Nations Unies A/HRC/46/37/Add.2

Assemblée générale

Distr. générale
1er février 2021
Français
Original : anglais

Conseil des droits de l'homme
Quarante-sixième session
22 février-19 mars 2021
Point 3 de l'ordre du jour
Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement

Visite en France

Rapport du Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci*, **

Résumé

Le Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci, a effectué une visite officielle en France du 13 au 17 novembre 2017. Dans le présent rapport, il fait part de ses préoccupations au sujet des lois sur l'état d'urgence et recommande de réformer plus avant la législation française afin d'asseoir les pouvoirs de contrôle de la Commission nationale de contrôle des techniques de renseignement et d'aligner les garanties et voies de recours applicables au renseignement extérieur sur celles qui s'appliquent au renseignement intérieur.

* Le résumé du rapport est distribué dans toutes les langues officielles. Le corps du rapport, annexé au résumé, est distribué dans la langue de l'original et en français seulement.

** Le présent document est soumis après la date prévue pour que l'information la plus récente puisse y figurer.

Annexe

Rapport du Rapporteur spécial sur le droit à la vie privée, Joseph A. Cannataci, sur sa visite en France

I. Introduction

1. Le présent rapport a été établi sous sa forme définitive à la fin de 2020, après que les résultats préliminaires des réunions tenues pendant la visite en France, du 13 au 17 novembre 2017, ont été évalués, recoupés avec des études de suivi et appréciés au regard de l'évolution de la situation. Il se fonde notamment sur les critères de mesure du respect de la vie privée que le Rapporteur spécial a définis en 2019 dans un projet de document[1].

2. La plus grande partie du présent rapport reprend et développe les conclusions déjà publiées en novembre 2017 dans la déclaration de fin de mission[2].

3. Le Rapporteur spécial remercie le Gouvernement français pour l'ouverture dont il a fait preuve en facilitant sa visite. Les entretiens avec les représentants de l'État ont été cordiaux, francs et fructueux.

4. Le Rapporteur spécial remercie les représentants de la société civile, les policiers, les fonctionnaires et les autres parties prenantes qui lui ont donné accès à une documentation détaillée ainsi que tous ceux qui ont organisé des réunions d'information à son intention.

5. Le Rapporteur spécial remercie également les membres et le personnel du Conseil d'État qui lui ont permis de mieux comprendre certaines questions particulièrement importantes s'agissant du respect de la vie privée.

II. Dispositions constitutionnelles et autres dispositions juridiques garantissant la protection de la vie privée

6. En France, la protection de la vie privée est considérée comme un droit consacré par le droit constitutionnel. Pourtant, elle n'est pas mentionnée expressément dans la Constitution de 1958, ni dans celle de 1946. Au fil des années, le droit à la vie privée, comme un certain nombre d'autres droits[3], a été érigé en principe à valeur constitutionnelle, expression qui, en droit français, désigne un principe dégagé de la jurisprudence, mais susceptible de ne pas figurer explicitement dans la Constitution. Il est juste de dire qu'en France, le droit à la vie privée a suivi un processus de « constitutionnalisation », surtout à partir de 1977, année où le Conseil constitutionnel a pris une première grande décision[4] sur la question. Le 12 juillet 2018, l'Assemblée nationale a refusé que le droit à la vie privée soit inscrit dans la Constitution au motif que ce droit existait déjà et avait été reconnu par la jurisprudence du Conseil constitutionnel. L'inscription de ce droit dans la Constitution avait déjà été recommandée par une commission sénatoriale, en mai 2009[5], et avait fait l'objet d'une proposition de loi émanant de la sénatrice Anne-Marie Escoffier, au cours de la même année.

[1] Disponible à l'adresse www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf (en anglais). Ce document a été élaboré pendant la période 2017-2019 dans le but de regrouper le plus grand nombre de critères généraux à partir desquels les résultats des pays pourraient être mesurés. Il a été amélioré plusieurs fois et publié pour consultation publique en mars 2019.

[2] Voir www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=22410&LangID=F. Cette déclaration et le présent rapport doivent être lus conjointement, notamment parce qu'en raison des limites de longueur applicables aux documents et des contraintes d'édition, certaines observations qui figuraient dans le document de 2017, en particulier celles concernant les mesures transitoires comme les lois sur l'état d'urgence, ont été supprimées dans le présent rapport.

[3] Dont le droit au respect de la dignité humaine et le droit d'accès aux documents publics.

[4] Décision nº 76-75 du 12 janvier 1977.

[5] Voir www.senat.fr/rap/r08-441/r08-44148.html.

Le 10 janvier 2010, le Ministère de la justice avait rejeté cette proposition, pour les mêmes raisons que celles qui seraient avancées en 2018.

7. Si, contrairement à la Constitution allemande, la Constitution française ne contient aucune mention du droit au libre développement de la personnalité, le droit constitutionnel français recouvre tout un ensemble de droits de la personnalité[6] et la liberté de développer ces droits était déjà évoquée à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789.

8. Les résidents et citoyens français bénéficient des garanties prévues par le règlement général sur la protection des données[7] qui, bien qu'imparfait, est considéré comme offrant l'une des meilleures protections de la vie privée dans le monde. La Commission nationale de l'informatique et des libertés (CNIL)[8], organisme national indépendant chargé de la protection des données, et certaines mesures et pratiques satisfont à première vue aux exigences du règlement général.

A. Législation relative à la surveillance

9. Sur la surveillance exercée par les États, le Rapporteur spécial a soumis au Conseil des droits de l'homme, en mars 2018, un projet d'instrument juridique qui pourra servir provisoirement de référence, car il n'existe encore aucun traité multilatéral contraignant et universellement accepté visant à régir la question. De ce fait, les États Membres ont quasiment dû « se débrouiller tout seuls » pour établir des garanties et des recours en la matière. La démarche adoptée par la France est très intéressante, en ce qu'elle témoigne d'une réelle volonté de s'attaquer à l'épineux problème du contrôle de la surveillance exercée par l'État. La France reste l'un des 13 rares pays qui se sont véritablement employés à encadrer cette surveillance depuis les révélations faites par Edward Snowden en 2013.

B. Surveillance

10. Il est extrêmement important de prendre note des particularités et des dynamiques du système de renseignement français :

a) Récemment, la réforme des services de renseignement a fait l'objet de nombreux débats, dans la sphère politique et dans les médias. Malheureusement, l'Europe fait face à des problèmes de sécurité et a été régulièrement frappée par des attentats depuis 2001. La France a été visée par plusieurs attaques terroristes, respectivement commises en mars 2012, en janvier 2015, en novembre 2015, en juillet 2016 et encore aujourd'hui, en 2020, avec les agissements de « loups solitaires ». La récurrence de ces attaques a accru la sensation de menace ;

b) En 2008, les services de renseignement français ont abandonné un système dualiste, qui séparait renseignement intérieur et renseignement extérieur, pour un modèle d'organisation communautaire. Conformément à un livre blanc publié en 2008 et en application du décret n° 2014-474 du 12 mai 2014, la communauté française du renseignement est divisée en six services (Direction générale de la sécurité extérieure (DGSE), Direction générale de la sécurité intérieure (DGSI)[9], Direction du renseignement militaire (DRM), Direction du renseignement et de la sécurité de la défense (DPSD), Service « Traitement du renseignement et action contre les circuits financiers clandestins »

[6] Voir, par exemple, Emmanuel Pierrat, « Protection des droits de la personnalité », *LEGICOM*, vol. 12, n° 2 (1996), p. 87 à 93 : « Dans son acception française, les droits de la personnalité recouvrent donc en vrac le secret de la correspondance et des conversations téléphoniques, le droit de s'opposer au traitement de données nominatives, les secrets de l'instruction et professionnels, le respect de la vie privée, le droit à l'image, le droit à la voix et le droit au nom. ».

[7] Règlement n° 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

[8] Voir www.cnil.fr/.

[9] Anciennement Direction centrale du renseignement intérieur (DCRI).

