Commentaire

Décision n° 2021-924 QPC du 9 juillet 2021

La Quadrature du Net

(Communication d'informations entre services de renseignement et à destination de ces services)

Le Conseil constitutionnel a été saisi le 19 mai 2021 par le Conseil d'État (décision n° 431980 du même jour) d'une question prioritaire de constitutionnalité (QPC) posée par l'association la Quadrature du Net portant sur la conformité aux droits et libertés que la Constitution garantit de l'article L. 863-2 du code de la sécurité intérieure (CSI), dans sa rédaction résultant de la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste.

Dans sa décision n° 2021-924 QPC du 9 juillet 2021, le Conseil constitutionnel a déclaré contraire à la Constitution le deuxième alinéa de cet article, dans cette rédaction, et a jugé conformes à la Constitution ses premier et troisième alinéas dans cette même rédaction.

I. – Les dispositions contestées

A. – Historique et objet des dispositions contestées

1. – Les traitements de données personnelles mis en œuvre par les services de renseignement

* La politique publique de renseignement est définie à l'article L. 811-1 du CSI. Elle *« concourt à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation »*.

Participent à cette politique deux types de services :

- les services spécialisés de renseignement, dits du *« premier cercle »* qui sont désignés par décret en Conseil d'État et *« ont pour missions, en France et à l'étranger, la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques*

ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. Ils contribuent à la connaissance et à l'anticipation de ces enjeux ainsi qu'à la prévention et à l'entrave de ces risques et de ces menaces »[1] . Ils peuvent en principe recourir à l'ensemble des techniques pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation énumérés à l'article L. 811-3 du CSI ;

- les services, autres que les services spécialisés de renseignement, relevant des ministres de la défense, de l'intérieur et de la justice ainsi que des ministères chargés de l'économie, du budget ou des douanes. Il s'agit des services dits du « *second cercle »*. Ils sont autorisés à recourir à certaines techniques de renseignement pour certaines des finalités énumérées à l'article L. 811-3[2].

***** Les services de renseignement sont amenés, dans le cadre des missions qui leur sont confiées, à procéder à de nombreux traitements de données personnelles[3] soumis soit à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[4], soit, lorsque sont mises en œuvre les techniques de renseignement instituées par le livre VIII du CSI, aux articles L. 821-1 et suivants de ce code issus principalement de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement. Ce cadre légal vise à concilier le droit au respect de la vie privée des personnes dont les données sont exploitées et la protection des intérêts fondamentaux de la Nation.

---

[1] Ce premier cercle, mentionné à l'article L. 811-2 du CSI, regroupe six services : la direction générale de la sécurité extérieure (DGSE), la direction du renseignement et de la sécurité de la défense (DRSD) et la direction du renseignement militaire (DRM), qui relèvent du ministère des armées ; la direction générale de la sécurité intérieure (DGSI), qui relève du ministère de l'intérieur ; la direction nationale du renseignement et des enquêtes douanières (DNDRED) et le service de *« traitement du renseignement et action contre les circuits financiers clandestins »* (Tracfin), qui relèvent du ministère de l'économie et des finances.

[2] Ce second cercle regroupe des services très différents désignés par décret en Conseil d'État, pris après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR), qui ne peuvent recourir aux techniques de renseignement que pour certaines finalités (article L. 811-4 du CSI). Ils relèvent notamment de la direction générale de la police nationale, de la direction générale de la gendarmerie nationale, de la préfecture de police, de certaines sections du ministère de la défense ou de la direction de l'administration pénitentiaire. Ces services peuvent ne pas avoir une activité exclusivement portée sur le renseignement.

[3] Il résulte de l'article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après *« loi informatique et libertés »*), tel qu'interprété à la lumière de l'article 4.2 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), que constitue un traitement de données à caractère personnel, *« sauf disposition contraire »*, *« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »*.

[4] Cette loi renvoie notamment au décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 33 de la loi n° 78-17 du 6 janvier 1978.

- À ce titre, le livre VIII du CSI, intitulé *« Du renseignement »*, comporte un article L. 801-1 du CSI qui rappelle que *« Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité ».* Il fixe, en conséquence, les conditions dans lesquelles l'autorisation et la mise en œuvre des techniques de recueil de renseignement[5] peuvent être décidées : elles doivent ainsi procéder d'une autorité ayant légalement compétence pour y recourir, résulter d'une procédure conforme au titre II du livre VIII[6], respecter les missions confiées aux services de renseignement et être justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation. Par ailleurs, les atteintes qu'elles portent au respect de la vie privée doivent être proportionnées aux motifs invoqués.

La Commission nationale de contrôle des techniques de renseignement (CNCTR) s'assure du respect de ces principes. À cette fin, elle dispose notamment *« d'un accès permanent, complet et direct aux relevés, registres, renseignements collectés, transcriptions et extractions mentionnés au présent livre, ainsi qu'aux dispositifs de traçabilité des renseignements collectés et aux locaux où sont centralisés ces renseignements en application de l'article L. 822-1 »*[7].

Le cadre légal applicable au renseignement est strictement défini : les finalités pouvant être poursuivies dans le cadre de la défense et de la promotion des intérêts fondamentaux de la Nation sont limitativement énumérées[8] et le recours à ces

[5] Ces différentes techniques sont prévues par le titre V du livre VIII du CSI. Elles comportent les techniques d'accès administratif aux données de connexion (articles L. 851-1 à L. 851-7), les interceptions de sécurité (articles L. 852-1 à L. 852-2), la sonorisation de certains lieux et véhicules ainsi que la captation d'images et de données informatiques (articles L. 853-1 à L. 853-3), les mesures de surveillance des communications électroniques internationales (articles L. 854-1 à L. 854-9) et les mesures de surveillance de certaines communications hertziennes (articles L. 855-1 A à L. 855-1 C).

