.CONSEIL D'ETAT
Assemblée générale

Séance du jeudi 6 mai 2021

N° 402791

EXTRAIT DU REGISTRE DES DELIBERATIONS

AVIS SUR UNE LETTRE RECTIFICATIVE AU PROJET DE LOI

relatif à la prévention d'actes de terrorisme et au renseignement

NOR : INTD2113198L/Verte-2

1. Le Conseil d'Etat a été saisi le 28 avril 2021 d'une lettre rectificative au projet de loi relatif à la prévention d'actes de terrorisme et au renseignement qu'il avait examiné le 21 avril (Avis n° 402562). Trois saisines rectificatives à la lettre rectificative ont été reçues les 29 avril, 4 et 6 mai 2021 en ce qui concerne le texte du projet et, s'agissant de l'étude d'impact, le 30 avril 2021.

2. La lettre rectificative comprend 13 articles répartis dans quatre chapitres du projet de loi. Le chapitre I^{er} comporte une disposition renforçant la prévention d'actes de terrorisme. Le chapitre II est relatif au renseignement. Le chapitre III *bis* est relatif aux archives intéressant la défense nationale. Le dernier chapitre comporte des dispositions relatives à l'outre-mer.

3. L'étude d'impact correspondant à la lettre rectificative, reçue le 30 avril 2021, satisfait dans son ensemble aux exigences de la loi organique n° 2009-403 du 15 avril 2009.

Dispositions relatives au renseignement

4. La lettre rectificative tire d'abord les conséquences de la décision du 21 avril 2021 *French Data Network et autres* (n° 399099 - 397844 - 397851 - 424717 - 424718) par laquelle le Conseil d'État, statuant au contentieux, faisant suite à l'arrêt *La Quadrature du net et autres* (Cour de justice de l'Union européenne, grande chambre, 6 octobre 2020, C-511/18), rendu à titre préjudiciel par la Cour, s'est prononcé sur la compatibilité des dispositions de droit national relatives au renseignement et à la conservation des données de connexion avec les normes supérieures, conventionnelles et constitutionnelles.

Elle modifie également deux techniques de renseignement, celle dite « *de l'algorithme* » (art. L. 851-3 du code de la sécurité intérieure, CSI) et celle du recueil en temps réel des données de connexion (art. L. 851-2 du même code).

5. La Commission nationale de contrôle des techniques de renseignement (CNCTR) a été consultée en application de l'article L. 833-11 du CSI sur ces dispositions, de même que la Commission nationale de l'informatique et des libertés (CNIL) en application du *a* du 4° de

l'article 8 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP), en application de l'article L. 36-5 du code des postes et communications électroniques (CPCE).

Régime de conservation des données de connexion

6. L'article L. 34-1 du CPCE et l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique imposent aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs de contenus de conserver, pour une durée d'un an, l'ensemble des données de trafic et de localisation de leurs utilisateurs, les données relatives à leur identité civile ainsi que certaines informations relatives à leurs comptes et, le cas échéant, aux paiements qu'ils effectuent en ligne, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

7. La décision *French Data Network et autres* juge que la législation nationale ne peut, sans méconnaître le droit de l'Union européenne, imposer aux opérateurs de communications électroniques et aux fournisseurs d'accès à internet la conservation généralisée et indifférenciée des données de connexion, autres que les données relatives, d'une part à l'identité civile pour les besoins de toute procédure pénale, de la prévention de toute menace contre la sécurité publique et de la sauvegarde de la sécurité nationale et sans limitation de durée, d'autre part, aux adresses IP à des fins de recherche dans le cadre de la criminalité grave ou de prévention des menaces graves contre la sécurité publique pour une durée limitée au strict nécessaire et, enfin, aux informations autres que l'identité fournies lors de la souscription d'un contrat pour une durée d'un an (points 35 à 38). Elle admet, en revanche, qu'une telle obligation de conservation généralisée et indifférenciée peut être fondée sur la sauvegarde de la sécurité nationale et considère que toutes les finalités énumérées à l'article L. 811-3 du CSI doivent être regardées comme relevant de la sécurité nationale. Elle juge que pour être conforme au droit de l'Union, cette obligation doit être subordonnée au constat, à une échéance régulière qui ne saurait raisonnablement excéder un an, par une décision soumise à un contrôle effectif, de la persistance d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale. La décision relève que les menaces dont la France est l'objet sont de nature à justifier l'obligation de conservation générale et indifférenciée des données pour une durée d'un an (points 42 à 44).