(TRACFIN) et Direction nationale du renseignement et des enquêtes douanières (DNRED)) auxquels s'ajoutent le Coordonnateur national du renseignement et l'Académie du renseignement. La communauté s'est enrichie d'une inspection des services de renseignement, en application du décret nº 2017-1095 du 14 juin 2017. Les six services institués par le décret nº 2014-474 sont des services spécialisés de renseignement. Ils se distinguent en ce qu'ils sont habilités, dans une certaine mesure, à demander à exercer des activités de renseignement non ciblées[10], alors que les services non spécialisés que sont, par exemple, la Direction du renseignement de la préfecture de police de Paris, le Service national du renseignement pénitentiaire et le Service central du renseignement territorial, peuvent seulement mener des activités de renseignement ciblées, dans le cadre de missions spéciales ;

c) Créée par la loi nº 2007-1443 du 9 octobre 2007, la délégation parlementaire au renseignement n'a réellement exercé ses fonctions qu'après l'entrée en vigueur de la loi de programmation militaire 2014-2019. Dans un rapport de 2018, le Secrétariat général de la défense et de la sécurité nationale a annoncé des réformes visant à faciliter l'échange d'informations et à simplifier la procédure de déclassification des documents ;

d) Le contrôle ne s'exerce pas directement sur les services de renseignement, qui sont placés sous l'autorité des ministres compétents, par l'intermédiaire de leurs directeurs. En fait, les députés sont associés au contrôle du caractère proportionnel des techniques de renseignement, non pas dans le cadre de la délégation parlementaire au renseignement, mais dans celui de la Commission nationale de contrôle des techniques de renseignement (CNCTR), qui est une autorité administrative indépendante ;

e) La création d'un conseil national du renseignement, dirigé par un coordonnateur[11] et chargé de mener des inspections conjointes et transversales, a fait l'objet de débats. L'Inspection des services de renseignement a ensuite été mentionnée dans la loi de programmation militaire, et finalement créée par le décret nº 2014-833 du 24 juillet 2014. Elle rend compte au Premier Ministre et procède à des missions d'inspection dans les services spécialisés de renseignement ;

f) La loi nº 2015-912 du 24 juillet 2015 et la loi nº 2015-1556 du 30 novembre 2015 représentent une avancée notable dans le contrôle des services de renseignement. Elles ont abouti à la mise en place d'un contrôle administratif de l'utilisation des techniques de renseignement et des fichiers intéressant la sûreté de l'État. L'attribution du pouvoir de contrôle administratif à deux autorités indépendantes, à savoir la CNCTR et la CNIL, est un grand progrès, mais ne constitue pas une rupture conceptuelle pour autant, compte tenu des pouvoirs qui étaient traditionnellement dévolus à la CNIL et à l'organisme auquel la CNCTR a succédé. La possibilité qui est maintenant donnée, après avis administratif, qu'un recours soit formé par l'autorité administrative indépendante compétente ou par les citoyens marque un tournant. C'est la première fois qu'un juge se voit accorder l'accès à des documents classifiés sans que leur contenu détaillé ne soit communiqué au requérant. Les lois précitées constituent donc à la fois un grand pas en avant, par la portée sans précédent du contrôle administratif qu'elles permettent, et une évolution sensible, par la création d'un mécanisme de recours ;

g) Pendant l'état d'urgence d'une durée de vingt-trois mois qui s'est achevé en octobre 2017, les juridictions judiciaires (et le Conseil d'État) ont eu pour pratique d'accepter les « notes blanches », qui sont fréquemment utilisées par le Ministère de l'intérieur pour justifier l'action de la police (assignation à résidence, interdiction de manifester) à l'égard de personnes soupçonnées de menacer l'appareil de l'État. Ces notes, qui émanent des services de renseignement, sont dites « blanches » parce qu'elles ne présentent ni titre, ni date, ni cote, ni signature. Leur caractère anonyme vise à protéger le secret des sources, mais il exonère aussi quiconque de toute responsabilité quant à leur contenu. Les faits ont montré que ces notes présentaient parfois des erreurs et faisaient par exemple référence à des condamnations qui n'avaient pas été prononcées ou à des actes qui n'avaient pas été commis. Tant que les notes blanches sont considérées comme des « éléments de preuve », il est très difficile, dans la pratique, de faire une distinction de valeur entre ces documents anonymes et sans aucune

[10] Voir Code de la sécurité intérieure, art. L851-2 et L851-3.

[11] Voir décret nº 2009-1657 du 24 décembre 2009.

garantie et les dossiers établis sous le strict contrôle de la loi. Les notes blanches n'étant pas mentionnées dans la loi sur le terrorisme adoptée en novembre 2017, il sera intéressant de voir comment elles seront accueillies par les juridictions judiciaires et si elles se verront accorder une valeur probante ou autre.

C. Surveillance à des fins d'application de la loi

11. En France, les prérogatives de surveillance varient en fonction de la finalité. Les services spécialisés de renseignement ont pour principal objectif et but ultime de garantir la sécurité nationale, alors que la police et, parfois, la gendarmerie (force paramilitaire) s'attachent à assurer l'ordre public.

12. Sur le territoire français, l'interception de communications est autorisée selon deux modalités distinctes :

a) Les interceptions judiciaires, ordonnées par un juge d'instruction dans le cadre d'une enquête pénale et réalisées par la police, la gendarmerie et la DGSI ;

b) Les interceptions administratives, ou interceptions de sécurité, qui peuvent être demandées à la fois par les services de la sécurité intérieure et les services de renseignement extérieur.

13. Selon la loi française, le juge d'instruction ordonne l'interception, l'enregistrement et la transcription de communications privées dans le cadre d'enquêtes pénales. Sous réserve d'autorisation, les forces de l'ordre demandent à toute personne qualifiée d'exécuter les opérations techniques permettant l'accès aux communications en question.

14. En janvier 2016, l'Assemblée nationale a créé une commission parlementaire chargée d'enquêter sur les attentats commis en janvier 2015 à Paris, dans les bureaux du journal satirique *Charlie Hebdo*, et ailleurs en région parisienne, et sur la série d'attaques coordonnées revendiquées par l'État islamique d'Iraq et du Levant, commises en novembre 2015 à Paris et dans sa périphérie, qui avaient conjointement tué 147 personnes. La commission parlementaire n'a pas ouvertement critiqué les mesures prises par l'exécutif en réaction à ces attentats, mais a soulevé des questions quant à l'efficacité de l'état d'urgence, déclaré en novembre 2015, et du déploiement de 10 000 soldats sur l'ensemble du territoire national en vue de protéger les villes et d'autres zones sensibles. Dans son rapport, la commission parlementaire a constaté que la police nationale, chargée de la protection des grandes villes, et la gendarmerie, chargée de la protection des villes de plus petite taille et des zones rurales, avaient chacune leur propre division du renseignement et a estimé que ces divisions devraient fusionner.

15. La loi n° 2017-1510 du 30 octobre 2017, qui a été adoptée à une large majorité et qui a mis fin à l'état d'urgence, a renforcé les pouvoirs de l'exécutif. Par exemple, elle a donné aux préfets le pouvoir de fermer des lieux de culte dans lesquels sont diffusées des idées incitant au terrorisme et de procéder à des contrôles d'identité aux frontières et dans les gares, les ports et les aéroports sans l'autorisation préalable d'un juge, ou d'ordonner des perquisitions dans des habitations. Les préfets prennent encore leurs décisions de perquisition et d'assignation à résidence sur la base d'éléments juridiquement bien peu solides, tels que des notes informelles, anonymes et souvent vagues des services secrets. Toute personne visée par une perquisition dispose d'un droit de recours. Les défenseurs des droits civils considèrent que la loi n° 2017-1510 jette la suspicion sur tous les citoyens. Ces dispositions sécuritaires remettent en question un principe important du droit français, en ce que les policiers n'ont plus besoin d'un motif pour procéder à une perquisition. Les représentants de la société civile ont aussi souligné que l'idée selon laquelle tout le monde est suspect et, lorsque l'on n'a rien à se reprocher, l'on ne craint pas les fouilles policières ne s'inscrit pas dans le respect des droits de l'homme − mais y contrevient.

16. La disposition relative aux communications par voie hertzienne, qui avait été censurée en octobre 2016 par le Conseil constitutionnel, a été réintroduite. Cependant, la loi précise maintenant le cadre juridique d'application de cette disposition, qui échappait jusqu'alors à tout contrôle. En outre, elle prolonge jusqu'en 2020 l'utilisation du dispositif décrié des

« boîtes noires » qui, au moyen d'algorithmes, permet aux services de renseignement de détecter des données de connexion Internet suspectes.

17. La loi nº 2017-1510 a enrichi le droit commun d'autres mesures de sécurité telles que la création des dossiers passagers, qui permettent aux autorités de connaître l'identité de tous les passagers des vols commerciaux opérés en Europe et d'ouvrir des enquêtes sur les personnes susceptibles de s'être radicalisées.

D. Surveillance à des fins de sécurité nationale (surveillance intérieure et surveillance extérieure)

18. Les interceptions administratives doivent être approuvées par le Premier Ministre. Sur demande écrite de l'un des ministres compétents et sous réserve de l'autorisation du Premier Ministre ou de la personne spécialement déléguée par lui, les services de sécurité et de renseignement peuvent intercepter et prendre connaissance de communications privées à des fins précises et prédéfinies et, s'il y a lieu, se doter des moyens de déchiffrer ces communications auprès de fournisseurs de services de cryptologie.