[6] Ce titre traite des procédures d'autorisation préalable pour recourir aux techniques de recueil de renseignement (voir ci-après).

[7] Article L. 833-2 du CSI.

[8] Ces finalités sont mentionnées à l'article L. 811-3 du CSI : *« 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ; /2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ; / 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ; / 4° La prévention du terrorisme ; / 5° La prévention : / a) Des atteintes à la forme républicaine des institutions ; / b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ; / c) Des violences collectives de nature à porter gravement atteinte à la paix publique ; / 6° La prévention de la criminalité et de la délinquance organisées ; / 7° La prévention de la prolifération des armes de destruction massive ».* Par ailleurs, l'article L. 855-1 permet au service national du renseignement pénitentiaire de recourir à ces techniques pour deux finalités particulières : la prévention des évasions et la sécurité des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues.

techniques fait l'objet d'une autorisation préalable par le Premier ministre, après avis de la CNCTR, portant sur des agents individuellement désignés et habilités (sauf en cas de procédure dite de *« l'urgence absolue »* permettant de déroger sous certaines conditions à l'avis de cette commission)[9]. Par ailleurs, la durée de cette autorisation[10] et de conservation des données recueillies[11] ainsi que les modalités de mises en œuvre de ces techniques sont précisément définies.

Enfin, les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles prévues par le CSI, ces opérations étant soumises au contrôle de la CNCTR. Par ailleurs, ils doivent être détruits dès que leur conservation n'est plus indispensable à la poursuite de ces finalités[12].

Si plusieurs dispositions ont modifié ce cadre depuis 2015, notamment pour remédier à des censures du Conseil constitutionnel ou pour adapter certaines dispositions à des besoins nouveaux, ses principaux équilibres ont été conservés.

- Au-delà de ce cadre légal spécifique aux techniques de renseignement[13], les traitements de données personnelles mis en œuvre par les services de renseignement peuvent également être soumis aux dispositions de la loi du 6 janvier 1978 relatives aux traitements intéressant la sûreté de l'État et la défense, en particulier lorsqu'ils sont autorisés à accéder à des fichiers poursuivant des finalités ne relevant pas du renseignement[14].

---

[9] Titre II du livre VIII précité, et notamment son article L. 821-1. Pour mémoire, le Conseil constitutionnel a censuré dans sa décision n° 2015-713 DC du 23 juillet 2015, *Loi relative au renseignement*, une procédure dite de *« l'urgence opérationnelle »* qui permettait de déroger à cette procédure d'autorisation dans le cadre de certaines opérations, sans information préalable du Premier ministre ou de la CNCTR. Il a en effet considéré qu'au regard des conditions dans lesquelles cette dérogation pouvait s'appliquer, l'atteinte au droit au respect de la vie privée et au secret des correspondances pouvant en résulter était manifestement disproportionnée.

[10] En application de l'article L. 821-4 du CSI, la durée de droit commun d'autorisation de mise en œuvre des techniques de renseignement est de quatre mois, réduite à deux mois ou moins pour les techniques les plus intrusives (par exemple, 48 heures pour l'utilisation d'un IMSI-catcher permettant d'intercepter des correspondances dans un rayon déterminé).

[11] L'article L. 822-2 du CSI fixe cette durée de 30 jours à quatre ans selon les données collectées et sous réserve de certaines dérogations.

[12] Article L. 822-3 du CSI.

[13] Les traitements de données personnelles à des fins de renseignement ne relèvent pas du *« paquet européen de protection des données personnelles »* constitué du RGPD et de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (directive « Police-Justice »).

[14] Par exemple, le traitement des antécédents judiciaires, le système européen de traitement des données d'enregistrement et de réservation, *etc*. Ces traitements sont soumis aux règles générales en matière de protection des données personnelles prévues notamment à l'article 4 de la loi du 6 janvier 1978 : ces dernières doivent ainsi être *« collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités », « adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées (…) non excessives », « exactes et, si nécessaire, tenues à jour », « conservées sous une forme permettant*

À ce titre, l'article 31 de la loi du 6 janvier 1978 prévoit un régime commun pour les traitements mis en œuvre pour le compte de l'État concernant *« la sûreté de l'État, la défense ou la sécurité publique »* ou *« la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté »*.

L'autorisation pour mettre en œuvre de tels traitements relève soit du ministre compétent après avis de la CNIL, soit d'un décret en Conseil d'État, pris après avis de cette commission, s'ils portent sur des données sensibles[15]. Certains de ces traitements peuvent toutefois être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise, seul le sens de l'avis émis par la CNIL étant alors publié[16]. Ce décret peut également dispenser le traitement de tout contrôle *a posteriori* par la CNIL[17].

S'ils sont autorisés par voie réglementaire, ils demeurent assujettis aux dispositions générales de la loi du 6 janvier 1978 et à certaines garanties reconnues aux personnes dont les données sont traitées.

2. – Le partage d'informations entre services de renseignement et la communication d'informations à ces services (les dispositions renvoyées)

a. – Présentation des dispositions

* L'article L. 863-2 du CSI résulte d'un amendement présenté dans le cadre de l'examen de la loi du 24 juillet 2015 précitée par le rapporteur de l'Assemblée nationale, M. Jean-Jacques Urvoas, pour améliorer l'information des services de renseignement. Après avoir souligné que *« le Gouvernement estime […] que les échanges entre [l'administration pénitentiaire et les services de renseignement] ne sont actuellement pas permis par la loi »* et que *« cette logique explique d'ailleurs*

---

l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées » et *« Traitées de façon à garantir une sécurité appropriée des données à caractère personnel ».*

[15] Les données sensibles sont les données mentionnées au paragraphe I de l'article 6 de la loi *« informatique et libertés »*, à savoir celles portant sur la *« prétendue origine raciale ou l'origine ethnique »*, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique, les données génétiques, les données biométriques, les données de santé, ainsi que la vie sexuelle ou l'orientation sexuelle d'une personne physique.