8. La décision *French Data Network et autres* juge également que pour garantir le respect des objectifs de valeur constitutionnelle de prévention des atteintes à l'ordre public, notamment des atteintes à la sécurité des personnes et des biens, ainsi que la recherche des auteurs des infractions pénales, la technique de « conservation rapide », prévue par la convention sur la cybercriminalité signée à Budapest le 23 novembre 2001, permet de protéger la conservation et l'intégrité des données nécessaires à la poursuite de ces finalités pendant une durée de quatre-vingt-dix jours renouvelable, y compris lorsque cette conservation porte sur des données initialement conservées aux fins de sauvegarde de la sécurité nationale. Elle en déduit que l'autorité judiciaire est en mesure d'accéder aux données nécessaires à la poursuite et à la recherche des auteurs des infractions pénales dont la gravité le justifie et que le même principe s'applique aux autorités administratives, en particulier les autorités administratives indépendantes, disposant d'un droit d'accès en vertu de la loi en vue de lutter contre les manquements graves aux règles dont elles ont la charge d'assurer le respect (points 55 à 57).

9. Le projet de loi modifie en conséquence l'article L. 34-1 du CPCE pour préciser que les opérateurs de communications électroniques sont tenus de conserver :

- les informations relatives à l'identité de l'utilisateur jusqu'à l'expiration d'un délai de cinq ans après la fin de validité de son contrat ;

- les autres informations fournies par l'utilisateur lors de la souscription de son contrat ou de la création d'un compte, ainsi que les informations relatives au paiement, pour une durée d'un an ;

- les données techniques permettant d'identifier l'utilisateur ou relatives aux équipements terminaux de connexion utilisés, pour une durée d'un an.

Le projet prévoit qu'en cas de menace grave, actuelle ou prévisible pour la sécurité nationale, le Premier ministre peut enjoindre aux opérateurs de communications électroniques, par un décret dont la durée d'application ne peut excéder un an, de conserver, pour une durée d'un an, en complément de leurs obligations de conservation pour leurs propres besoins, certaines catégories de données relatives aux communications électroniques dont la nature sera précisée par un décret en Conseil d'Etat.

Le projet, tel qu'il résulte de la saisine rectificative reçue le 6 mai 2021, prévoit enfin de créer un régime transversal de conservation permettant à toutes les autorités disposant en vertu de la loi d'un accès aux données relatives aux communications électroniques, aux seules fins de prévention et de répression de la criminalité grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, d'adresser aux opérateurs une injonction de conservation rapide des données qu'ils détiennent.

L'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique est également modifié pour rendre applicables ces dispositions aux fournisseurs d'accès à internet et aux hébergeurs de contenus.

Ces dispositions appellent les observations suivantes du Conseil d'Etat.

10. Les nouvelles règles fixées par le projet sur la conservation, pour un délai de cinq ans, des informations relatives à l'identité civile de l'utilisateur et pour un délai d'un an des informations fournies par l'utilisateur lors de la souscription de son contrat ainsi que des informations de paiement, répondent aux exigences qui résultent de la décision *French Data Network et autres* et de l'arrêt *La Quadrature du net et autres.* Le Conseil d'Etat suggère de préciser que le point de départ du délai d'un an pour la conservation des informations fournies par l'utilisateur lors de la souscription de son contrat, ainsi que des informations de paiement, est la fin de validité du contrat ou, le cas échéant, la clôture de son compte.

11. Le Conseil d'Etat interprète l'obligation faite aux opérateurs de conserver pendant un délai d'un an les « *données techniques permettant d'identifier l'utilisateur ou relatives aux équipements terminaux de connexion utilisés* » comme visant la conservation des adresses « IP », c'est-à-dire des données permettant l'identification de la source d'une connexion sur un réseau et des données nécessaires à l'identification des équipements terminaux de téléphonie ainsi que, le cas échéant, des utilisateurs de ces réseaux ou de ces terminaux et que le point de départ du délai d'un an de conservation de ces données est la connexion ou l'utilisation des équipements terminaux. Il propose d'aménager la rédaction du texte à cet effet. Il souligne que la nature de ces données, comme l'a rappelé la CNIL dans son avis, ne peut permettre d'en connaître la localisation. La durée de conservation d'un an retenue répond au critère de stricte nécessité posé dans la décision *French Data Network et autres* (point 40).