19. Les principaux services de sécurité et de renseignement sont :

a) La DGSI, rattachée au Ministère de l'intérieur et chargée de la sécurité nationale. Elle emploie quelque 3 500 personnes et dispose d'un budget annuel de 300 millions d'euros. Elle est née en 2008 de la fusion de la Direction centrale des renseignements généraux et de la Direction de la surveillance du territoire, qui relevait de la police nationale ;

b) La DGSE, placée sous l'autorité du Ministre de la défense et chargée de recueillir des renseignements d'intérêt civil ainsi que de mener des opérations paramilitaires et des activités de contre-espionnage à l'étranger. Elle recueille des renseignements à la fois d'origine humaine et d'origine électromagnétique. En tant que service de renseignement extérieur, elle n'est pas censée opérer sur le territoire français, mais est autorisée à demander des données et à intercepter des communications intérieures. Experte en techniques de déchiffrement et de collecte de données de communication, elle fait profiter de ses moyens et compétences d'autres organismes, comme la DGSI et la DRM ;

c) La DRM, placée sous l'autorité directe du Chef d'état-major des armées et du Président de la République française en tant que chef des armées. La DRM est une direction du Ministère de la défense. Elle est chargée de recueillir des renseignements d'intérêt militaire pour appuyer les forces armées françaises ;

d) La DRSD, relevant du Ministère de la défense et chargée de la sécurité du personnel, des informations, du matériel et des installations des forces armées et du secteur de la défense ;

e) La DNRED, relevant du Ministère de l'économie et chargée des activités de renseignement extérieur sur les questions frontalières ;

f) TRACFIN, service du Ministère de l'économie chargé de recueillir, principalement à l'étranger, des informations concernant notamment le blanchiment d'argent et le financement du terrorisme.

20. Le décret nº 2015-1639 du 11 décembre 2015 a habilité plus de 20 services de police et de gendarmerie, dont certains ne sont pas officiellement des services de renseignement, à intercepter des communications et à demander l'accès à des données, principalement au titre de la lutte contre le terrorisme. Pour le Gouvernement français, ce bouleversement des usages se justifie au regard de la menace terroriste persistante.

21. À l'instar de ce qui se passe dans la plupart des pays, le droit français protège mieux la vie privée des citoyens français et des personnes communiquant depuis le territoire français que celle des personnes communiquant depuis l'étranger, qui ont peu de garanties juridiques contre la collecte d'informations. Les opérations de recueil de renseignements autorisées par le Premier Ministre peuvent s'étendre à toutes les communications effectuées par des moyens

électroniques, y compris les communications par téléphonie fixe et mobile, et à toutes les métadonnées obtenues auprès des fournisseurs de services Internet et d'autres services en ligne.

22. Les opérateurs téléphoniques et les fournisseurs de services Internet et d'autres services en ligne peuvent être contraints de transmettre un large éventail de métadonnées concernant une personne ciblée, notamment les données techniques permettant l'identification des numéros de connexion ou des numéros d'abonnement (numéros de téléphone, adresses IP, etc.) de cette personne, la liste de tous les numéros de connexion ou numéros d'abonnement en lien avec elle, les données de géolocalisation de tous les appareils en sa possession et les métadonnées téléphoniques. Sous l'autorité du Premier Ministre, les opérateurs téléphoniques peuvent être tenus de coopérer avec les services de renseignement ayant été autorisés à procéder à des écoutes téléphoniques ciblées. Ces écoutes ne sont pas effectuées par les services de renseignement eux-mêmes, qui doivent agir par l'intermédiaire d'un organisme technique spécialisé, le Groupe interministériel de contrôle.

23. Le Parlement a autorisé les services de renseignement à utiliser des dispositifs tels que les intercepteurs d'identités internationales d'abonnement mobile (intercepteurs d'IMSI) pour tracer les téléphones mobiles ou les ordinateurs en lien avec une personne ciblée. Les intercepteurs d'IMSI doivent uniquement servir à la collecte de métadonnées, et toutes les données sans relation avec la personne ciblée qui ont été recueillies doivent être détruites. La loi relative au renseignement présentée au Conseil des ministres le 19 mars 2015 pousse plus loin la logique de l'affaiblissement du contrôle juridictionnel, en autorisant officiellement les services de renseignement à user d'un certain nombre de pratiques et de technologies auparavant illégales, comme l'utilisation des intercepteurs d'IMSI, la géolocalisation des voitures, la sonorisation de lieux et de véhicules privés, l'accès aux réseaux de fournisseurs de services Internet privés et la mise en place de « boîtes noires »[12] sur ces réseaux à des fins d'identification de terroristes présumés par le recours à des algorithmes. Aucune de ces pratiques ne nécessite l'autorisation d'un juge. Un contrôle peut être exercé a posteriori[13], mais compte tenu de l'ampleur de l'intrusion, cela peut sembler bien insuffisant pour garantir le respect des droits de l'homme, la protection de la vie privée et la démocratie. Les « boîtes noires » sont les dispositifs à la portée la plus étendue que les services de renseignement ont utilisés pour surveiller les communications des citoyens français. En octobre 2017, la CNCTR a émis un avis favorable pour l'utilisation du premier de ces algorithmes au titre de la prévention du terrorisme. Selon la procédure applicable, l'utilisation de l'algorithme doit d'abord être autorisée par le Premier Ministre, qui aura préalablement reçu de la CNCTR un avis favorable à ce sujet et l'assurance que l'algorithme serait uniquement appliqué à des données anonymisées (c'est-à-dire des données de connexion, et non des données de contenu). Par la suite, lorsque l'algorithme met en évidence des données méritant une attention particulière, le service de renseignement à l'origine de son activation peut demander que ces données ne soient plus anonymes. Cette « désanonymisation » des données est elle aussi subordonnée à un avis favorable de la CNCTR et à l'autorisation du Premier Ministre. Enfin, une fois que les données ne sont plus anonymes, le service de renseignement peut demander que la personne ciblée soit soumise à d'autres techniques de surveillance, plus traditionnelles.

24. Le droit français impose déjà aux opérateurs de télécommunications et aux fournisseurs de services Internet de conserver les métadonnées de leurs clients pendant au moins une année. Un décret impose même à des entreprises d'hébergement de sites Web comme Facebook, Google et Amazon de conserver les données de leurs utilisateurs pendant au moins un an et de les communiquer aux autorités sur demande. Cependant, ces métadonnées peuvent servir uniquement dans le cadre d'enquêtes ciblées, car les services de renseignement sont tenus de se conformer à une procédure qui leur impose d'adresser aux fournisseurs de services Internet et aux entreprises d'hébergement de sites Web des demandes précises, qui font mention du nom complet de la personne ciblée, de son nom d'utilisateur, de son adresse IP ou d'autres données d'identification, et d'obtenir l'autorisation du Premier Ministre. Il semble que la mise en place de « boîtes noires » sur les réseaux des fournisseurs

[12] Voir loi nº 2015-912 du 24 juillet 2015 (art. 5) et Code de la sécurité intérieure, art. L851-3.

[13] Si le Premier Ministre ne suit pas la recommandation de la CNCTR, celle-ci peut saisir le Conseil d'État d'un recours.

de services Internet serve également à faciliter la collecte massive de plus petits ensembles de données. Les « boîtes noires » filtrent le trafic à l'aide d'algorithmes de détection des menaces et n'extraient donc que les métadonnées qui satisfont à certains critères de sélection, établis à partir des données de criminalistique numérique issues d'enquêtes antiterroristes − par exemple, des modèles et habitudes de communication. Les métadonnées extraites servent ensuite à l'identification des utilisateurs correspondants.

25. En ce qui concerne les communications intérieures, les enregistrements de communications vocales doivent être détruits dans un délai de trente jours à compter de l'interception, mais leurs transcriptions peuvent être conservées « aussi longtemps que nécessaire » par les services de renseignement. Les métadonnées transmises sur demande par les fournisseurs de services Internet et d'autres services de télécommunication peuvent être conservées pendant quatre ans maximum. Ce délai s'étend à six ans pour les communications interceptées qui sont cryptées.

26. Le Ministère de l'intérieur a souligné qu'en application de la législation actuelle, les services de renseignement pouvaient uniquement procéder à des activités de surveillance ciblées, sauf dans le cas de l'utilisation d'algorithmes, pour laquelle la pseudonymisation était obligatoire.