[16] C'est le décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 33 de la loi du 6 janvier 1978 qui établit, actuellement, la liste des traitements ayant bénéficié d'une telle dispense de publication.

[17] Article 19, paragraphe IV, de la loi *« informatique et libertés ».* Les traitements concernés, comme ceux mis en œuvre en application du titre VIII du CSI peuvent, en tout état de cause, faire l'objet de recours devant la formation spécialisée du Conseil d'État créée par la loi du 24 juillet 2015 relative au renseignement.

que les capacités d'échange d'informations aient été précisées par la loi uniquement pour Tracfin à l'article L. 561-29 du code monétaire et financier », l'auteur de l'amendement considérait qu'il s'agissait, par son adoption, *« d'éviter tout risque de raisonnement* a contrario *et de maintenir les capacités de dialogue entre les administrations publiques sur des thématiques décisives pour la sécurité de nos concitoyens »*[18].

La garde des sceaux de l'époque, Mme Christiane Taubira, avait considéré qu'*« Il est incontestable que cet amendement permet d'améliorer et de sécuriser juridiquement les échanges d'informations et la capacité opérationnelle des services »*, tout en indiquant qu'il restait *« simplement à encadrer plus précisément les échanges. L'expertise qui a été conduite nous amène à penser qu'un décret en Conseil d'État devrait en déterminer les modalités »*[19].

* Le premier alinéa de l'article L. 863-2 du CSI permet ainsi aux services de renseignement du premier et du second cercles de partager *« toutes les informations utiles à l'accomplissement de leurs missions définies au titre I^er [du livre VIII du CSI] ».*

Comme précédemment rappelé, ce titre définit, de manière générale, les missions poursuivies par les services de renseignement et les finalités justifiant la mise en œuvre de techniques de renseignement. Ces dispositions doivent donc s'entendre comme limitant ce partage au respect des missions respectives de chacun des services intéressés. Par ailleurs, la notion d'informations utiles peut couvrir un champ de données plus larges que celles issues des seules techniques de renseignement.

* Le deuxième alinéa de l'article L. 863-2 du CSI prévoit, quant à lui, que certaines administrations publiques *« peuvent transmettre »* à ces services de renseignement, *« de leur propre initiative ou sur requête de ces derniers »,* des informations utiles à l'accomplissement de leurs missions. Par renvoi à l'article 1^er de l'ordonnance du 8 décembre 2005[20], sont concernés les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes de protection sociale et les organismes chargés de la gestion d'un service public administratif.

Il résulte de ces dispositions que *« lorsqu'elles seraient sollicitées par les services*

[18] Compte-rendu des débats, première séance du jeudi 16 avril 2015.
[19] *Ibidem*.
[20] Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

de renseignement, les administrations concernées pourraient refuser de fournir les éléments demandés »[21]. Ces dispositions ne précisent toutefois pas si l'administration publique doit justifier ce refus ni les motifs qui pourraient le fonder.

* Enfin, le troisième alinéa de l'article L. 863-2 renvoie à un décret en Conseil d'État la définition des modalités et des conditions de l'application de cet article. Ce décret est le seul décret d'application de la loi du 24 juillet 2015 à n'avoir pas été publié à ce jour.

Ajoutons, pour finir, que ces dispositions ont été récemment modifiées par l'article 9 de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

B. – Origine de la QPC et question posée

L'association La Quadrature du Net avait saisi le Conseil d'État d'un recours pour excès de pouvoir contre un acte administratif, non publié mais révélé par voie de presse[22], qui était présenté comme permettant la mise en œuvre d'un partage d'informations entre les services de renseignement et la transmission d'informations par certaines administrations à ces services, tels que prévus par l'article L. 863-2 du CSI.

À cette occasion, elle avait soulevé une QPC à l'encontre de cet article.

Par sa décision précitée du 19 mai 2021, le Conseil d'État avait jugé que *« le grief tiré de ce que, faute de déterminer les conditions d'exploitation et de conservation des données susceptibles d'être transmises et partagées sur le fondement de l'article L. 863-2 du code de la sécurité intérieure, le législateur aurait méconnu l'étendue de sa compétence et affecté, ce faisant, le droit au respect de la vie privée et le secret des correspondances, soulève une question présentant un caractère sérieux.»*. Il l'avait dès lors renvoyée au Conseil constitutionnel.

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

[21] Sénat, rapport n° 460 (2014-2015) de M. Philippe BAS, fait au nom de la commission des lois, déposé le 20 mai 2015.

[22] L'association requérante s'appuyait sur un article publié le 24 avril 2019 par le journal *Le Monde*, intitulé *«* "L'entrepôt"*, bâtiment ultrasécurisé et outil essentiel du renseignement français »*, dans lequel le journaliste Jacques Follorou décrivait un dispositif de stockage et de partage d'informations collectées par différents services de renseignement. Ce dispositif était présenté comme étant mis en œuvre par la DGSE sur le fondement de l'article L. 863-2 du CSI.

* L'association requérante, rejointe par l'association intervenante, soutenait qu'en autorisant le partage d'informations entre services de renseignement et la communication d'informations par certaines administrations à ces derniers sans encadrer ces pratiques par aucune garantie, le législateur était resté en deçà de sa compétence et avait ainsi méconnu le droit au respect de la vie privée, la protection des données personnelles, le secret des correspondances et la liberté d'expression.

À l'appui de ces griefs, l'association reprochait notamment aux dispositions renvoyées de ne pas définir les informations pouvant être partagées, les catégories de personnes pouvant y accéder, les finalités de ce partage ainsi que son régime juridique. En outre, la requérante dénonçait l'absence de contrôle par la CNCTR.

A. – La jurisprudence du Conseil constitutionnel relative au droit au respect de la vie privée

Depuis 1999, le Conseil constitutionnel rattache 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[23]. La notion de *« vie privée »* est entendue par le Conseil constitutionnel de façon classique : c'est la sphère d'intimité de chacun.