12. Le Conseil d'Etat relève cependant que le projet impose ces obligations de conservation des données de connexion sans préciser les finalités pour lesquelles elles peuvent l'être, telles que celles-ci ont été précisées par la décision *French Data Network et autres* et l'arrêt *La Quadrature du net et autres.* Or, l'encadrement de la conservation des données, tel que fixé dans ces décisions, diffère selon la nature des données, les finalités poursuivies et le type de conservation. Le Conseil d'Etat considère que la mise en conformité avec les exigences du droit de l'Union impose de préciser les finalités auxquelles est associée l'obligation de conservation de chaque type de données, d'autant que les textes de droit national régissant l'accès aux données ne comportent pas toujours les finalités pour lesquelles cet accès est autorisé. Il précise en conséquence, dans la rédaction qu'il adopte, quelles sont les finalités associées à chaque type d'obligation de conservation.

13. Le Conseil d'Etat estime que le régime transversal de conservation rapide des données prévu par le projet répond, dans son principe, aux exigences résultant de la décision *French Data Network et autres*. Ce régime permettra à l'autorité judiciaire et aux autorités disposant en vertu de la loi d'un accès aux données relatives aux communications électroniques d'adresser aux opérateurs, pour la poursuite de finalités conformes au droit de l'Union européenne, une demande destinée à protéger la conservation et l'intégrité des données de connexion déjà conservées, afin d'y accéder. Ce régime transversal pourrait néanmoins justifier des aménagements sectoriels portant sur ses modalités et sa durée. Le Conseil d'Etat invite en conséquence le Gouvernement à procéder à une revue de l'ensemble des textes régissant l'accès de l'autorité judiciaire et des autorités concernées aux données de connexion et à les adapter si nécessaire.

14. Le Conseil d'Etat observe enfin que la procédure d'injonction de conservation des données de connexion par un décret du Premier ministre permettra une appréciation annuelle régulière, sous le contrôle du juge administratif, de la réalité et de la gravité de la menace pour la sécurité nationale et de la nécessité de prolonger la conservation générale et indifférenciée des données de connexion. Cette procédure répond aux exigences du droit de l'Union européenne.

Il précise que les données, dont la liste sera fixée par un décret en Conseil d'Etat, sur lesquelles est susceptible de porter l'injonction de conservation sont des données de trafic ou de localisation.

Contrôle préalable à la mise en œuvre des techniques de renseignement sur le territoire national

15. La décision *French Data Network et autres* et l'arrêt *La Quadrature du net et autres,* jugent que la mise en œuvre de plusieurs des techniques de renseignement prévues aux articles L. 851-1 à L. 851-4 du CSI n'est pas compatible avec les exigences du droit de l'Union dès lors que, sauf urgence dûment justifiée, elle ne donne pas lieu à un contrôle préalable par une juridiction ou par une autorité administrative indépendante dotée d'un pouvoir de décision contraignant.

En conséquence le projet de loi procède à plusieurs modifications du livre VIII du code de la sécurité intérieure.

16. Il prévoit, d'abord, à l'article L. 821-1 du CSI, que lorsque l'autorisation de mise en œuvre d'une technique de renseignement sur le territoire national est délivrée après avis défavorable de la CNCTR, le Conseil d'État est immédiatement saisi et statue dans un délai de vingt-quatre heures. La décision d'autorisation du Premier ministre ne peut être exécutée

avant que le Conseil d'État ait statué, sauf en cas d'urgence dûment justifiée lorsque le Premier ministre a ordonné sa mise en œuvre immédiate.

Ce dispositif de saisine du Conseil d'Etat en cas d'avis défavorable de la CNCTR est déjà prévu au III de l'article L. 853-3 du CSI, dans l'hypothèse où une autorisation d'introduction dans un lieu privé à usage d'habitation pour y placer un dispositif de captation est prise après un avis défavorable de la commission. Le choix retenu par le Gouvernement a pour effet de généraliser cette procédure à l'ensemble des techniques de renseignement relevant des chapitres I à III du titre V du livre VIII du code de la sécurité intérieure.