27. Deux lois sur le terrorisme et la sécurité ont été adoptées : la loi de programmation militaire 2014-2019, en décembre 2013, et la loi antiterroriste, en novembre 2014. La première offre un cadre pour l'utilisation de la géolocalisation en temps réel par les services de renseignement. La seconde autorise le blocage administratif de sites Web considérés comme faisant l'apologie d'actes de violence terroriste.

28. La surveillance des communications internationales, que ce soit par la DGSI, la DGSE ou l'une des autorités militaires, est soumise à moins de restrictions. Après avoir reçu l'avis de la CNCTR, le Premier Ministre délivre des autorisations de portée générale, qui permettent aux services de renseignement de surveiller des communications et de collecter des données associées à une région géographique, un pays, des organisations ou des groupes de personnes. Il précise quels types de réseaux de communication peuvent être visés. Ces autorisations ont une durée de validité de quatre mois, renouvelable sans limitation.

29. Les données des communications internationales interceptées peuvent être conservées pour une durée maximale d'un an à compter de leur traitement et de quatre ans à compter de leur interception. Les métadonnées collectées peuvent être conservées pendant six ans. Les données chiffrées peuvent être conservées pour une durée maximale de six ans à compter de leur déchiffrement et de huit ans à compter de leur interception.

30. La loi relative à la surveillance des communications internationales s'applique uniquement aux communications entre utilisateurs se trouvant à l'étranger ; celles-ci sont interceptées depuis la France, y compris les territoires d'outre-mer, comme cela est précisé dans les dernières lois en date sur le renseignement. Autrement dit, la loi s'applique aux données collectées non seulement à partir des principaux réseaux de câbles à fibres optiques et stations d'interception des communications par satellite situés en métropole, mais aussi à partir des stations d'interception des communications par satellite situés en Guyane française, en Nouvelle-Calédonie et à Mayotte, si bien que, pour ce qui est de la couverture des communications satellitaires dans le monde, la communauté française du renseignement n'est probablement devancée que par le partenariat « Five Eyes », conclu entre l'Australie, le Canada, les États-Unis, la Nouvelle-Zélande et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, qui a abouti au programme de surveillance *Echelon*. En référence à celui-ci, le réseau français de renseignement d'origine électromagnétique a été surnommé « Frenchelon ». Si les communications internationales se révèlent finalement être des communications intérieures (le numéro d'appel ou le numéro d'abonnement renvoient à un numéro français), les données qui en ont été extraites ne peuvent être exploitées que dans le cadre des dispositions applicables aux communications intérieures ou doivent être détruites dans un délai de six mois.

31. Depuis 2008, la DGSE est en mesure d'intercepter les communications Internet par câbles sous-marins. La surveillance ciblée a laissé place à la surveillance de masse.

32. Le Ministère de l'intérieur a indiqué qu'en application de l'article L801-1 du Code de la sécurité intérieure, un service de renseignement peut uniquement faire usage d'une technique donnée pour une finalité donnée.

33. Le Ministère de l'intérieur a confirmé une déclaration de la CNCTR, selon laquelle les services de renseignement français n'exercent pas une surveillance de masse.

E. Contrôle des organismes de surveillance

34. Des lois telles que la loi nº 2015-912 et la loi nº 2015-1556 accordent au Premier Ministre les pleins pouvoirs pour ordonner et autoriser des activités de renseignement, à la fois à l'intérieur et à l'extérieur du pays. Le directeur du service de renseignement intéressé adresse la demande de collecte de données à son ministère de tutelle, qui la soumet ensuite au Premier Ministre pour autorisation. Ce contrôle *ex ante* est régi par les principes de proportionnalité, de légalité et de subsidiarité (il s'agit de déterminer si d'autres techniques, moins intrusives, sont disponibles).

35. La loi de novembre 2017, qui prévoit que les autorités administratives maintiennent l'Assemblée nationale et le Sénat informés en leur transmettant une copie de toutes les mesures qu'elles prennent, ne sera applicable que jusqu'au 31 décembre 2020.

36. La CNCTR est tenue informée de toutes les demandes et supervise la mise en œuvre des techniques de renseignement.

37. La CNCTR a un rôle consultatif uniquement et doit se soumettre à la décision du Premier Ministre concernant les demandes de recueil de renseignements. Si elle rend un avis défavorable, le Premier Ministre est libre de ne pas en tenir compte et d'autoriser le recueil de renseignements demandé. En pareil cas, la CNCTR peut saisir le Conseil d'État.

38. La CNCTR a accès à toutes les transcriptions et à tous les journaux des données recueillies avec l'autorisation du Premier Ministre, mais ne peut pas exiger d'un service de renseignement qu'il produise d'autres documents ou informations, ni enquêter sur une quelconque irrégularité de sa propre initiative. Tous ces contrôles a posteriori visent à vérifier si une autorisation préalable a été obtenue et à évaluer la manière dont les techniques ont été mises en œuvre. Cependant, la CNCTR peut formuler des recommandations au sujet des procédures de renseignement et, si elle constate une irrégularité, notifier le fait au Premier Ministre et saisir le Conseil d'État. Tous les débats tenus dans le cadre de la CNCTR, de même que tous les échanges de la CNCTR avec le Premier Ministre et les services de renseignement, sont couverts par le secret défense.

39. La CNCTR est tenue de notifier au Conseil d'État la commission de certains faits, comme les entrées par effraction. En dehors des cas particuliers ainsi définis, la notification n'est pas obligatoire et reste à la discrétion de la Commission. La notification n'a pas un effet suspensif, le Conseil d'État pouvant rendre une décision rapidement (en moins d'une journée).

40. Un statut spécial est accordé aux journalistes, aux avocats et aux parlementaires. Lorsqu'une demande de renseignements concerne l'un d'eux, la CNCTR doit en être informée avant toute collecte de données afin de déterminer si cette collecte est nécessaire et proportionnée. Dans l'affirmative, les transcriptions des communications qui auront été interceptées lui seront ensuite transmises. Lorsque les écoutes visent de simples citoyens, la CNCTR peut accéder aux transcriptions si elle en fait la demande ; lorsque les écoutes visent des membres de professions dont les communications relèvent du secret professionnel, les transcriptions lui sont obligatoirement transmises pour examen.

41. En théorie, toute personne vivant en France ou à l'étranger peut demander à la CNCTR de vérifier si la surveillance dont elle fait éventuellement l'objet respecte la procédure applicable. La CNCTR peut s'assurer qu'aucune irrégularité n'a été commise, mais ne peut ni confirmer ni infirmer le placement sous surveillance. Elle peut uniquement déclarer avoir procédé à une vérification en bonne et due forme et notifier toute irrégularité qu'elle aura constatée au Conseil d'État.

42. La principale question soulevée concerne le pouvoir de contrôle *ex ante* attribué à la CNCTR.

43. La CNCTR a aussi vu ses pouvoirs enrichis par la loi nº 2017-1510, qui l'habilite à contrôler les transcriptions de communications sans fil, et par la décision du Conseil constitutionnel du 21 octobre 2016.

44. Le rapport 2017 de la CNCTR fournit quelques données chiffrées intéressantes, notamment le nombre de demandes d'autorisation pour l'utilisation de certaines techniques de surveillance. En 2017, la CNCTR a rendu 70 432 avis, soit 5 % de plus qu'en 2016, dont 30 116 en réponse à des demandes d'identification d'abonnés ou de numéros téléphoniques − cette identification étant, selon le Président de la Commission, la plus utilisée des techniques peu intrusives. Un grand nombre d'avis (8 758 précisément, soit 5 % de plus qu'en 2016) concernait des demandes d'interceptions de sécurité. En 2017, il y a eu 18 512 demandes de factures téléphoniques détaillées.

45. L'augmentation la plus importante par rapport à 2016 (+55 %) a concerné les demandes de géolocalisation en temps réel.

46. L'évolution du pourcentage d'avis défavorables rendus par la CNCTR (3,6 % en 2017, contre 6,9 % en 2016) montre que les services de renseignement comprennent mieux ce que la loi les autorise à faire et comment formuler une demande d'autorisation. Le Premier Ministre n'a recouru à la procédure d'urgence ni en 2016, ni en 2017 ; il n'a appliqué cette procédure qu'à la fin 2015, face à la menace d'une attaque terroriste imminente. En outre, à la date de publication du rapport de 2017, plus de 21 000 personnes avaient été placées sous surveillance au moins une fois, sans qu'une enquête judiciaire ait été ouverte, dont 9 157 (42,8 %) au titre de la prévention du terrorisme (+5 % par rapport à 2016). Les autres demandes d'autorisation de techniques de surveillance avaient pour finalité la prévention de la criminalité, y compris la criminalité organisée (18 %), la protection d'intérêts majeurs de la politique étrangère (17 %), la protection des intérêts de la France (8 %) et la prévention des atteintes à l'ordre public (6 %).