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 »*[24]. Il déduit plus spécifiquement du droit au respect de la vie privée, en ce qui concerne la mise en œuvre de traitements de données à caractère personnel, que *« la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif »*[25].

[23] 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.
[24] Décision n° 2011-209 QPC du 17 janvier 2012, *M. Jean-Claude G. (Procédure de dessaisissement d'armes)*, cons. 3.
[25] Décision n° 2012-652 DC du 22 mars 2012, *Loi relative à la protection de l'identité*, cons. 8 ou, plus récemment, décision n° 2019-797 QPC, *Unicef France et autres (Création d'un fichier des ressortissants étrangers se déclarant mineurs non accompagnés)*, paragr. 4, décision n° 2021-817 DC du 20 mai 2021, *Loi pour une sécurité globale préservant les libertés*, paragr. 86, et décision n° 2021-819 DC du 31 mai 2021, *Loi relative à la gestion de la sortie de crise sanitaire*, paragr. 24.

Par ailleurs, le Conseil tient compte de la sensibilité des données traitées, notamment lorsque sont en cause des données médicales[26] ou des données de connexion[27]. Il s'assure également du lien direct entre les données dont le traitement est autorisé et la finalité poursuivie par le législateur[28]. À ce titre, il exige du législateur qu'il définisse avec suffisamment de précision les conditions des atteintes portées à la vie privée.

Sur le fondement du droit au respect de la vie privée, le Conseil a déjà été amené à contrôler des dispositions portant sur la mise en place d'un dispositif de collecte et d'enregistrement de données à caractère personnel et parmi elles, celles permettant la mise en œuvre de certaines techniques de renseignement, des dispositions autorisant un droit de communication au bénéfice de certaines autorités administratives ou enfin des dispositions organisant un partage de données personnelles entre personnes publiques.

1. – Le contrôle des fichiers et traitements de données personnelles

* Dans sa décision n° 2020-800 DC du 11 mai 2020[29], le Conseil s'est prononcé sur le traitement et le partage des données à caractère personnel relatives à la santé des personnes atteintes par le virus de la covid-19 et des personnes en contact avec elles, sans leur consentement, par des organismes et des professionnels de santé. Après avoir relevé que le législateur avait poursuivi l'objectif de valeur constitutionnelle de protection de la santé, le Conseil a constaté qu'il avait prévu des garanties suffisantes pour assurer que ces dispositions ne méconnaissent pas le droit au respect de la vie privée.

En l'espèce, la collecte, le traitement et le partage des données personnelles ne pouvaient ainsi être mis en œuvre que pour des finalités précises et pour une durée limitée, les données recueillies devaient être strictement nécessaires à ces finalités, les organismes et personnes pouvant accéder à ces données étaient limitativement énumérées, tandis que l'accès à ces données devait être nécessaire à leur intervention

[26] Il a ainsi affirmé que *« Lorsque sont en cause des données à caractère personnel de nature médicale, une particulière vigilance doit être observée dans la conduite de ces opérations et la détermination de leurs modalités »* (décision n° 2020-808 DC du 13 novembre 2020, *Loi autorisant la prorogation de l'état d'urgence sanitaire et portant diverses mesures de gestion de la crise sanitaire*, paragr. 18).

[27] Le Conseil a notamment relevé, concernant les données de connexion, que *« compte tenu de leur nature et des traitements dont elles peuvent faire l'objet, de telles données fournissent sur les personnes en cause des informations nombreuses et précises, particulièrement attentatoires à leur vie privée »* (décision n° 2020-841 QPC du 20 mai 2020, *La Quadrature du Net et autres [Droit de communication à la Hadopi]*, paragr. 17).

[28] Décision n° 2019-789 QPC du 14 juin 2019, *Mme Hanen S. (Droit de communication des organismes de sécurité sociale)*, paragr. 13.

[29] Décision n° 2020-800 DC du 11 mai 2020, *Loi prorogeant l'état d'urgence sanitaire et complétant ses dispositions*, paragr. 62 à 78.

et ces personnes ou les agents des organismes intéressés étaient soumis au secret professionnel[30]. Ces traitements étaient également limités dans le temps.

Par ailleurs, le Conseil a précisé, d'une part, que si les dispositions contestées *« exemptent la collecte, le traitement et le partage des données de santé de l'obligation d'obtenir le consentement des intéressés, elles n'exemptent pas ces mêmes opérations du respect des dispositions du règlement du 27 avril 2016 […] et de la loi du 6 janvier 1978 […], notamment leurs droits d'accès, d'information et de rectification »* et d'autre part, qu'il appartient *« au pouvoir réglementaire de définir des modalités de collecte, de traitement et de partage des informations assurant leur stricte confidentialité et, notamment, l'habilitation spécifique des agents chargés, au sein de chaque organisme, de participer à la mise en œuvre du système d'information ainsi que la traçabilité des accès à ce système d'information »*[31].

Dans le cadre de ce contrôle, le Conseil a déjà admis, dans sa décision n° 2019-797 QPC du 26 juillet 2019 relative à la création d'un fichier concernant les mineurs non accompagnés[32], le renvoi général, même implicite, aux dispositions de la loi du 6 janvier 1978[33] et des renvois à des dispositions réglementaires. En l'occurrence, pour examiner le caractère adéquat et proportionné des dispositions contestées à l'objectif poursuivi, le Conseil s'était assuré que les données recueillies étaient *« nécessaires à l'identification de la personne »* et que *« le fichier instauré par les dispositions contestées est mis en œuvre dans le respect de la loi du 6 janvier 1978 »*.