Ce choix, qui combine un mécanisme d'avis conforme d'une autorité administrative indépendante avec celui d'un contrôle préalable et effectif d'une juridiction lorsque le Premier Ministre passe outre l'avis défavorable de la CNCTR, assure une mise en conformité avec le droit de l'Union et n'appelle pas d'observation du Conseil d'Etat.

17. Le texte permet au Premier ministre de mettre en œuvre immédiatement sa décision, en cas d'avis défavorable de la CNCTR, sans attendre que le Conseil d'Etat ait statué, même si la décision de celui-ci est rendue dans le délai de vingt-quatre heures, en invoquant l'urgence.

Cette faculté est ouverte au Premier ministre pour l'ensemble des techniques de renseignement, à l'exception de la mise en œuvre d'un algorithme en application des I et II de l'article L. 851-3.

Elle est en outre restreinte aux finalités mentionnées aux 1°, 4° et au *a* du 5° de l'article L. 811-3 du CSI (défense et promotion de l'indépendance nationale, de l'intégrité du territoire et de la défense nationale ; prévention du terrorisme ; prévention des atteintes à la forme républicaine des institutions) pour les trois techniques suivantes :

- la captation de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé (art. L. 853-1 du CSI) ;

- le recueil et la captation de données informatiques par des dispositifs techniques (art. L. 853-2) ;

- l'introduction dans un lieu privé afin d'y mettre en place un dispositif de captation (art. L. 853-3).

Enfin, lorsque la technique est celle de l'article L. 853-3 et porte sur un lieu privé à usage d'habitation, le caractère d'urgence ne peut être invoqué que si l'autorisation a été délivrée pour la finalité de prévention du terrorisme.

Par voie de conséquence, le projet supprime l'article L. 821-5 qui permet au Premier ministre, en cas d'urgence et pour un nombre limité de finalités, de délivrer une autorisation de mise en œuvre d'un certain nombre de techniques de renseignement, sans avis préalable de la CNCTR.

18. Le Conseil d'Etat observe que la décision *French Data Network et autres* et l'arrêt *La Quadrature du Net* permettent de faire exception au contrôle préalable en cas d'« *urgence dûment justifiée* ». Dans l'hypothèse où, en cas d'avis défavorable de la CNCTR, le pouvoir exécutif aurait invoqué l'urgence et décidé la mise en œuvre immédiate d'une technique de renseignement, il note que le délai de vingt-quatre heures dans lequel le Conseil d'Etat devra

statuer, comme les pouvoirs qui lui sont conférés en application de l'article L. 773-7 du code de justice administrative, permettront, s'il y a lieu, de faire cesser sans délai l'atteinte disproportionnée portée au droit au respect de la vie privée en annulant l'autorisation et en ordonnant la destruction de l'intégralité des captations ou enregistrements effectués. L'équilibre ainsi aménagé entre la sauvegarde de la sécurité nationale en cas d'urgence dûment justifiée et l'ingérence dans la vie privée lui paraissent conformes au droit de l'Union ainsi qu'aux exigences constitutionnelles.

19. Il estime toutefois, comme la CNCTR, que le projet permet d'invoquer l'urgence lorsque la mise en œuvre de la technique est sollicitée pour un parlementaire, un magistrat, un avocat ou un journaliste, alors que l'article L. 821-7 du CSI prohibe la surveillance de ces personnes à raison de l'exercice de leur mandat ou de leur profession. Il considère par suite nécessaire de prévoir que l'urgence ne peut être invoquée lorsque la demande porte sur ces personnes afin que la formation spécialisée du Conseil d'Etat puisse statuer, avant tout début d'exécution de la technique de renseignement envisagée, sur les conditions de sa légalité.

20. S'agissant du contrôle préalable de l'accès aux données, par les autorités autres que les services de renseignement, le Conseil d'Etat recommande au Gouvernement, comme il l'avait fait lors de son examen du projet de loi renforçant la confiance dans l'institution judiciaire (Avis n° 402569 – Assemblée générale 8 avril 2021, point 18), d'évaluer les conséquences à tirer des arrêts du 21 décembre 2016, Tele2 Sverige AB (C-203/15) et Secretary of State for the Home Department (C-698/15) et du 2 mars 2021 (H/K Prokuratuur, C-746/18), sous réserve que ce que la Cour de justice a jugé pour le procureur estonien soit transposable en France.