47. En 2017, la CNCTR a effectué 130 contrôles a posteriori (contre 60 en 2016). Aucun problème majeur n'ayant été détecté, il semble que les services de renseignement n'aient pas tenté de se soustraire à la loi.

48. La CNIL est l'organisme de réglementation des données à caractère personnel. Elle aide les professionnels à se conformer à la loi et les particuliers à contrôler leurs données personnelles et à exercer leurs droits.

49. Cependant, la CNIL n'a pas accès aux fichiers de renseignement et ne peut pas exercer sur eux un contrôle public ; elle peut uniquement avoir connaissance de leur existence.

50. La CNIL souligne que la loi antiterroriste de 2017 (loi nº 2017-1510) peut être considérée comme représentant un changement de paradigme en matière de surveillance. Précédemment, les autorités identifiaient les personnes considérées comme dangereuses puis les plaçaient sous surveillance. Aujourd'hui, elles surveillent tous les citoyens dans le but de déterminer lesquels représentent une menace. Au vu des décisions récentes de la Cour de justice européenne, il est difficile de savoir quel est le statut de la surveillance par « boîtes noires », même si on peut arguer que celle-ci est une forme de surveillance ciblée, car elle fait intervenir des critères de sélection, et que la pseudonymisation constitue une garantie suffisante.

51. La CNIL a aussi soulevé la question de la formation des juges et de l'opportunité de doter les juges de connaissances techniques.

52. Une formation de jugement spécialisée, chargée de régler les différends relatifs à l'utilisation des techniques de surveillance à des fins de protection de la sûreté de l'État et les différends portant sur l'accès indirect à un document, a été créée en novembre 2015 au sein du Conseil d'État. Sa saisine n'intervient qu'après que le citoyen requérant a présenté une demande de vérification à la CNIL et que la CNCTR a été informée du différend. Les cinq conseillers d'État et deux rapporteurs publics qui composent la formation spécialisée sont habilités au secret de la défense nationale. Ils sont autorisés à demander et à obtenir l'accès à tous les éléments dont ils auraient besoin. Dans cette procédure contradictoire asymétrique,

les juges ont tous les pouvoirs et l'administration est tenue de répondre à toutes les questions qui lui sont posées, alors que les requérants ne peuvent rien savoir des réponses données. Un certain équilibre et une certaine confiance entre les pouvoirs de l'État sont donc assurés.

53. Lorsque le Premier Ministre ne tient pas compte d'un avis défavorable qu'elle a rendu, la CNCTR peut saisir une commission spéciale du Conseil d'État pour demander que le différend soit réglé par voie d'arbitrage. Pendant deux ans, jusqu'en novembre 2017, le Premier Ministre n'est jamais passé outre un avis défavorable de la CNCTR.

54. Ayant hérité de plus de 100 affaires renvoyées par les juridictions parisiennes, la formation spécialisée a eu des difficultés à débuter ses travaux. Actuellement, seulement une dizaine des affaires qu'elle traite chaque année portent sur des questions de surveillance. Le plus souvent, les requêtes concernent des fichiers ou, plus précisément, l'effacement de données obtenues de façon irrégulière. Dans les affaires relatives à la surveillance de personnes étrangères, c'est le caractère approfondi des vérifications effectuées qui est mis en cause.

55. En ce qui concerne la composition des différents organes de contrôle, les membres de la CNCTR possèdent des connaissances techniques dans le domaine des technologies de l'information et de la communication. Le Président de la formation spécialisée a indiqué que les membres de ladite formation, qui avaient des compétences juridiques, n'étaient pas des spécialistes des technologies de l'information et de la communication et qu'il serait donc utile qu'ils bénéficient d'une formation technique ou aient un manuel qui puisse les guider.

56. Le Conseil d'État a également un rôle consultatif et son avis est obligatoire pour ce qui est de la légalité et de la conformité juridique des projets de loi. Bien que ce contrôle *ex ante* soit de nature spécialisée, les membres du Conseil qui ont le statut de juges et qui examinent les projets de loi n'ont pas de connaissances techniques. Ils ont dit qu'ils estimaient inappropriée la présence d'experts indépendants dans leurs rangs et préféraient que ces experts aident le Gouvernement dans sa prise de décisions, de manière à garantir le principe de responsabilité. Si les mesures de contrôle et la prise de décisions étaient confiées à un organe extérieur, le rôle du Conseil d'État risquerait d'être compromis.

57. Les conseillers d'État se sont dits préoccupés de constater qu'une loi avait été élaborée pour protéger contre les interceptions simples mais que personne ne semblait s'être intéressé aux métadonnées et au profil plus détaillé qu'elles offraient d'un individu. Cet aspect doit aussi être examiné.

F. Données de santé

58. La loi n° 78-17 du 6 janvier 1978, qui a été modifiée à plusieurs reprises et en grande partie supplantée par le règlement général sur la protection des données, joue un rôle essentiel dans la protection des données de santé personnelles, c'est-à-dire des données qui permettent l'identification des individus ; elle met l'accent sur le principe de la légalité, de la limitation des finalités du traitement des données et de la conservation de celles-ci pour une durée limitée, et sur le fait qu'il importe de veiller à ce que les données soit exactes et actualisées.

59. La loi n° 2016-41 du 26 janvier 2016 a apporté d'importants changements au texte de 1978. Elle est articulée autour de trois objectifs, qui sont le renforcement de la médecine préventive, la réorganisation de l'accès aux soins au niveau territorial autour des médecins généralistes et l'amélioration du respect des droits des patients. Elle a aussi mis en évidence l'existence de données pseudonymisées. Un autre élément important de ce nouveau texte est qu'il insiste sur l'obligation pour tout organe souhaitant avoir accès à des données de démontrer que l'obtention de ces données est d'intérêt public. C'est là une pratique intéressante, peu appliquée ailleurs en Europe, et une garantie nécessaire pour protéger la vie privée des patients. Il existe des exceptions à la règle de l'intérêt public, telles que le marketing, le service ou le contrôle des prestations de santé et l'assurance. La principale garantie est fournie par la CNIL, dont l'autorisation est obligatoire. La loi impose aussi le respect du principe de la transparence, ce qui signifie, concrètement, que lorsque des données de santé sont utilisées à des fins de recherche médicale, les résultats de la recherche doivent impérativement être rendus publics.

60. Les données de santé sont considérées comme des données sensibles et doivent être traitées comme telles. À cet égard, la CNIL a un rôle à jouer en cas d'exception à la règle, telle que l'obtention de données justifiée par l'intérêt public. En outre, lorsqu'elle analyse l'une ou l'autre des exceptions, elle doit prendre en considération la question du consentement, le principe de l'accès à l'information et les droits des patients.

61. L'Institut national des données de santé fournit des avis à la CNIL sur les demandes d'accès.

62. En ce qui concerne l'autorisation de traiter des données de santé, les hébergeurs de données doivent disposer d'un agrément dans le domaine de la gestion de la sécurité et de l'analyse des risques. Il leur est interdit de partager des données de santé à des fins commerciales, même avec le consentement des intéressés.

63. La France applique le principe d'ouverture des données (« open data »), mais la préservation des données est aussi une préoccupation majeure. En d'autres termes, les données ne peuvent être réutilisées pour une autre finalité (sauf statistique). En France, les données ouvertes doivent être strictement anonymes.

64. Le problème de certaines nouvelles technologies comme les traceurs d'activité portables (ou *wearables*) est que le consentement s'y donne d'un simple clic, ce qui n'est pas une garantie suffisante, la plupart des gens ne sachant pas ce que leur consentement implique ou ce à quoi ils consentent réellement. Par conséquent, face à la constante augmentation du nombre d'outils connectés et à la transformation numérique, notamment dans le domaine médical, qui font apparaître une nouvelle forme de vulnérabilité et de nouveau risques d'attaques, il est urgent de trouver une autre solution.

65. La CNIL a indiqué que les données ouvertes rendues anonymes ne relevaient pas de son champ de compétence. De nombreux acteurs privés souhaitent accéder à ce type de données. Celles-ci doivent être recueillies de manière transparente, et c'est à ce niveau que la CNIL intervient, en informant les individus qu'ils ont le droit de s'opposer à ce que leurs données soient rendues publiques et en exigeant que les données rendues publiques soient parfaitement anonymisées, et pas seulement pseudonymisées.