Dans une décision du 13 mars 2003[34], le Conseil, après avoir contrôlé la conformité à la Constitution d'un fichier des antécédents judiciaires, a écarté le grief tiré de l'incompétence négative en jugeant *« que, loin d'avoir méconnu l'étendue de sa compétence, le législateur a assorti les dispositions critiquées de précisions dont*

[30] La communication des données recueillies à des tiers étant sanctionnée pénalement.
[31] Le législateur avait, à ce titre, expressément renvoyé à un décret en Conseil d'État *« les modalités d'exercice des droits d'accès, d'information, d'opposition et de rectification des personnes concernées, celles atteintes par le virus ou celles en contact avec ces dernières, lorsque leurs données personnelles sont collectées dans ces systèmes d'information à l'initiative de tiers »*.
[32] Décision n° 2019-797 QPC du 26 juillet 2019, *Unicef France et autres (Création d'un fichier des ressortissants étrangers se déclarant mineurs non accompagnés)*, paragr. 8 à 10.
[33] Le Conseil contrôle en revanche l'éventuelle incompétence négative dont les dispositions de cette loi pourraient être entachées : voir par exemple décision n° 2004-499 DC du 29 juillet 2004, *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* cons. 11, dans laquelle il avait considéré que le législateur n'avait pas prévu *« les garanties appropriées et spécifiques aux exigences de l'article 34 de la Constitution »* nécessaires pour permettre à une personne morale de droit privée de collecter, sous certaines conditions, des données relatives à des infractions pénales.
[34] Décision n° 2003-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*, cons. 45.

certaines relèvent du pouvoir réglementaire et qui, au demeurant, avaient jusqu'ici été traitées comme telles ».

De même, le Conseil, dans une décision du 29 décembre 2013[35], a validé la création d'un fichier dans le domaine des contrats d'assurance-vie en jugeant que *« si la mise en œuvre des dispositions de l'article 10 doit conduire à la création d'un traitement de données à caractère personnel des informations ainsi recueillies, il ressort des débats parlementaires, qu'en adoptant ces dispositions, le législateur n'a pas entendu déroger aux garanties apportées par la loi du 6 janvier 1978 susvisée relatives notamment aux pouvoirs de la Commission nationale de l'informatique et des libertés, qui s'appliqueront aux traitements en cause ; que, par suite, il appartiendra aux autorités compétentes, dans le respect de ces garanties et sous le contrôle de la juridiction compétente, de s'assurer que la collecte, l'enregistrement, la conservation, la consultation, la communication, la contestation et la rectification des données de ce fichier des contrats d'assurance-vie seront mis en œuvre de manière adéquate et proportionnée à l'objectif poursuivi »*.

Dans sa décision du 16 juin 2017, le Conseil a validé les dispositions prévoyant l'établissement d'un fichier des personnes qui ont contrevenu ou contreviennent aux dispositions des conditions générales de vente ou du règlement intérieur relatives à la sécurité des manifestations sportives. Examinant des dispositions législatives qui renvoyaient à un décret en Conseil d'État la nature des données ainsi que les règles de conservation et de consultation, le Conseil a, après avoir constaté l'existence d'un objectif d'intérêt général, jugé que le législateur *« n'a pas entendu déroger aux garanties apportées par la loi du 6 janvier 1978 […] relatives notamment aux pouvoirs de la Commission nationale de l'informatique et des libertés, qui s'appliquent aux traitements en cause. / Le fichier prévu par les dispositions contestées ne peut être établi que par les organisateurs de manifestations sportives à but lucratif. Il ne peut recenser que les personnes qui ont contrevenu ou contreviennent aux dispositions des conditions générales de vente ou du règlement intérieur relatives à la sécurité de ces manifestations. Il ne peut être employé à d'autres fins que l'identification desdites personnes en vue de leur refuser l'accès à des manifestations sportives à but lucratif. Il en résulte que le traitement de données prévu par les dispositions contestées est mis en œuvre de manière adéquate et proportionnée à l'objectif d'intérêt général poursuivi »*[36].

[35] Décision n° 2013-684 DC du 29 décembre 2013, *Loi de finances rectificative pour 2013*, cons. 13.
[36] Décision n° 2017-637 QPC du 16 juin 2017, *Association nationale des supporters (Refus d'accès à une enceinte sportive et fichier d'exclusion)*, paragr. 13 et 14.

* De manière plus spécifique, le Conseil a également été amené à se prononcer sur le traitement de données personnelles opéré dans le cadre de la mise en œuvre des techniques de renseignement.

Dans sa décision n° 2015-713 DC du 23 juillet 2015 concernant la loi relative au renseignement, le Conseil constitutionnel a validé les dispositions relatives aux conditions de mise en œuvre de la plupart des techniques de renseignement en prenant en compte les garanties particulières prévues par le législateur.

À titre général, le Conseil a jugé que le recueil de données au moyen des techniques de renseignement *« par les services spécialisés de renseignement pour l'exercice de leurs missions respectives relève de la seule police administrative »*. Il a dès lors considéré *« qu'il ne peut donc avoir d'autre but que de préserver l'ordre public et de prévenir les infractions »* et *« qu'il ne peut être mis en œuvre pour constater des infractions à la loi pénale, en rassembler les preuves ou en rechercher les auteurs »*[37].

Le Conseil a ensuite tenu compte de l'encadrement strict, d'une part, des finalités pouvant justifier la mise en œuvre de ces techniques et, d'autre part, des services pouvant y recourir, de l'institution d'une procédure d'autorisation préalable par le Premier ministre, de la durée limitée de l'autorisation accordée, des contrôles exercés par la CNCTR et des mesures de traçabilité des techniques mises en œuvre.

En revanche, le Conseil a censuré les dispositions relatives à la surveillance des communications émises ou reçues à l'étranger prévues au paragraphe I de L. 854-1 du CSI aux seules fins de protection des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code.

