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

CONSEIL CONSTITUTIONNEL

QUESTION PRIORITAIRE DE CONSTITUTIONNALITÉ

Sur la question transmise par décision du Conseil d'Etat en date du 17 mai 2017

Tendant à faire constater qu'en adoptant les dispositions de l'article L. 851-2 du code de la sécurité intérieure telle qu'elles résultent de la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste, le législateur a porté une atteinte disproportionnée au droit au respect de la vie privée et au secret des correspondances.

POUR : **1/ La Quadrature du Net**

2/ French Data Network

3/ La Fédération française des fournisseurs d'accès à Internet associatifs

SCP SPINOSI & SUREAU

Question n° 2017-648 QPC

DISCUSSION

I. Par décision en date du 17 mai 2017, le Conseil d'Etat a transmis au Conseil constitutionnel une question prioritaire de constitutionnalité posée à l'appui du recours formé par les associations exposantes tendant à l'annulation de la décision implicite de rejet de la demande d'abrogation du décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

Cette question a pour objet de faire constater la non-conformité à la Constitution des dispositions de l'article L. 851-2 du code de la sécurité intérieure, telle que modifiées par la loi n° 2016-987 du 21 juillet 2016, en ce qu'elles disposent :

« *I.-Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des informations ou documents mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée susceptible d'être en lien avec une menace. Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.*

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

II. Pour transmettre la question de constitutionnalité, le Conseil d'Etat a notamment relevé que :

« *Le moyen tiré de ce qu'elles portent atteinte aux droits et libertés garantis par la Constitution, et notamment au droit au respect de la vie privée garanti par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, soulève une question qui présente un caractère sérieux. Ainsi, il y a lieu de renvoyer au Conseil*

constitutionnel la question prioritaire de constitutionnalité invoquée » (CE, 17 mai 2017, n° 405792).

III. Au soutien de la présente question, les exposantes entendent faire valoir qu'en édictant les dispositions litigieuses, le législateur a porté une atteinte disproportionnée au droit au respect de la vie privée et au secret des correspondances et a par conséquent rompu l'équilibre entre ces droits constitutionnels et l'objectif constitutionnel de prévention des atteintes à l'ordre public et des infractions.

IV. D'emblée, et à titre liminaire, il n'est pas inutile de rappeler les conditions particulières de l'adoption de la loi du 21 juillet 2016, au regard notamment de celles dans lesquelles a été votée la loi du 24 juillet 2015 relative au renseignement qui est à l'origine de l'article L. 851-2 du code de la sécurité intérieure.

En effet, et d'un côté, la loi du 24 juillet 2015 a donné lieu à de nombreux travaux parlementaires ainsi qu'à des débats très fournis tant devant les deux chambres du Parlement que dans l'opinion publique.

Ainsi, après avoir fait l'objet d'un avis du Conseil d'Etat mais aussi d'une étude d'impact, le projet de loi a été discuté durant plus de trois mois au Parlement, du 19 mars au 24 juin 2015.

Au terme de ces débats, le Conseil constitutionnel a été saisi sur le fondement de l'article 61 de la Constitution.

Par contraste, et d'un autre côté, la loi du 21 juillet 2016 a quant à elle été adoptée dans l'urgence et après seulement deux jours de débats parlementaires, dans un contexte marqué par l'émotion suscitée par l'attentat de Nice le 14 juillet.

En outre, dans ce cadre temporel très étroit, les dispositions litigieuses ont été introduites par la voie d'un amendement parlementaire, de sorte qu'elles n'ont fait l'objet d'aucune étude d'impact et pas davantage d'un avis du Conseil d'État.

C'est en ayant à l'esprit la précipitation avec laquelle le législateur a considérablement élargi un dispositif de surveillance particulièrement intrusif qu'il convient d'en apprécier la constitutionnalité.

V. En droit et de jurisprudence constante, le Conseil constitutionnel considère qu'il « *incombe au législateur d'assurer la conciliation entre, d'une part, la prévention des atteintes à l'ordre public et des infractions, nécessaire à la sauvegarde de droits et de principes de valeur constitutionnelle, et, d'autre part, l'exercice des droits et des libertés constitutionnellement garantis* » (Cons. constit., Déc. n° 2015-713, 23 juillet 2015, cons. 2).