Traitement automatisé des données de connexion (technique de « l'algorithme »)

21. L'article L. 851-3 du CSI permet aux services de renseignement, à titre expérimental jusqu'au 31 décembre 2021, de faire fonctionner des traitements automatisés sur les données de connexion des opérateurs de communication électronique aux fins de détecter des connexions susceptibles de révéler une menace terroriste. La mise en œuvre de ces traitements est autorisée par la Premier ministre après avis de la CNCTR pour une durée de deux mois, renouvelable pour une durée de quatre mois. La demande de renouvellement comporte un relevé du nombre d'identifiants signalés et de la pertinence de ces signalements. La CNCTR dispose d'un accès permanent, complet, et direct aux traitements. Lorsque ceux-ci détectent des données susceptibles de caractériser une menace à caractère terroriste, le Premier ministre peut autoriser, après avis de la CNCTR, l'identification de la personne concernée. Ces données sont exploitées dans un délai de soixante jours et sont détruites à l'issue de ce délai, sauf en cas d'éléments sérieux confirmant l'existence d'une menace terroriste.

Le Conseil constitutionnel a jugé ce dispositif conforme à la Constitution dans sa décision n° 2015-713 DC du 23 juillet 2015. La décision *French Data Network et autres* et l'arrêt *La Quadrature du net et autres* ont jugé compatibles avec le droit de l'Union ces dispositions de l'article L. 851-3, à l'exception du IV de cet article dans la mesure où l'identification de la personne concernée n'était pas subordonnée à un contrôle préalable exercé par une juridiction ou par une autorité administrative indépendante dotée d'un pouvoir contraignant. Ainsi qu'il a été dit au point 16 le projet modifie l'article L. 821-1 du même code pour remédier à cette inconventionnalité.

Le projet de loi prévoit de pérenniser la technique de l'algorithme, tout en y apportant plusieurs aménagements procéduraux. Il ajoute également les « *adresses*

complètes de ressources sur internet » au champ des données faisant l'objet d'un traitement automatisé.

22. S'agissant de la pérennisation, le Conseil d'Etat relève, d'une part, que ni le Conseil constitutionnel, ni la Cour de justice de l'Union européenne ne se sont fondés sur le caractère expérimental de la technique de l'algorithme pour juger les dispositions de l'article L. 851-3 du CSI conformes, respectivement, à la Constitution et au droit de l'Union.

Le Conseil d'Etat observe, d'autre part, que si l'étude d'impact contient des informations à caractère général sur le déroulement de l'expérimentation, elle comporte très peu d'indications sur la mesure de l'efficacité opérationnelle de la technique, couverte par le secret de la défense nationale. Il relève néanmoins qu'un rapport sur l'application de l'article L. 851-3 du CSI a été adressé à la délégation parlementaire au renseignement le 30 juin 2020. La CNCTR, destinataire de ce rapport et étroitement associée à l'expérimentation, a estimé dans sa délibération du 7 avril 2021 que la menace terroriste « *se traduit notamment par l'émergence de nouveaux profils d'individus isolés, sensibles aux messages de propagande incitant au passage à l'acte, dont le potentiel dangereux ne peut parfois être révélé qu'à travers leur activité numérique* » et considère que les « *impératifs de sécurité nationale justifient que le dispositif de l'article L. 851-3 soit conservé ».* Le Conseil d'Etat en prend acte.

S'agissant des aménagements procéduraux apportés au dispositif, le projet prévoit que seuls les services de renseignement du premier cercle pourront demander à mettre en œuvre des algorithmes. Il précise également que le Groupement interministériel de contrôle (GIC), service du Premier ministre, sera seul habilité à exécuter ces traitements sur les flux de données dupliquées depuis les réseaux des opérateurs. Enfin, il supprime la possibilité de conserver les données exploitées dans le cadre d'une identification faisant suite à un signalement au-delà de soixante jours. Ces aménagements apportent ainsi des garanties supplémentaires d'encadrement au dispositif.

23. S'agissant de l'ajout des *« adresses complètes de ressources sur internet* » aux données faisant l'objet d'un traitement automatisé, le Conseil d'Etat relève, comme la CNCTR et la CNIL, que de telles adresses, dont l'étude d'impact indique qu'elles sont assimilées aux « URL » (« *Uniform Ressource Locator* »), revêtent la nature de données à caractère mixte. Elles sont en effet susceptibles de comporter à la fois des données de connexion et des mots faisant référence au contenu de correspondances échangées ou d'informations consultées, sans toutefois être elles-mêmes porteuses de ce contenu. L'extension des données traitées par les algorithmes - qui jusqu'ici ne concernaient que les données de trafic et de connexion de téléphonie - aux adresses complètes Internet ouvre donc un champ nouveau d'investigation potentiellement attentatoire à la protection de la vie privée et des données personnelles.