Le Conseil constitutionnel a, par conséquent, jugé *« qu'en ne définissant dans la loi ni les conditions d'exploitation, de conservation et de destruction des renseignements collectés en application de l'article L. 854-1, ni celles du contrôle par la commission nationale de contrôle des techniques de renseignement de la légalité des autorisations délivrées en application de ce même article et de leurs conditions de mise en œuvre, le législateur n'a pas déterminé les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques »*. Il en a conclu que les dispositions du paragraphe I de l'article L. 854-1 méconnaissaient l'article 34 de la Constitution et devaient être déclarées contraires à la Constitution[38].

[37] Décision n° 2015-713 DC du 23 juillet 2015, *Loi relative au renseignement*, cons. 9.
[38] *Ibidem*, cons. 78.

Saisi d'une nouvelle rédaction de ces dispositions dans sa décision n° 2015-722 DC du 26 novembre 2015 concernant la loi relative aux mesures de surveillance des communications électroniques internationales, le Conseil constitutionnel les a, cette fois, validées au motif *« que le législateur a précisément défini les conditions de mise en œuvre de mesures de surveillance des communications électroniques internationales, celles d'exploitation, de conservation et de destruction des renseignements collectés ainsi que celles du contrôle exercé par la commission nationale de contrôle des techniques de renseignement ; que ces dispositions doivent être déclarées conformes à la Constitution »*[39].

Enfin, dans sa décision n° 2016-590 QPC du 21 octobre 2016[40], le Conseil a censuré des dispositions relatives à la surveillance et au contrôle des transmissions empruntant la voie hertzienne à des fins de défense des intérêts nationaux. Après avoir relevé qu'elles n'étaient soumises ni aux dispositions relatives au renseignement figurant au livre VIII du CSI ni aux dispositions du code pénal qui encadrent les interceptions de correspondances émises par la voie de communications électroniques prescrites par un juge d'instruction, il a constaté que le recours à ces mesures de surveillance n'était soumis à aucune condition de fond ni de procédure et que leur mise en œuvre n'était encadrée d'aucune garantie.

2. – Le contrôle de prérogatives conférant un droit de communication à l'administration

Le Conseil constitutionnel s'est prononcé à plusieurs reprises sur des dispositions prévoyant un droit de communication au profit de certaines personnes publiques ou autorités administratives indépendantes.

Dans sa décision n° 2015-715 DC du 5 août 2015, le Conseil s'est prononcé sur des décisions prévoyant la communication de données de connexion à des agents de l'Autorité de la concurrence. Après avoir rappelé qu'une telle communication est de nature à porter atteinte au droit au respect de la vie privée de la personne intéressée, le Conseil a relevé que si le législateur avait réservé cette communication à des agents habilités et soumis au respect du secret professionnel, il n'avait assorti cette procédure d'aucune autre garantie et que *« le fait que les opérateurs et prestataires ne sont pas tenus de communiquer les données de connexion de leurs clients ne saurait constituer une garantie pour ces derniers »*. Par conséquent, il a jugé que ces

[39] Décision n° 2015-722 DC du 26 novembre 2015 précitée, cons. 15.
[40] Décision n° 2016-590 QPC du 21 octobre 2016, *La Quadrature du Net et autres (Surveillance et contrôle des transmissions empruntant la voie hertzienne)*, cons. 5 à 8.

dispositions ne permettaient pas une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions[41].

Dans sa décision n° 2019-789 QPC du 14 juin 2019, le Conseil était saisi de dispositions octroyant à certains agents des organismes de sécurité sociale un droit de communication leur permettant d'obtenir, d'une part, des établissements bancaires, les relevés de comptes et autres documents bancaires relatifs au bénéficiaire d'une prestation sociale et, d'autre part, des opérateurs de communications électroniques, des fournisseurs d'accès à un service de communication au public en ligne ou des hébergeurs de contenu, les données de connexion détenues d'un bénéficiaire.

Distinguant selon la nature des données communiquées, le Conseil a validé celles de ces dispositions qui permettaient la communication des données bancaires en jugeant : *« En premier lieu, en adoptant les dispositions contestées, le législateur a poursuivi l'objectif de valeur constitutionnelle de lutte contre la fraude en matière de protection sociale. / En deuxième lieu, d'une part, en vertu de l'article L. 114-19 du code de la sécurité sociale, il ne peut être fait usage du droit de communication que pour le contrôle de la sincérité et de l'exactitude des déclarations souscrites ou de l'authenticité des pièces produites en vue de l'attribution et du paiement des prestations servies par les organismes de sécurité sociale, pour l'exercice des missions de contrôle des cotisants aux régimes obligatoires de sécurité sociale et de lutte contre le travail dissimulé et pour le recouvrement de prestations versées indûment à des tiers. / D'autre part, ce droit de communication, qui n'est pas assorti d'un pouvoir d'exécution forcée, n'est ouvert qu'aux agents des organismes de sécurité sociale, lesquels sont soumis, dans l'utilisation de ces données, au secret professionnel. / En dernier lieu, la communication de données bancaires permet à titre principal aux organismes sociaux d'avoir connaissance des revenus, des dépenses et de la situation familiale de la personne objet de l'investigation. Elle présente un lien direct avec l'évaluation de la situation de l'intéressé au regard du droit à prestation ou de l'obligation de cotisation. / Si ces données peuvent révéler des informations relatives aux circonstances dans lesquelles la personne a dépensé ou perçu ses revenus, l'atteinte ainsi portée au droit au respect de la vie privée n'est pas disproportionnée au regard de l'objectif poursuivi. Il résulte de ce qui précède que le législateur a assorti le droit de communication contesté de garanties propres à assurer, entre le respect de la vie privée et l'objectif de valeur constitutionnelle de*

[41] Décision n° 2015-715 DC du 5 août 2015, *Loi pour la croissance, l'activité et l'égalité des chances économiques*, paragr. 134 à 138.

lutte contre la fraude en matière de protection sociale, une conciliation qui n'est pas déséquilibrée »[42].