Or, le Conseil constitutionnel affirme avec la même constance que le droit au respect de la vie privée et le secret des correspondances sont protégés par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789 et figurent ainsi parmi les droits et libertés constitutionnellement garantis (Cons. constit., Déc. n° 2004-492 DC, 2 mars 2004, cons. 4).

Toujours en droit, dans le cadre de ce contrôle de la conciliation opérée par le législateur entre la prévention des atteintes à l'ordre public et le droit au respect de la vie privée, le Conseil constitutionnel a jugé que le dispositif de recueil d'informations en temps réel prévu par les dispositions de l'article L. 851-2 du code de la sécurité intérieure, dans sa version initiale, n'était pas contraire à la Constitution (Cons. constit., Déc. n° 2015-713, 23 juillet 2015, cons. 56 et 57).

En effet, le Conseil constitutionnel a considéré que « *lorsque le recueil des données a lieu en temps réel, il ne pourra être autorisé que pour les besoins de la prévention du terrorisme, pour une durée de deux mois renouvelable, uniquement à l'égard d'une personne préalablement identifiée comme présentant une menace et sans le recours à la procédure d'urgence absolue prévue à l'article L. 821-5 du même code ; que, par suite, le législateur a assorti la procédure de réquisition de données techniques de garanties propres à assurer entre, d'une part, le respect de la vie privée des personnes et, d'autre part, la prévention des atteintes à l'ordre public et celle des infractions, une conciliation qui n'est pas manifestement déséquilibrée* » (Déc. n° 2015-713 préc., cons. 56).

Ainsi, si le Conseil constitutionnel a jugé que cette conciliation n'était pas « *manifestement déséquilibrée* », c'est seulement après avoir énuméré les quatre caractéristiques du dispositif prévu qui lui sont apparues comme assurant cet équilibre.

Ces caractéristiques étaient :

- La circonstance que le recueil d'informations ne pourra être mis en œuvre qu'en vue de la prévention du terrorisme ;

- La circonstance que ce recueil en temps réel ne pourra être autorisé que pour une durée de deux mois renouvelable, à la différence des autres dispositifs de recueil d'informations en ligne qui peuvent être autorisés pour une durée de quatre mois renouvelable en application de l'article L. 821-4 du code de la sécurité intérieure ;

- La circonstance que ce recueil ne pourra concerner que les personnes préalablement identifiées comme présentant une menace ;

- La circonstance que la procédure d'urgence absolue prévue par l'article L. 821-5 du code de la sécurité intérieure ne serait pas applicable à ce recueil en temps réel.

Ces différentes caractéristiques, explicitement mentionnées par le Conseil constitutionnel dans sa décision, apparaissent comme ayant été déterminantes dans la déclaration de conformité à la Constitution des dispositions de l'article L. 851-2 du code de la sécurité intérieure.

VI. Or, **en l'occurrence**, il n'est pas inutile de rappeler que l'article L. 851-2 du code de la sécurité intérieure - dans sa rédaction issue de la loi du 21 juillet 2016 - ne présente plus les garanties indispensables au respect du droit au respect de la vie privée et au secret des correspondances.

En effet, cet article dispose désormais que :

« *I.-Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des informations ou documents mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée* ***susceptible d'être en lien avec une menace. Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.***

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

VI-1 En premier lieu, il ressort de ces dispositions que **le champ d'application personnel** de ce dispositif de recueil des informations en temps réel a été considérablement élargi.

Et ce, à au moins deux titres.

VI-1.1 D'une part, le dispositif de surveillance ne concerne plus seulement les « *personnes préalablement identifiées comme présentant une menace* » mais est étendu à toute personne identifiée comme « *susceptible d'être en lien* » avec une menace.

À elle seule, cette extension du champ d'application de l'article L. 851-2 du code de la sécurité intérieure justifierait sa censure tant elle élargit considérablement et de façon parfaitement imprécise le champ des personnes susceptibles d'être concernées par le dispositif.

En effet, **non seulement** le dispositif de surveillance en temps réel ne concerne désormais plus seulement des personnes dont il n'est pas établi qu'elles présentent une menace.

Il peut également viser des personnes dont il n'est même pas établi qu'elles seraient susceptibles d'être elles-mêmes en lien avec une menace.

