratégique pour prévenir les infractions énumérées à l'article 3 § 1. La mesure ne vise donc pas à surveiller des journalistes ; en général, les autorités ne découvrent que lorsqu'elles examinent, le cas échéant, les télécommunications interceptées que les conversations d'un journaliste ont été surveillées. En particulier, les mesures de surveillance ne sont pas destinées à découvrir des sources journalistiques. L'ingérence dans l'exercice de la liberté d'expression que constitue la surveillance stratégique ne saurait dès lors être qualifiée de particulièrement grave.*

« *152. Certes, les dispositions litigieuses de la loi G 10 dans sa teneur modifiée ne renferment pas de dispositions spéciales protégeant la liberté de la presse et, en particulier, prémunissant les journalistes contre la divulgation de leurs sources dès lors que les autorités découvrent qu'elles ont intercepté la conversation d'un journaliste. Toutefois, eu égard à ses constats sous l'angle de l'article 8, la Cour observe que les dispositions litigieuses offrent de nombreuses garanties qui permettent de limiter les atteintes au secret des télécommunications – et donc à la liberté de la presse – à ce qui est nécessaire pour atteindre les buts légitimes poursuivis. En particulier, les garanties grâce auxquelles les données recueillies ne peuvent être utilisées que pour prévenir certaines infractions pénales graves doivent également passer pour adéquates et effectives aux fins de maintenir au minimum inévitable la divulgation des sources journalistiques. Dès lors, la Cour conclut que l'Etat défendeur a fourni des raisons pertinentes et suffisantes pour justifier l'atteinte à la liberté d'expression résultant des dispositions litigieuses, au regard des intérêts légitimes que sont la sécurité nationale et la prévention des infractions pénales. Compte tenu de sa marge d'appréciation, l'Etat défendeur était fondé à considérer que ces exigences l'emportaient sur le droit à la liberté*

[19] Décision n° 54934/00 du 29 juin 2006, *Weber et Saravia c/ Allemagne*

d'expression ».

C. - L'application à l'espèce

Les associations requérantes soutenaient que les dispositions contestées étaient entachées de plusieurs incompétences négatives, lesquelles affecteraient le droit au respect de la vie privée, la liberté d'expression et de communication, le droit au secret des correspondances entre un avocat et son client et le droit au secret des sources d'information des journalistes, de sorte qu'elles seraient critiquables en QPC.

1. – Sur l'incompétence négative dans la détermination des modalités d'accès aux données de connexion

Les associations requérantes soutenaient que l'incompétence négative résultant de l'absence de définition légale des notions d' « informations ou documents », d' « opérateurs de communications électroniques » et de « sollicitation du réseau » figurant aux articles L. 246-1 et L. 246-3 est de nature à porter atteinte au droit au respect de la vie privée.

Pour être invocables en QPC, les griefs d'incompétence négative doivent être de nature à entraîner une méconnaissance d'un droit ou liberté garanti par la Constitution.

Sur ce point, le Conseil constitutionnel a admis l'invocabilité du grief, en considérant « *qu'aux termes de l'article 34 de la Constitution : "La loi fixe les règles concernant… les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques" ; que la méconnaissance par le législateur de sa compétence, dans la détermination de ces garanties dans le cadre d'une procédure de réquisition administrative de données de connexion, affecte par elle-même le droit au respect de la vie privée* » (cons. 10).

a) Sur l'absence de définition légale des notions d' « opérateurs de communications électroniques » et d' « informations ou documents »

* Les associations requérantes soutenaient, d'une part, qu'en visant les « *opérateurs de communications électroniques et [l]es personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que [l]es 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* », l'article L. 246-1 du CSI serait entaché d'une incompétence négative dès lors que la notion d' « opérateurs de communications électroniques » était insuffisamment précise et, d'autre part, qu'en s'abstenant de définir suffisamment précisément la

notion d' « informations ou documents » susceptibles d'être recueillis par les autorités administratives en application de l'article L. 246-1 du CSI, la loi permettait aux services de renseignement d'accéder par ces techniques au contenu des correspondances.

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

Par ailleurs, en ce qui concerne les « informations et documents » susceptibles d'être recueillis en application de l'article L. 246-1 du CSI, le Conseil constitutionnel a relevé que, au-delà de l'énumération figurant à cet article, des textes législatifs encadrent par ailleurs les données traitées ou conservées par les réseaux ou services de communications électroniques. Ainsi, l'article L. 34-1 du code des postes et des communications électroniques prévoit dans son paragraphe VI que : « *Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation*

des équipements terminaux. / Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ». Par ailleurs, le paragraphe II de l'article 6 de la loi du 21 juin 2004 indique que les données conservées sont celles de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires. Le Conseil constitutionnel en a déduit, d'une part, que les données recueillies en application de l'article L. 246-1 ne pouvaient porter sur le contenu de correspondances ou les informations consultées et, d'autre part, que le législateur avait suffisamment défini la notion de données de connexion (cons. 12).

b) Sur l'absence de définition légale de la notion de « sollicitation du réseau »

Les associations requérantes soutenaient également qu'en indiquant à l'article L. 246-3 du CSI que « *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* », le législateur n'avait pas exclu la possibilité pour les autorités administratives d'accéder directement aux données de connexion et non plus de se voir uniquement transmettre ces données par les opérateurs.