66. Une autre obligation est celle de préserver la confidentialité des données de santé ; elle est notamment énoncée dans le programme Hôpital numérique (2012-2017). À la fin de 2017, environ 2 000 des 3 000 établissements de santé respectaient l'obligation de confidentialité. L'objectif est à présent d'accroître le niveau d'exigence et le nombre d'établissements qui s'y conforment, notamment en satisfaisant aux prescriptions énoncées dans le programme HOP'EN (2019-2023), plan d'action stratégique pour les systèmes d'information hospitaliers qui est le prolongement du programme Hôpital numérique, qui avait lui aussi pour objectif de développer les capacités des hôpitaux dans le domaine des technologies de l'information.

67. La CNIL entretient un dialogue fructueux avec les hôpitaux et travaille en concertation avec eux, mais elle a souligné que le budget était souvent insuffisant dans des conditions spéciales.

III. Conclusions et recommandations

A. Contrôle du renseignement, sécurité et surveillance

68. **Depuis 300 ans, la question des contrôles et contrepoids qui doivent exister entre les trois branches du pouvoir − l'exécutif, le législatif et le judiciaire − est au centre des discussions sur les différentes formes de gouvernement. Dans toute société, le débat sur la surveillance doit donc tenir compte des contre-pouvoirs qui peuvent être intégrés et de ceux qui n'ont pas été prévus dans le système. On recense dans le monde différentes formes d'autorisation de la surveillance** :

a) Exclusivement interne au service (on entend par « service » à la fois les services de sécurité tels que les services de renseignement et les organes chargés de

l'application des lois responsables au premier chef du maintien de l'ordre public et de la détection et la prévention des infractions, des enquêtes et des poursuites) ;

b) Extérieure au service, donnée exclusivement par un responsable politique occupant des fonctions au sein de l'exécutif, en général un ministre, voire parfois le Premier Ministre ;

c) Extérieure au service, donnée exclusivement par un ou plusieurs membres du pouvoir judiciaire, sans intervention d'aucun responsable politique à aucun stade du processus ;

d) Extérieure au service, donnée selon un système hybride, dit « à double verrou », dans lequel l'autorisation est donnée par un responsable politique puis contrôlée par un ou plusieurs membres du pouvoir judiciaire.

69. **Il est compréhensible que le gouvernement élu d'un pays, composé en grande partie ou exclusivement de responsables politiques, définisse les priorités en matière de politique étrangère et donc qu'il fixe raisonnablement des priorités opérationnelles à ses services de renseignement. Ces grandes orientations en matière de renseignement extérieur incluront nécessairement des questions relatives aux pays alliés et pays ennemis, aux partenaires de négociation et partenaires commerciaux, aux pays à qui il faut prêter assistance, à ceux dont il faut se méfier et à ceux qu'il ne faut veiller à ne pas froisser. Les choses sont assez différentes pour ce qui est des questions de sécurité nationale liées aux activités des services du renseignement intérieur, car celles-ci devraient être suffisamment encadrées par la Constitution, qu'elles visent en principe à protéger, et par les dispositions détaillées des lois nationales garantissant la protection des droits de l'homme fondamentaux.**

70. **En ce qui concerne le respect de la vie privée, la règle est claire : il ne peut être porté atteinte à la vie privée, sauf pour des motifs spécifiques tels que la sécurité nationale ou la détection et la prévention des infractions, les enquêtes et les poursuites. Même dans ces circonstances, l'ingérence dans la vie privée n'est autorisée que si l'on a recours à des moyens prévus par la loi et qui sont nécessaires et proportionnés dans une société démocratique, qu'il soit question de renseignement extérieur ou de renseignement intérieur. Les contrôles et contrepoids qui s'exercent devraient être tout aussi clairs : les responsables politiques de la branche législative du pouvoir, sous la conduite de l'exécutif, dans la plupart des démocraties, élaborent et approuvent les lois qui garantissent le respect de la vie privée et définissent les recours possibles. Les services de sécurité et les organes responsables de l'application de la loi, qui en règle générale relèvent de l'exécutif, agissent dans le cadre strict de la loi. La légalité de leurs actions est ensuite contrôlée par le pouvoir judiciaire.**

71. **Un autre contre-pouvoir est exercé par le pouvoir législatif au moyen de commissions parlementaires chargées de contrôler les activités des services de sécurité. Dans la plupart des cas, même si ces commissions sont utiles, il ne s'agit que d'une forme de haut niveau de contrôle *ex post*, essentiellement limité à la vérification de la bonne exécution des politiques et de l'utilisation des ressources budgétaires approuvées par le pouvoir législatif, car ces commissions ne disposent pas du temps, des ressources et des connaissances techniques nécessaires pour procéder à un examen approfondi des opérations.**

72. **Rien ne prouve, et encore moins de manière irréfutable, que l'intervention de responsables politiques, de l'exécutif ou du pouvoir législatif, apporte une quelconque valeur ajoutée aux décisions prises au quotidien pour déterminer qui devrait être mis sous surveillance, quand et pourquoi, en particulier lorsque l'on parle de renseignement intérieur. Au contraire, l'histoire regorge d'exemples de responsables politiques qui font un usage abusif du renseignement intérieur pour se maintenir au pouvoir. En règle générale, il convient d'éviter dans toute la mesure possible que des responsables politiques soient impliqués dans les décisions ad hoc visant à déterminer quelle ligne téléphonique mettre sur écoute, dans quel smartphone déployer un logiciel malveillant, dans quel bureau ou quelle chambre à coucher placer des micros, et quand et pourquoi mettre en place de telles mesures. Dans le passé prédémocratique de la plupart des pays, la direction et le contrôle des activités des espions faisaient partie des prérogatives d'un**

pouvoir exécutif tout-puissant. C'est un héritage dont de nombreuses démocraties ne sont pas encore parvenues à se défaire. Alors que rien ne prouve qu'une telle pratique aie une quelconque valeur ajoutée, il reste encore plusieurs démocraties dynamiques où ce sont des membres de l'exécutif qui décident au quotidien qui doit être espionné.

73. **Les pratiques optimales recensées au niveau mondial suggèrent ce qui suit** :

a) Les agents des services de renseignement et des services de police de tous rangs devraient recevoir une formation complète sur les droits de l'homme qui mette l'accent sur les conduites et les mesures nécessaires et proportionnées dans une société démocratique ;

b) Tout agent des services de renseignement ou des services de police qui souhaite mettre en place une forme quelconque de surveillance doit être tenu par la loi de démontrer que cette surveillance s'inscrit dans le cadre de la loi et répond aux critères de nécessité et de proportionnalité, et ce, à chaque étape du processus d'autorisation interne à un service ;

c) Tout responsable des services de renseignement ou des organes d'application des lois qui doit autoriser une opération exigeant la mise en place d'une forme quelconque de surveillance doit être tenu de vérifier que celle-ci s'inscrit dans le cadre de la loi et répond aux critères de nécessité et de proportionnalité et de refuser d'autoriser la surveillance si celle-ci n'a pas une base légale suffisante ou ne répond pas aux critères de nécessité et de proportionnalité ;

d) À condition que les critères de légalité, de nécessité et de proportionnalité soient appliqués de façon cohérente et à différents niveaux au sein d'un service, il est en général préférable de laisser aux professionnels de ce service qui ont une connaissance approfondie et actuelle des risques et des acteurs le soin de décider en premier lieu qui devrait être placé sous surveillance, quand et pourquoi. Ces décisions prises en interne devraient cependant toujours être validées par une instance ou une personne extérieure réellement indépendante. Il peut être nécessaire de réfréner des services trop zélés ou qui commettraient des abus, mais souvent les responsables politiques ne sont pas les mieux placés pour assurer un contrôle approprié ;

e) Dans certains pays, l'autorisation externe est traditionnellement donnée par un juge, qui n'a parfois reçu, au mieux, qu'une formation minimale concernant le fonctionnement d'un service de renseignement ou de maintien de l'ordre. Même si ce système d'autorisation fonctionne raisonnablement bien dans certains cas, cette pratique a entraîné de grandes variations dans la qualité des décisions prises en matière de surveillance : dans certains pays, certains juges − ou de nombreux juges − sont excellents et s'imposent solidement face aux services qui demandent l'autorisation de mettre en place des mesures de surveillance, tandis que, dans d'autres pays, les juges se contentent d'acquiescer. Ailleurs encore, c'est l'indépendance même des juges qui est remise en cause et, par voie de conséquence, on peut alors douter de leur capacité à s'opposer réellement à certaines demandes de surveillance émanant de l'exécutif, en particulier s'ils dépendent de ce même pouvoir exécutif pour la reconduite dans leurs fonctions. Dans d'autres pays encore, l'entité extérieure chargée d'autoriser les opérations n'est souvent extérieure qu'au service concerné sans pour autant être détachée de l'exécutif, et il s'agit souvent d'un membre de haut rang de l'exécutif, comme un ministre ou le Premier Ministre lui-même ;

f) Depuis 2015, certains pays, par exemple les Pays-Bas et le Royaume-Uni, se sont dotés, comme la France, d'autorités spécialisées véritablement indépendantes réunissant plusieurs domaines de compétence (législative, opérationnelle et technique), mais dans lesquelles, comme c'est le cas aussi en France, les responsables politiques continuent d'intervenir à un stade ou un autre de l'adoption des décisions en matière de surveillance. Il semble que la qualité des décisions prises en matière de surveillance ne serait pas amoindrie si l'autorisation externe était donnée :

i) Dans le cas du renseignement intérieur, exclusivement par l'organisme indépendant spécialisé ;

ii) Dans le cas du renseignement extérieur, exclusivement par l'organisme indépendant spécialisé, qui devrait toutefois prendre en compte les avis que le Ministère des affaires étrangères pourrait émettre sur la question.