Tout au plus suffit-il à l'administration de faire valoir qu'il existe des raisons sérieuses de penser que ces personnes seraient susceptibles de fournir des informations au titre de la prévention du terrorisme pour qu'elles soient elles-mêmes surveillées.

En d'autres termes, la surveillance d'une personne est totalement déconnectée de la menace que celle-ci pourrait représenter.

Mais **au surplus**, en usant de l'expression « *susceptible d'être en lien* » avec une menace, le législateur a permis aux autorités administratives compétentes de placer des personnes sous surveillance à la faveur de simples soupçons et autres hypothèses.

VI-1.2 D'autre part, les dispositions de loi du 21 juillet 2016 ont procédé à une autre extension encore plus importante du champ d'application personnel du dispositif de recueil des informations en temps réel, puisque l'article L. 851-2 du code de la sécurité intérieure vise désormais aussi les personnes appartenant à **l'entourage** de la personne concernée par l'autorisation.

Or, les dispositions litigieuses ne définissent aucunement cette notion.

Dans ces conditions, chaque citoyen – indépendamment même de son propre comportement – pourrait être visé par ce dispositif de surveillance.

Couplé avec le premier élargissement décrit précédemment, le seul fait qu'une personne soit regardée par les autorités administratives compétentes comme « *susceptible* » de fournir des informations sur celle-ci suffit donc désormais à justifier la surveillance.

Potentiellement, les dispositions contestées permettent ainsi de recueillir en temps réel les données de toutes les personnes appartenant à l'entourage d'une personne préalablement identifiée comme « *susceptible d'être en lien avec une menace* », ce qui revient à permettre un élargissement exponentiel d'un dispositif de

surveillance pourtant particulièrement intrusif et initialement conçu de façon restrictive.

Ce seul constat suffit à attester du caractère parfaitement disproportionné du nouveau dispositif prévu à l'article L. 851-2 du code de la sécurité intérieure et de l'atteinte qu'il porte aux droits et libertés que la Constitution garantit.

VI-1.3 Une telle conclusion ne saurait être infléchie par la circonstance que des interceptions administratives de correspondances électroniques visant « *l'entourage* » ont déjà été admises par le Conseil constitutionnel (Cons. constit. Déc. n° 2015-713 DC du 23 juillet 2015, cons. 64 à 67).

En effet, il est manifeste que le dispositif de surveillance en temps réel prévu par l'article L. 851-2 du code de la sécurité intérieure permet une surveillance nettement plus conséquente.

De fait, non seulement la surveillance des données de connexion permise notamment par les dispositions litigieuses ne saurait être réputée moins intrusive que l'accès au contenu des communications, dans la mesure où ces données révèlent en elles-mêmes quantité d'informations sur les faits et gestes d'un individu.

Entre autres analyses, et à titre d'illustration, la Cour de justice de l'Union européenne a ainsi relevé que :

« *Les données que doivent conserver les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, au titre des articles 3 et 5 de la directive 2006/24, sont, notamment, les données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent, notamment, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le*

temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée.

Ces données, prises dans leur ensemble, sont ***susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées****, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci* » (CJUE, G.C., 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a*, Aff. C-293/12 et C-594/12, § 26 et 27 – éclairée notamment par les éloquentes conclusions de l'avocat général VILLALON, en particulier § 73-74 - et CJUE, G.C., 21 déc. 2016, *Tele2 Sverige et al*., Aff. C-203/15 et C-698/15, § 101).

En outre, et à la différence du contenu des communications, ces données de connexion sont dites « structurées » et donc particulièrement propices à une exploitation en masse, non individualisée, à l'aide d'algorithmes et autres outils informatiques très puissants (« Big Data »), ce qui est de nature à renforcer l'ampleur de l'ingérence induite par ce type de surveillance.