Or le Conseil d'Etat observe que pour estimer conformes à la Constitution les dispositions de l'article L. 851-1 du CSI, le Conseil constitutionnel a notamment relevé que les données conservées et traitées par les opérateurs de communication électronique et susceptibles d'être recueillies par les services de renseignement « *ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications* » (Décision n° 2015-713 DC du 23 juillet 2015, ct 55) et que s'agissant des algorithmes « *ces traitements automatisés utilisent exclusivement les données de l'article L. 851-1* » (ct 58). Par ailleurs, la Cour de justice de l'Union, en jugeant conformes au droit de l'Union, dans leur principe, les dispositions de l'article L. 851-3 du CSI dans leur rédaction aujourd'hui applicable, ne s'est

prononcée que sur un traitement automatisé de « *données relatives au trafic et à la localisation* ». Le Conseil d'Etat estime en conséquence que dans ce cadre, l'ajout d'éléments relatifs au contenu des informations consultées dans le champ des données faisant l'objet de traitements automatisés à grande échelle, même sans possibilité d'identifier les personnes concernées, appelle un contrôle de proportionnalité exigeant entre les atteintes portées aux libertés d'une part et la protection des intérêts fondamentaux de la Nation de l'autre.

24. L'étude d'impact explique que, du fait de l'évolution des usages en matière de communication qui recourent de plus en plus à des applications Internet et non aux voies téléphoniques classiques, particulièrement dans le cas de la population qu'il s'agit de détecter, les adresses complètes Internet sont les données les plus pertinentes pour repérer les comportements caractérisés par les paramètres d'un algorithme, qui, fondé en partie sur les URL, pourrait ainsi permettre la détection de consultations ou de téléchargements caractérisant une menace. La CNCTR relève dans son avis que « *la menace terroriste persiste à un niveau très élevé et que le comportement d'auteurs d'actes terroristes est souvent caractérisé par une utilisation intensive d'internet (...) le besoin opérationnel d'utilisation d'URL dans le cadre de l'article L. 851-3 semble donc établi* ».

Le Conseil d'Etat prend acte des justifications ainsi données pour étendre le champ des données traitées afin d'adapter les techniques de détection de la menace à l'évolution des modes de communication.

25. Il estime toutefois que les garanties actuelles encadrant le recours aux traitements automatisés, tels que décrits aux points 22 et 23, doivent être renforcées.

A cette fin, le Conseil d'Etat complète le projet sur plusieurs points :

- il propose d'inscrire dans la loi que, à l'exception des données détectées par les traitements comme susceptibles de caractériser l'existence d'une menace à caractère terroriste, qui sont conservées pour faire l'objet d'une demande d'autorisation d'identification, les données issues des flux de communication dupliqués et traités par le GIC devront être détruites immédiatement ;

- ainsi que le recommande la CNCTR, il propose de circonscrire le traitement des adresses complètes de ressources sur Internet aux seules adresses effectivement utilisées par un utilisateur ;

- il recommande qu'un bilan de l'application de cette technique incluant l'analyse automatisée des URL soit remis par le Gouvernement au Parlement dans un délai de trois ans.

Il rappelle enfin que l'article L. 833-6 du CSI permet à la CNCTR d'adresser à tout moment au Premier ministre une recommandation tendant à ce qu'une technique de renseignement soit interrompue si elle est mise en œuvre dans des conditions non conformes au code et que ces dispositions s'appliquent à la technique de l'algorithme.

Au bénéfice de ces aménagements et précisions, le dispositif n'appelle pas d'objection.

Recueil de données de connexion en temps réel

26. L'article L. 851-2 du CSI autorise, pour les seuls besoins de la prévention du terrorisme, le recueil en temps réel sur les réseaux des opérateurs des données techniques de connexion relatives à « *une personne préalablement identifiée susceptible d'être en lien avec une menace* ». Cette technique est autorisée pour une durée de quatre mois renouvelable. La même technique peut également être autorisée individuellement pour les personnes appartenant à l'entourage de la personne identifiée, lorsqu'il existe des raisons sérieuses de penser qu'elles « *sont susceptibles de fournir des informations* » en relation avec la menace.