74. **La France a montré l'exemple en créant, par une loi, une solide instance ou autorité de contrôle des activités de surveillance indépendante et spécialisée, la CNCTR. La France mais aussi l'Allemagne, les Pays-Bas et le Royaume-Uni, en Europe, et le Canada et les États-Unis, en Amérique du Nord, ont consacré beaucoup de réflexion, d'efforts et de temps de débat législatif à la mise en place d'une ou de plusieurs instances indépendantes[14] chargées de contrôler toutes les activités des services de sécurité et des services de renseignement nationaux. Le Rapporteur spécial considère qu'il s'agit là d'une bonne pratique, qu'il recommande vivement à tous les États Membres d'adopter. À cet égard, la France s'est acquittée également de ses obligations internationales en suivant l'esprit et la lettre de l'article 9 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et de l'article 11 de cette convention modernisée en adoptant une loi qui prévoit des garanties, dont l'autorité indépendante de contrôle est l'une des plus importantes.**

75. **Comme on l'a vu plus haut, dans la partie du présent rapport consacrée à la surveillance, le système juridique français prévoit la participation de responsables politiques au processus d'autorisation préalable (*ex ante*) de la surveillance, la décision prise par l'exécutif étant ensuite examinée par l'organisme de contrôle indépendant. Compte tenu de la participation de la CNCTR depuis 2015, on pourrait dire du système français de contrôle de la surveillance qu'il est hybride[15], puisque la demande est examinée par l'organisme de contrôle indépendant (la CNCTR) avant que la décision soit prise par un responsable politique (le Premier Ministre). La France n'est pas le seul pays démocratique qui continue d'utiliser cette approche, qui rappelle cependant des temps anciens où l'exécutif était le pouvoir suprême, souverain et incontesté. C'est aussi une approche qui, dans de nombreux pays, met mal à l'aise les responsables politiques et les représentants de la société civile et suscite la crainte, exprimée auprès du Rapporteur spécial, de voir l'exécutif en place abuser de ce pouvoir. Ce n'est donc pas une approche que le Rapporteur spécial recommanderait en tant que bonne pratique. Même si rien ne peut laisser penser que les Premiers Ministres français qui se sont succédé depuis l'adoption des réformes en 2015 aient abusé de ce pouvoir, il serait préférable qu'à l'occasion de prochaines réformes, le mécanisme soit modifié de manière à ce que l'autorisation *ex ante* de la surveillance soit donnée par un organisme totalement indépendant, sans qu'aucun responsable politique ne soit impliqué dans le processus. La France montrerait ainsi l'exemple au reste du monde, où les exemples de responsables politiques qui s'accrochent au pouvoir en abusant de leur autorité ne manquent pas.**

76. **On ne saurait en aucun cas dire du système de contrôle du renseignement de la France qu'il est défaillant. Bien au contraire, il est relativement robuste et semble bien fonctionner dans la pratique. Toutefois, la CNCTR n'a actuellement qu'un rôle purement consultatif et, d'autant plus si la participation d'un responsable politique au processus de décision devait perdurer, le pouvoir de révoquer une décision concernant la surveillance devrait être inscrit dans la loi, de même que les bonnes pratiques décrites aux alinéas a) à c) du paragraphe 73 . Au minimum, la CNCTR devrait avoir autorité pour annuler et révoquer toute autorisation de surveillance accordée par le Premier Ministre, sachant qu'il serait encore bien préférable que celui-ci ne prenne jamais part à de telles décisions.**

[14] Certaines instances sont plus indépendantes que d'autres. Voir, à ce propos, le rapport du Rapporteur spécial sur sa visite aux États-Unis en 2017, qui sera soumis au Conseil des droits de l'homme à sa quarante-sixième session, et le courrier adressé au Gouvernement de ce pays en juillet 2020, dans lequel le Rapporteur spécial a dit regretter que, par sa structure, le droit américain laisse toute latitude au Président des États-Unis pour destituer l'Inspecteur général de la direction du renseignement, ce qui pourrait aller à l'encontre de l'indépendance de cette fonction et à son efficacité.

[15] Sauf dans les cas où la surveillance est ordonnée par un juge d'instruction ou un magistrat.

77. **Au cours d'autres consultations tenues après la visite, il a été dit que la participation de l'exécutif au système d'autorisation des activités de surveillance trouvait son fondement dans le droit et la pratique constitutionnels. La France a largement contribué à poser les bases de la théorie de la séparation des pouvoirs, et il est peut-être temps pour elle d'être une nouvelle fois à l'initiative d'un nouveau mode de pensée, après 300 ans de mise en pratique des idées de Montesquieu, Voltaire et Rousseau au niveau national et mondial. Les philosophes des Lumières ne pouvaient pas savoir quelles conséquences les technologies modernes auraient un jour, y compris en matière de compétences spécialisées. La France devrait sérieusement envisager de montrer la voie à suivre concernant la prochaine refonte de la doctrine de la séparation des pouvoirs, en créant ou en consolidant un organisme hybride, distinct et indépendant. Il reste à déterminer si un tel organisme devrait être indépendant de la CNCTR et être responsable uniquement de l'autorisation *ex ante*. Une autre solution pourrait consister à donner à la CNCTR un statut plus élevé de manière à ce que ses décisions qu'elle prend en matière de surveillance, avant les opérations ou a posteriori, soient définitives**[16]**. Le plus important est que cette autorité indépendante distincte soit dotée de ressources adéquates regroupant plusieurs domaines de compétence (juridique, opérationnelle et technique), en continuant éventuellement de bénéficier de la contribution de juges expérimentés, et soit habilitée à autoriser et/ou à contrôler les opérations de surveillance en prenant des décisions en toute indépendance et souvent même sans que l'exécutif en ait connaissance.**

78. **Le Rapporteur spécial a pris note avec satisfaction de la pratique adoptée par la CNCTR, à la demande du Gouvernement français, consistant à appliquer au renseignement extérieur le même régime de garanties que celui qui est appliqué aux activités de renseignement intérieur, en dépit du fait que, à proprement parler, la loi relative à la surveillance internationale (loi nº 2015-1556 du 30 novembre 2015) n'est pas aussi stricte sur ces questions que la loi relative au renseignement intérieur (loi nº 2015-912 de juillet 2015). Compte tenu du succès de cette expérimentation, et conformément aux principes du droit international, le Rapporteur spécial observe que cette pratique de facto pourrait utilement devenir *de jure*. Il recommande très vivement que les prochaines réformes qui seront apportées à la législation dans ce domaine soient l'occasion d'aligner le système de garanties et de recours applicable au renseignement extérieur sur celui qui s'applique au renseignement intérieur. Cela va dans le sens de la recommandation faite par le Rapporteur spécial au Conseil des droits de l'homme selon laquelle la vie privée ne devrait pas être un droit qui dépend du passeport que l'on a en poche. La vie privée d'un individu devrait être protégée indépendamment du lieu où il se trouve physiquement**[17]**. Cette mesure permettrait également à la France de montrer au reste du monde la voie à suivre, tout comme l'a fait l'Allemagne, dont la Cour constitutionnelle, en mai 2020, a obligé le Gouvernement à modifier la loi relative au renseignement extérieur afin de la rendre plus équitable et plus protectrice des droits de l'homme.**

79. **En France, les réformes législatives de 2015 ont inscrit dans la loi une pratique optimale en donnant à la CNCTR un accès illimité aux journaux de connexion et données collectés dans le cadre des activités autorisées par le Premier Ministre. Le Rapporteur spécial recommande que cette pratique soit étendue à l'ensemble des fichiers et enregistrements des services de renseignements. C'est une pratique indispensable que tous les États Membres devraient imiter et un bon exemple donné par la législation française. Il ne sert à rien de créer une instance de contrôle si celle-ci**

[16] Au Royaume-Uni, le Bureau du commissaire chargé des pouvoirs d'enquête prend les décisions *ex ante* et *ex post* dans toutes les affaires de surveillance, que l'opération de surveillance soit menée par un service de renseignement ou par un organe chargé du maintien de l'ordre. Comme le Rapporteur spécial l'indique dans le rapport qu'il a établi à l'issue de sa visite au Royaume-Uni (qui sera soumis au Conseil des droits de l'homme à sa quarante-sixième session), le Bureau semble être devenu un organisme de contrôle très efficace et les commentaires laissant entendre qu'en intervenant *ex ante* et *ex post* il pouvait être accusé de « noter son propre travail » ont été contestés.