Ainsi, comme le souligne Edward W. Felten, professeur en informatique à l'Université de Princeton, « *Les métadonnées téléphoniques sont faciles à agréger et analyser car elles sont, par nature, des données structurées […] les informations relatives à l'heure et la date associées au début et à la fin de chaque appel seront stockées dans un format prévisible et standardisé. […] La nature structurée des métadonnées facilite l'analyse d'ensembles massifs de données en utilisant des programmes sophistiqués d'exploitation de données et d'analyse de lien de causalité* » (Traduction libre de "*Telephony metadata is easy to aggregate and analyze because it is, by its nature, structured data […] the time and date information associated with the beginning and end of each call will be stored in a predictable, standardized format. […] The structured nature of metadata makes it easy to analyze massive datasets using sophisticated data-mining and link-analysis programs*." - Written Testimony of Edward W. Felten Professor of Computer Science and Public Affairs, Princeton University United States Senate, Committee

on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act October 2, 2013, p. 4).

Ainsi, les métadonnées, en raison des outils désormais disponibles pour les exploiter, exigent un haut niveau de protection et ce, à double titre : d'une part, au titre du droit au respect de la vie privée, en ce qu'elles révèlent des informations particulièrement sensibles sur la vie des personnes concernées; mais également, d'autre part, au titre du secret des correspondances, en ce qu'elles peuvent révéler *de facto* des informations substantielles sur la teneur du contenu des communications.

Certes, dans sa décision 2015-478 QPC, le Conseil constitutionnel retient, pour écarter les métadonnées du champ de protection du secret des correspondances, que « *les dispositions contestées instituent une procédure de réquisition administrative de données de connexion excluant l'accès au contenu des correspondances ; que, par suite, elles ne sauraient méconnaître le droit au secret des correspondances et la liberté d'expression* » (Conseil constit., Dec. n° 2015-478 QPC du 24 juillet 2015, cons. 17).

Cette exclusion du champ du secret des correspondances semble s'appuyer sur le caractère « technique » des métadonnées, les distinguant ainsi du « contenu » du message, qui constituerait l'unique objet à même de bénéficier de cette protection du secret des correspondances.

Or, en ce qui concerne les communications électroniques, cette dichotomie entre contenu et contenant n'est pas aussi stricte qu'il y paraît.

Ainsi, le simple fait que les données de connexion soient des données techniques ne saurait, de ce seul fait, les exclure du champ matériel de protection du secret des correspondances. C'est d'ailleurs la solution retenue dernièrement par le législateur (v. ainsi la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique modifiant notamment l'article L. 32-3 du code des postes et des communications électroniques).

En effet, ainsi que le résume M. Morell, l'ex-directeur adjoint de la CIA américaine :

« *Il n'y a pas de distinction nette entre les métadonnée et le contenu. C'est davantage un continuum* » (Traduction libre de "There's not a sharp distinction between metadata and content. It's more of a continuum" par M. Morell, ex-directeur adjoint de la CIA, *in* S. Ackerman, « NSA review panel casts doubt on bulk data collection claims », *The Guardian*, 14 janvier 2014).

Le Commissariat à la protection de la vie privée du Canada en conclut à juste titre que « *la ligne de séparation entre les métadonnées et le contenu réel d'une communication peut dès lors sembler illusoire* » (« Aperçu technique et juridique » de la question des métadonnée, Octobre 2014, disponible à l'adresse: https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2014/md_201410/).

De nombreuses études récentes démontrent la possibilité de déduire des informations importantes sur le contenu de correspondances privées à partir des données de connexion y afférant.

En utilisant les métadonnées des téléphones portables de participants volontaires, des chercheurs sont parvenus à déduire le contenu des communications passées par un individu en croisant plusieurs informations concernant uniquement les caractéristiques techniques de ses correspondances (date, heure et durée de l'appel, émetteur, destinataire etc.).

Dans ces exemples, dans le cas d'un participant B, à partir de la fréquence des appels reçus de la part d'une pharmacie spécifique, de ceux émis envers une assistance téléphonique pour les dispositifs de surveillance d'arythmie cardiaque et à un laboratoire médical, ainsi que la longueur de l'appel reçu de la part du service de cardiologie d'un centre médical régional, il est possible – pour quiconque ayant l'expertise et les moyens nécessaires, tels que des services de renseignement – de déduire l'objet et le contenu de chacune de ces correspondances.