Le Premier ministre faisait valoir dans ses observations que le terme « sollicitation » a uniquement pour objet de désigner la technique nécessaire à l'obtention « en temps réel » des données nécessaires à la localisation d'une personne. Cette « sollicitation » serait effectuée par les opérateurs de communications électroniques qui enverraient alors, depuis leur réseau, des signaux vers les terminaux mobiles des personnes aux fins de recherches de la station de base la plus proche d'un terminal donné.

Cette explication se trouvait également dans le rapport de la commission des affaires étrangères, de la défense et des forces armés du Sénat : « *Il est donc proposé de compléter l'article L. 34-1-1 du code des postes et communications électroniques en indiquant que les données des opérateurs de communication électroniques traitées par leurs réseaux ou leurs services de communication électroniques sont obtenues après conservation ou en temps réel, le cas échéant après mise à jour des données, c'est-à-dire après sollicitation des équipements par le réseau* »[20].

[20] Rapport n° 50 (2013-2014) de M. Jean-Louis CARRÈRE, fait au nom de la commission des affaires étrangères, de la défense et des forces armées, déposé le 8 octobre 2013

Le Conseil constitutionnel a jugé « *qu'il résulte de l'article L. 246-1 que les données de connexion requises sont transmises par les opérateurs aux autorités administratives compétentes ; que selon l'article L. 246-3, lorsque les données de connexion sont transmises en temps réel à l'autorité administrative, celles-ci ne peuvent être recueillies qu'après " sollicitation " de son réseau par l'opérateur ; que, par suite, les autorités administratives ne peuvent accéder directement au réseau des opérateurs dans le cadre de la procédure prévue aux articles L. 246-1 et L. 246-3* » (cons. 13).

2. – Sur l'incompétence négative résultant de l'absence des garanties légales protégeant les données de connexion des avocats et journalistes

Les associations requérantes formulaient un second grief d'incompétence négative à l'encontre des dispositions contestées, tiré cette fois de ce qu'en ne prévoyant aucune garantie légale spécifique pour protéger le secret professionnel des avocats et des journalistes, le législateur a permis qu'il puisse être porté atteinte au droit au respect de la vie privée, à la liberté d'expression et de communication, ainsi qu'aux droits de la défense et au droit à un procès équitable. Plus encore, il serait ainsi porté atteinte à deux droits qui en découleraient : le droit au secret des échanges et correspondances des avocats et le droit au secret des sources journalistiques. Dans leurs écritures, les associations requérantes suggéraient au Conseil constitutionnel de reconnaître ces deux derniers droits comme des droits garantis par la Constitution au sens de l'article 61-1.

En ce qui concerne les atteintes au droit au secret des correspondances et à la liberté d'expression, le Conseil a jugé « *que les dispositions contestées instituent une procédure de réquisition administrative de données de connexion excluant l'accès au contenu des correspondances* » et en a conclu qu'elles ne sauraient méconnaître ces droits (cons. 17).

En ce qui concerne les atteintes au droit au respect de la vie privée, aux droits de la défense et au droit à un procès équitable, le Conseil a d'abord relevé les garanties encadrant la procédure de recueil des données de connexion en indiquant « *qu'outre qu'elle ne peut porter sur le contenu de correspondances, la procédure de réquisition administrative résultant des dispositions contestées est autorisée uniquement aux fins de recueillir 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 ; qu'elle est mise en œuvre par des agents spécialement habilités ; qu'elle est subordonnée à l'accord préalable d'une*

personnalité qualifiée, placée auprès du Premier ministre, désignée par la commission nationale de contrôle des interceptions de sécurité ; que, si l'autorisation de recueil des données en temps réel est délivrée par le Premier ministre, cette autorisation est soumise au contrôle de la commission nationale de contrôle des interceptions de sécurité ; que cette dernière dispose d'un accès permanent au dispositif de recueil des informations ou documents et adresse des recommandations au ministre de l'intérieur ou au Premier ministre lorsqu'elle constate un manquement aux règles édictées ou une atteinte aux droits et libertés ; qu'enfin, aux termes de l'article 226-13 du code pénal : "La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende" » (cons. 18).

Il en a conclu que « *le législateur a prévu des garanties suffisantes afin qu'il ne résulte pas de la procédure prévue aux articles L. 246-1 et L. 246-3 du code de la sécurité intérieure une atteinte disproportionnée au droit au respect de la vie privée, aux droits de la défense, au droit à un procès équitable, y compris pour les avocats et journalistes* » et il a donc écarté le grief tiré de l'incompétence négative affectant les dispositions contestées (cons. 19).

Il a, en conséquence, déclaré les dispositions contestées conformes à la Constitution (cons. 20).