[17] Sauf dans certaines circonstances telles que l'emprisonnement, où une surveillance particulière peut être autorisée par la loi, dans le respect de modalités clairement définies.

n'a pas l'autorité légale et les ressources nécessaires pour s'acquitter convenablement de sa tâche et n'a pas pleinement accès aux dossiers et aux systèmes informatiques des services de renseignement et des forces de l'ordre.

80. **Une autre pratique optimale que la CNCTR a développée consiste à maintenir au sein de sa structure − et à déployer − des compétences techniques. En examinant et en testant, avant leur déploiement opérationnel, les codes sources des algorithmes utilisés pour analyser les métadonnées des communications, la CNCTR a établi une nouvelle garantie appliquant à première vue les principes de la surveillance ciblée demandés par la Cour européenne des droits de l'homme et la Cour de justice européenne.**

81. **Le Rapporteur spécial note en outre avec satisfaction que, dans le cas où l'analyse de métadonnées automatisée fait ressortir un ensemble de transactions ou d'utilisateurs présentant un intérêt, le service de renseignement qui a demandé l'analyse doit demander à l'instance de contrôle, c'est-à-dire à la CNCTR, l'autorisation d'accéder aux bases de données concernées.**

82. **Le Rapporteur spécial a pris note avec satisfaction des importantes avancées enregistrées dans la mise en place de voies de recours ouvertes aux citoyens dans le cadre du système de contentieux administratif. La loi de 2015 a en effet donné une nouvelle voie de recours importante aux citoyens en cas de collecte illégale de leurs données personnelles en créant, au sein du Conseil d'État, une formation spécialisée composée de cinq juges ayant accès aux fichiers des services de renseignement.**

83. **À la suite de ses échanges avec des juges et des représentants de la CNIL et de la Commission nationale consultative des droits de l'homme, le Rapporteur spécial recommande très vivement que tous les juristes de formation qui contribuent au contrôle des activités de surveillance reçoivent aussi une formation appropriée en matière de technologies de l'information et de la communication ainsi qu'aux pratiques opérationnelles optimales.**

B. Modernisation de la loi française sur la protection des données

84. **État membre de l'Union européenne, la France a récemment achevé sa deuxième année de mise en œuvre du règlement général sur la protection des données. Le règlement prévoyant un mécanisme de suivi, il est attendu du Gouvernement français ainsi que des autorités et ministères compétents qu'ils apportent leur contribution au processus de suivi mené au niveau de l'Union européenne.**

C. Vie privée et données de santé

85. **La pandémie de maladie à coronavirus (COVID-19) a été l'occasion d'une réflexion, notamment sur le détail de la mise en œuvre des dispositions du règlement général sur la protection des données concernant les données de santé. Le Rapporteur spécial a traité la plupart des questions, sinon toutes les questions que soulèvent l'informatisation des dossiers médicaux, l'utilisation de l'intelligence artificielle dans ce domaine, les applications de traçage des contacts et les normes à respecter, y compris en temps de pandémie, dans les recommandations qu'il a formulées sur la protection et l'utilisation des données de santé[18] et dans une note explicative accompagnant ces recommandations[19]. Il attire respectueusement l'attention du Gouvernement français sur les recommandations relatives à la protection des données de santé figurant dans le rapport qu'il a soumis à l'Assemblée générale en août 2019[20]. Ces recommandations sont en parfaite adéquation avec les principes énoncés dans le règlement général sur la protection des données et dans la Convention pour la protection des personnes à l'égard**

[18] A/74/277, annexe.

[19] Voir www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf.

[20] A/74/277.

du traitement automatisé des données à caractère personnel modernisée, mais vont au-delà de ces principes sur certains points. Le Rapporteur spécial encourage vivement le Gouvernement français à mener une réflexion sur les succès − et les échecs − des démarches qu'il a engagées pour mettre les technologies appliquées, en particulier les applications pour téléphones mobiles, au service de la lutte contre la pandémie de COVID-19.

D. Genre et vie privée

86. **Au cours de sa visite, le Rapporteur spécial a observé que, dans certaines circonstances, le genre pouvait influer sur la jouissance du droit à la vie privée. Il attire donc respectueusement l'attention du Gouvernement français sur les conclusions et recommandations relatives au respect de la vie privée et au genre figurant dans le rapport qu'il a soumis au Conseil des droits de l'homme en mars 2020[21]. Les principes énoncés dans ce rapport devraient être strictement respectés et appliqués dans toute réforme à venir et dans toute contribution de la France au débat sur l'examen et la réforme des lois applicables en matière de protection des données, y compris le règlement général sur la protection des données.**

E. Mégadonnées, données ouvertes, enfants et vie privée

87. **Lors d'un événement organisé à Paris avec le soutien du Fonds des Nations Unies pour l'enfance (UNICEF) six mois avant sa visite officielle en France, le Rapporteur spécial a pris la mesure de l'inquiétude de la société civile au sujet de la vie privée des enfants. Dans certains cas, des technologies avancées, notamment des techniques d'analyse des mégadonnées, avaient été déployées ou été envisagées. Le Rapporteur spécial souhaite donc attirer l'attention du Gouvernement français sur les conclusions et recommandations figurant dans ses rapports sur les mégadonnées et les données ouvertes[22] et sur le genre et la vie privée[23], ainsi que les conclusions et recommandations figurant dans le rapport sur la vie privée et les enfants qu'il soumettra au Conseil des droits de l'homme à sa quarante-sixième session, en mars 2021.**

F. Harmonisation de la législation, des politiques et de la pratique fédérales et de celles des États

88. **La France n'étant pas un État fédéral, le Rapporteur spécial n'a pas, à son égard, les mêmes préoccupations que celles qu'il a exprimées au sujet d'États fédéraux comme l'Allemagne, l'Argentine et les États-Unis.**

G. Rôle de la France sur la scène internationale

89. **Le Rapporteur spécial note que la France a signé le Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, signalant ce faisant son intention d'adhérer à cette convention telle qu'amendée, mais note aussi qu'elle n'a pas encore ratifié le Protocole. Le Rapporteur spécial, conscient cependant des perturbations causées par la pandémie de COVID-19, recommande vivement au Gouvernement français de concrétiser son intention et de ratifier le Protocole sans tarder.**

90. **Le Rapporteur spécial encourage vivement le Gouvernement français à jouer un rôle de premier plan dans la recherche du plus large consensus qui puisse être trouvé au niveau international sur les questions touchant le respect de la vie privée, en particulier les garanties applicables et les voies de recours disponibles en ce qui**

[21] A/HRC/43/52.
[22] A/72/540 et A/73/438.
[23] A/HRC/43/52.

concerne la surveillance exercée par les États. Depuis janvier 2020, la France est le seul État à la fois membre permanent du Conseil de sécurité et membre de l'Union européenne. Cette position lui confère une grande responsabilité, compte tenu en particulier de la soumission à l'Assemblée générale des deux initiatives distinctes sur le comportement des États dans le cyberespace. Le Rapporteur spécial prend note avec satisfaction de la participation de l'Ambassadeur pour le numérique de la France aux travaux du Groupe d'experts gouvernementaux chargé d'examiner les moyens de favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale. Mis à part le Royaume-Uni, la France est aussi le seul autre membre du Conseil de sécurité qui s'emploie à respecter les normes de protection de la vie privée dans les questions de sécurité nationale énoncées dans la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel telle que modifiée. Pour le Rapporteur spécial, la France est particulièrement bien placée pour jouer un rôle prépondérant s'agissant de jeter des ponts entre l'Europe et les États-Unis ainsi qu'entre l'Europe et le reste du monde sur les questions de vie privée et de surveillance.