De la même manière, pour une participante E, savoir qu'elle a émis un appel très tôt le matin à sa sœur, croisé aux appels répétés passés quelques jours plus tard à un service de planning familial à proximité,

révèle des éléments très précis sur la vie privée de cette personne et au delà, permet de déduire l'objet et le contenu de ses correspondances – avec un degré de certitude élevé et que l'agrégation de davantage de données de connexion ne fait qu'affiner (Voir "Evaluating the privacy properties of telephone metadata", J. Mayera, P. Mutchlera, and J.C. Mitchella, Edited by Cynthia Dwork, Microsoft Research Silicon Valley, Mountain View, CA, and approved March 1, 2016, p.5 , disponible à l'adresse : https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4878528/)

Cette approche rejoint, par ailleurs, l'interprétation retenue par le droit de l'Union, qui prévoit, dans la première phrase du considérant 26 de la directive 2002/58, que « *[l]es données relatives aux abonnés qui sont traitées dans des réseaux de communications électroniques pour établir des connexions et transmettre des informations contiennent des informations sur la vie privée des personnes physiques et* ***touchent au droit au secret de leur correspondance*** ».

Cette analyse est prolongée par l'article 5 de la même directive qui s'attache à décrire la confidentialité qui doit être garantie aux communications électroniques « *ainsi que la confidentialité des données relatives au trafic y afférentes* » (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 vie privée et communications électroniques)).

Dès lors, c'est autant au regard du respect de la vie privée que du secret des correspondances que les données de connexion des individus doivent être constitutionnellement protégés.

Enfin, et surtout, les dispositions contestées se distinguent des simples interceptions administratives – qui, outre le contenu des communications, incluent également les données de connexion – dans la mesure où celles-ci sont plafonnées au moyen d'un contingent (cf. le VI de l'article L. 852-1 du code de la sécurité intérieure). Or, ce plafond est inexistant en ce qui concerne la surveillance en temps réel des seules données de connexion.

C'est d'ailleurs précisément en raison du caractère particulièrement intrusif du dispositif litigieux qu'initialement, le législateur a limité

bien plus drastiquement son ampleur et que le Conseil constitutionnel n'a admis sa constitutionnalité qu'en raison de ces strictes limitations.

Ce faisant, le législateur a manifestement rompu, au détriment du respect de la vie privée des personnes et du secret des correspondances, l'équilibre qui avait été constaté par le Conseil constitutionnel dans sa décision DC n° 2015-713 précitée.

Car une fois encore, à l'aune du raisonnement retenu par le Conseil constitutionnel dans cette décision, il apparait explicitement que la stricte limitation du champ personnel du recueil des informations en temps réel aux seules personnes « *présentant une menace* » a été déterminante dans la déclaration de conformité à la Constitution de l'article L. 851-2 du code de la sécurité intérieure.

L'atteinte portée au droit au respect de la vie privée apparait ainsi totalement disproportionnée par rapport à l'objectif poursuivi, si éminent soit-il.

De ce seul chef, la censure des dispositions de l'article L. 851-2 du code de la sécurité intérieure est donc acquise.

Mais il y a plus.

VI-2 En second lieu, **le champ d'application temporel** du dispositif de recueil d'information en temps réel a lui aussi été excessivement élargi.

En supprimant l'alinéa qui prévoyait l'inapplication à ce dispositif de l'article L. 821-4 du code de la sécurité intérieure et qui n'autorisait le recueil en temps réel que pour une durée de deux mois renouvelable, le législateur a implicitement mais nécessairement permis au Gouvernement d'autoriser le recueil en temps réel pour une durée de quatre mois renouvelable, conformément à l'article L. 821-4 précité.

Or, la dérogation initiale à l'article L. 821-4 prévue pour le recueil en temps réel a également été déterminante dans la déclaration de conformité à la Constitution de l'article L. 851-2 du code de la sécurité intérieure par la décision DC n° 2015-713 précitée, dès lors

que celle-ci était explicitement motivée par cette dérogation (cf. Déc. n° 2015-713 préc., cons. 56).

En supprimant cette garantie qui assurait un équilibre entre la prévention des atteintes à l'ordre public et le respect de la vie privée, le législateur a porté une atteinte disproportionnée au droit au respect de la vie privée et au secret des correspondances.

De ce second chef, la censure des dispositions de l'article L. 851-2 du code de la sécurité intérieure s'impose.