Il a, en revanche, censuré les dispositions relatives aux données de connexion : *« compte tenu de leur nature et des traitements dont elles peuvent faire l'objet, les données de connexion fournissent sur les personnes en cause des informations nombreuses et précises, particulièrement attentatoires à leur vie privée. Par ailleurs, elles ne présentent pas de lien direct avec l'évaluation de la situation de l'intéressé au regard du droit à prestation ou de l'obligation de cotisation. Dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation équilibrée entre le droit au respect de la vie privée et la lutte contre la fraude en matière de protection sociale »*[43].

Dans sa décision n° 2020-841 QPC du 20 mai 2020, le Conseil a jugé qu'en faisant porter le droit de communication de la Hadopi sur *«* "tous documents, quel qu'en soit le support" *et en ne précisant pas les personnes auprès desquelles il est susceptible de s'exercer, le législateur n'a ni limité le champ d'exercice de ce droit de communication ni garanti que les documents en faisant l'objet présentent un lien direct avec le manquement à l'obligation énoncée à l'article L. 336-3 du code de la propriété intellectuelle, qui justifie la procédure mise en œuvre par la commission de protection des droits. / D'autre part, ce droit de communication peut également s'exercer sur toutes les données de connexion détenues par les opérateurs de communication électronique. Or, compte tenu de leur nature et des traitements dont elles peuvent faire l'objet, de telles données fournissent sur les personnes en cause des informations nombreuses et précises, particulièrement attentatoires à leur vie privée. Elles ne présentent pas non plus nécessairement de lien direct avec le manquement à l'obligation énoncée à l'article L. 336-3. / Il résulte de ce qui précède que, dans ces conditions, le législateur n'a pas entouré la procédure prévue par les dispositions contestées de garanties propres à assurer une conciliation qui ne soit pas manifestement déséquilibrée entre le droit au respect de la vie privée et l'objectif de sauvegarde de la propriété intellectuelle »*[44].

3. – Le contrôle de dispositions organisant des partages d'information entre administrations

[42] Décision n° 2019-789 QPC du 14 juin 2019 précitée, paragr. 10 à 14.
[43] *Ibid.*, paragr. 15.
[44] Décision n° 2020-841 QPC du 20 mai 2020, précitée, paragr. 16 à 18.

Enfin, le Conseil constitutionnel s'est également prononcé à plusieurs reprises sur des dispositions prévoyant une transmission d'information entre des personnes publiques.

Dans sa décision n° 2007-553 DC du 3 mars 2007, il a validé des dispositions déterminant le cadre dans lequel les professionnels de l'action sociale peuvent partager entre eux des informations confidentielles et les transmettre au maire ou au président du conseil général. À cette occasion, il a jugé : *« que c'est afin de mieux prendre en compte l'ensemble des difficultés sociales, éducatives ou matérielles d'une personne ou d'une famille et de renforcer l'efficacité de l'action sociale, à laquelle concourt une coordination accrue des différents intervenants, que le législateur a prévu, dans certaines hypothèses, de délier ces derniers du secret professionnel ; qu'il a précisé que, si l'un d'eux agit seul auprès d'une personne ou d'une famille, il ne doit donner d'informations au maire de la commune ou au président du conseil général que* "lorsque l'aggravation des difficultés sociales, éducatives ou matérielles" *de cette personne ou de cette famille* "appelle l'intervention de plusieurs professionnels" *; qu'il n'a autorisé les professionnels qui agissent auprès d'une personne ou d'une même famille, ainsi que le coordonnateur éventuellement désigné parmi eux par le maire,* "à partager entre eux des informations à caractère secret" *qu'*"afin d'évaluer leur situation, de déterminer les mesures d'action sociale nécessaires et de les mettre en œuvre" *et seulement dans la mesure* "strictement nécessaire à l'accomplissement de la mission d'action sociale" *; qu'il n'a permis à un professionnel, agissant seul ou en tant que coordonnateur, de délivrer ces informations confidentielles au maire ou au président du conseil général, qui disposent déjà, à d'autres titres, d'informations de cette nature, que si elles sont strictement nécessaires à l'exercice des compétences de ceux-ci ; qu'il a, enfin, précisé que la communication de telles informations à des tiers est passible des peines prévues à l'article 226-13 du code pénal ».* Par conséquent, le Conseil a considéré que le législateur avait ainsi assorti *« les échanges d'informations qu'il a autorisés de limitations et précautions propres à assurer la conciliation qui lui incombe entre, d'une part, le droit au respect de la vie privée et, d'autre part, les exigences de solidarité découlant des dixième et onzième alinéas du Préambule de 1946 »*[45].

Dans sa décision n° 2016-569 QPC du 23 septembre 2016, le Conseil était appelé à se prononcer sur des dispositions autorisant des échanges d'informations en vue d'améliorer le suivi et le contrôle des personnes condamnées, favoriser l'exécution des peines et prévenir la récidive. Il a considéré que le législateur avait prévu que

[45] Décision n° 2007-553 DC du 3 mars 2007, *Loi relative à la prévention de la délinquance*, cons. 6 et 7.

« puisse être transmise à l'état-major de sécurité et à la cellule de coordination opérationnelle des forces de sécurité intérieure "toute information" *que les juridictions de l'application des peines et le service pénitentiaire d'insertion et de probation* "jugent utile" *au bon déroulement du suivi et du contrôle des personnes condamnées, sans définir la nature des informations concernées, ni limiter leur champ. Ce faisant, même s'il s'agissait d'améliorer le suivi et le contrôle des personnes condamnées, de favoriser l'exécution des peines et de prévenir la récidive, le législateur a porté une atteinte disproportionnée au droit au respect de la vie privée »*[46].

B. – L'application à l'espèce

* Pour examiner les dispositions dont il était saisi, le Conseil a énoncé, tout d'abord, la formule de principe selon laquelle il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Il a rappelé qu'à ce titre, *« Il lui incombe d'assurer la conciliation entre, d'une part, les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation et, d'autre part, le droit au respect la vie privée protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 »* (paragr. 3).

* Le Conseil a examiné séparément les dispositions relatives au partage d'informations entre services de renseignement et celles prévoyant la communication d'informations à ces services.

- Après avoir rappelé l'objet des dispositions relatives au partage d'informations entre services de renseignement (paragr. 4), il a constaté, en premier lieu, qu'en application de l'article L. 811-1 du CSI, la politique publique de renseignement concourt à la stratégie de sécurité nationale ainsi qu'à la défense et à la promotion des intérêts fondamentaux de la Nation. Il a ensuite souligné que, *« En adoptant les dispositions contestées, le législateur a entendu organiser et sécuriser le partage d'informations entre les services de renseignement et améliorer leur capacité opérationnelle »* et que, ce faisant, ces dispositions permettent de mettre en œuvre les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation (paragr. 5).

[46] Décision n° 2016-569 QPC du 23 septembre 2016, *Syndicat de la magistrature et autre (Transaction pénale par officier de police judiciaire - Participation des conseils départementaux de prévention de la délinquance et des zones de sécurité prioritaires à l'exécution des peines)*, paragr. 25 et 26.

En deuxième lieu, le Conseil a examiné les garanties entourant le partage d'informations entre services de renseignement.

Il a constaté que, *« d'une part, les services mentionnés à l'article L. 811-2 du même code sont les services spécialisés de renseignement. Ils ont pour missions la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation. À cette fin, ils peuvent recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation énumérés à l'article L. 811-3. D'autre part, les services mentionnés à l'article L. 811-4 sont ceux, autres que les services spécialisés de renseignement, qui peuvent être autorisés à recourir à ces techniques pour une ou plusieurs des finalités mentionnées à l'article L. 811-3. Le partage d'informations autorisé par les dispositions contestées ne concerne ainsi que des services concourant à la défense des intérêts fondamentaux de la Nation »* (paragr. 6). Le Conseil a ainsi considéré que les services intéressés étaient précisément définis et concouraient à la défense des intérêts fondamentaux de la Nation.

En troisième lieu, le Conseil a relevé que le service détenteur d'une information ne peut la partager que si elle est nécessaire à l'accomplissement des missions du service destinataire (paragr. 7).

En quatrième et dernier lieu, il a rappelé que, d'une part, les informations ainsi partagées demeurent soumises aux règles encadrant les traitements de données à caractère personnel mis en œuvre par les services de renseignement et, en particulier, aux règles prévues par le livre VIII du CSI, présentées ci-dessus, pour les données recueillies au moyen de techniques de renseignement. D'autre part, les dispositions contestées ne font pas obstacle au contrôle susceptible d'être exercé, par les autorités compétentes, sur les informations partagées (paragr. 8).

Au regard de l'ensemble de ces éléments, le Conseil constitutionnel a jugé *« que les premier et troisième alinéas de l'article L. 863-2 du code de la sécurité intérieure ne méconnaissent pas le droit au respect de la vie privée »* et que *« ces dispositions, qui ne sont pas non plus entachées d'incompétence négative et qui ne méconnaissent aucun autre droit ou liberté que la Constitution garantit, doivent être déclarés conformes à la Constitution »* (paragr. 9).

- Après avoir ainsi validé les dispositions intéressant le partage d'informations entre services de renseignement, le Conseil constitutionnel a examiné les dispositions du deuxième alinéa de l'article L. 863-2 du CSI, qui autorisait quant à lui certaines autorités administratives à communiquer des informations aux services de renseignement (paragr. 10).

Dans le prolongement des paragraphes précédents, il a constaté que, *« En adoptant les dispositions contestées, le législateur a entendu améliorer l'information des services de renseignement »* et que ces dispositions contribuent également à la sauvegarde des intérêts fondamentaux de la Nation (paragr. 11).

Toutefois, le Conseil a considéré que la transmission d'informations par certaines administrations aux services de renseignement n'était pas entourée des mêmes garanties que le partage d'informations entre services de renseignement.

Il a d'abord rappelé que les autorités administratives autorisées à transmettre des informations à ces services étaient nombreuses et que cette transmission pouvait avoir lieu à leur seule initiative et ce, alors même que leurs missions pouvaient être sans lien avec celles des services de renseignement (paragr. 12).

Le Conseil a ensuite souligné qu'il résultait des dispositions contestées que pouvaient *« être communiquées aux services de renseignement toutes les* "informations utiles" *à l'accomplissement des missions de ces derniers sans que le législateur n'ait précisé la nature des informations concernées »* et que *« la communication d'informations ainsi autorisée peut porter sur toute catégorie de données à caractère personnel, dont notamment des informations relatives à la santé, aux opinions politiques et aux convictions religieuses ou philosophiques des personnes »* (paragr. 13).

Or, le Conseil a constaté que le législateur n'avait prévu aucune garantie encadrant ces transmissions d'informations (paragr. 14).

Par conséquent, il a jugé que le deuxième alinéa de l'article L. 863-2 du CSI méconnaissait le droit au respect de la vie privée et l'a déclaré contraire à la Constitution, sans qu'il soit donc besoin de se prononcer sur les autres griefs (paragr. 15).

* S'agissant des effets de la déclaration d'inconstitutionnalité, le Conseil a jugé, d'une part, que l'abrogation immédiate des dispositions déclarées inconstitutionnelles entraînerait des conséquences manifestement excessives. Il a donc décidé de reporter au 31 décembre 2021 la date de leur abrogation (paragr. 17).

D’autre part, se prononçant sur les effets déjà produits par ces dispositions, le Conseil a considéré que *« Les mesures prises avant la publication de la présente décision ne peuvent être contestées sur le fondement de cette inconstitutionnalité »* (même paragr.).