VI-3 Enfin, et en tout état de cause, en supprimant deux des quatre garanties qui ont conduit le Conseil constitutionnel à considérer que la conciliation, par l'article L. 851-2 du code de la sécurité intérieure, entre la prévention des atteintes à l'ordre public et le respect de la vie privée n'était pas « *manifestement déséquilibré* », le législateur a nécessairement rompu cet équilibre.

Un tel constat est d'autant plus manifeste que l'élargissement considérable du champ d'application personnel et temporel du dispositif litigieux ne s'est accompagné d'aucun effort du législateur pour rétablir cet équilibre constaté par le Conseil constitutionnel.

VI-3.1 En effet, face à l'accroissement des potentialités invasives des mesures de surveillance en temps réel, strictement aucune garantie légale supplémentaire n'a été créée, ouvrant ainsi la voie à la généralisation d'un dispositif pourtant conçu initialement de façon restrictive.

Cette absence de garantie nouvelle est encore plus flagrante s'agissant de l'extension du dispositif aux membres de l'entourage, le régime juridique applicable à ces derniers étant identique à celui prévu pour les personnes prétendument censées représenter une menace.

VI-3.2 Par ailleurs, le seul fait qu'une telle mesure de surveillance soit autorisée par le Premier ministre sur simple avis de la CNCTR ne saurait en aucune façon constituer une garantie légale permettant d'éviter que des personnes soient visées en raison de simples soupçons.

En effet, non seulement l'autorisation de la mesure ne résulte pas de la décision d'un organe indépendant de l'exécutif, de sorte qu'aucun contrôle effectif n'est réalisé avant la mise œuvre de la surveillance et guère davantage ensuite.

Mais en tout état de cause, à supposer même qu'un tel contrôle ait été prévu par les dispositions litigieuses, il se serait irrémédiablement heurté au fait que l'expression « *susceptible de* » comporte une irréductible connotation hypothétique, laquelle permet à l'autorité compétente de se fonder sur de simples suppositions et non sur une menace caractérisée ou avérée.

En somme, et faute de précision et d'encadrement légal, l'autorité administrative dispose de toute latitude pour mettre en place la mesure litigieuse envers la première catégorie de personnes visées par l'article L. 851-2 du code de la sécurité intérieure.

Partant, l'article L. 851-2 du code de la sécurité intérieure a porté au droit au respect de la vie privée garanti par les articles 2 et 4 de la Déclaration des droits de l'homme et du citoyen du 26 août 1789 une atteinte parfaitement disproportionnée.

VII. En définitive et à l'aune de l'ensemble de ces éléments, les associations exposantes tiennent à souligner combien la modification expéditive des dispositions de l'article L. 851-2 du code de la sécurité intérieure par la loi n° 2016-987 du 21 juillet 2016 illustre à l'envi la logique d'extension continue des dispositifs de surveillance numérique, selon une démarche législative observée à maintes reprises dans le domaine des lois sécuritaires.

Dans un premier temps, le législateur créé un mécanisme de surveillance particulièrement invasif, mais tâche de convaincre de son caractère équilibré et donc de sa constitutionnalité en insistant sur l'existence de strictes limites quant à son champ d'application.

C'est d'ailleurs souvent à l'aune de ces strictes limites que la constitutionnalité de ce nouveau dispositif est finalement admise par le Conseil constitutionnel.

Puis, dans un second temps, au gré des circonstances et par petites touches, ce même législateur élargit progressivement ce mécanisme jusqu'à transformer ce qui n'était qu'un instrument exceptionnel en outil tout à fait usuel et habituel.

Dès lors, sauf à réduire à néant les impératifs protecteurs de la Constitution affirmés par le Conseil constitutionnel, un tel glissement législatif ne saurait être toléré tant il est riche en menaces.

Il résulte donc de tout ce qui précède que **la censure des dispositions litigieuses s'impose avec effet immédiat**.

PAR CES MOTIFS, et tous autres à produire, déduire ou suppléer, au besoin même d'office, les associations exposantes concluent à ce qu'il plaise au Conseil constitutionnel :

- **DECLARER** contraire à la Constitution les dispositions de l'article L. 851-2 du code de la sécurité intérieure telles qu'elles résultent de la loi n° 2016-987 du 21 juillet 2016.

  Avec toutes conséquences de droit.

SPINOSI & SUREAU

SCP d'Avocat au Conseil d'État