Dans sa décision n° 2017-648 QPC du 4 août 2017, le Conseil constitutionnel, s'il a admis la conformité de ces dispositions à la Constitution, en relevant notamment « *qu'elles excluent l'accès au contenu des correspondances* », a estimé qu'en s'appliquant aux personnes de l'entourage de la personne concernée - à la suite de l'introduction de cette extension par une loi du 21 juillet 2016 - le législateur avait « *permis que fasse l'objet de cette technique un nombre élevé de personnes sans que leur lien avec la menace soit nécessairement étroit* » et n'avait pas opéré une conciliation équilibrée entre la prévention des atteintes à l'ordre public et le droit au respect de la vie privée « *faute d'avoir prévu que le nombre d'autorisations simultanément en vigueur doive être limité* ». A la suite de cette décision, la loi du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme a introduit un contingentement des autorisations pouvant être délivrées en application de l'article L. 851-2 du CSI.

La décision *French Data Network et autres* et l'arrêt *La Quadrature du Net et autres* jugent que le droit de l'Union autorise le recueil en temps réel des données de trafic et de localisation lorsque celui-ci est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme. Bien que ce point n'ait pas été expressément jugé, il paraît possible de considérer que la Cour de justice n'a pas entendu limiter le dispositif aux personnes directement et personnellement impliquées dans une démarche ou une organisation terroriste et admis que pouvaient en faire l'objet les personnes ayant un lien étroit avec la menace, ce que permet d'assurer le contingentement des autorisations depuis la loi du 30 octobre 2017.

27. Le projet de loi inclut, dans le champ des données susceptibles de faire l'objet de ce recueil en temps réel, à l'instar de ce qu'il fait pour l'algorithme, les adresses complètes de ressources sur internet utilisées par une personne préalablement identifiée susceptible d'être en lien avec une menace.

Ainsi qu'il a été dit ci-dessus, le recueil de données prévu par l'article L. 851-2 du code de la sécurité intérieure est ciblé sur *« une personne préalablement identifiée susceptible d'être en lien avec une menace »* terroriste. Il note que le projet du Gouvernement tire les conséquences du caractère mixte des adresses complètes de ressources sur internet en proposant d'aligner la durée de conservation de ces adresses sur celle applicable aux renseignements collectés par la mise en œuvre des techniques de captation ou de recueil de données informatiques prévue par l'article L. 853-2 du CSI qui est de cent-vingt jours. Il estime, dans ces conditions, au regard de l'évolution des usages de communication décrits plus haut, que le projet opère une conciliation conforme à la Constitution entre, d'une part, la défense et la protection des intérêts fondamentaux de la Nation et, d'autre part, la protection du droit au respect de la vie privée et du secret des correspondances.

Il considère qu'eu égard aux garanties entourant la mise en œuvre de cette technique, parmi lesquelles figure le contingentement du nombre d'autorisations susceptibles d'être mises en œuvre en même temps, l'extension de son champ d'application aux URL utilisées par les personnes appartenant à l'entourage de la personne ciblée ne porte pas, au regard de

l'objectif de prévention du terrorisme, une atteinte disproportionnée au droit au respect de la vie privée de ces personnes.

Sur les dispositions relatives à la transmission d'informations par le procureur et le juge d'instruction aux services de renseignements

28. L'article 706-25-2 du code de procédure pénale (CPP) prévoit que, par dérogation au secret de l'enquête garanti par l'article 11 du même code, le procureur de la République antiterroriste, peut, pour les procédures ouvertes en matière de terrorisme, communiquer aux services de renseignement du premier cercle, de sa propre initiative ou à la demande de ces services, des éléments figurant dans ces procédures nécessaires à l'exercice de leurs missions. Si la procédure fait l'objet d'une information, cette communication ne peut intervenir qu'avec l'avis favorable du juge d'instruction. Cette communication peut être réalisée selon les mêmes modalités et pour les mêmes finalités à destination des services compétents pour la prévention du terrorisme (premier et deuxième cercles) par tout procureur pour des procédures ouvertes pour un crime ou un délit puni d'une peine d'emprisonnement révélant des comportements en lien avec la menace terroriste.

Le projet transpose cette possibilité de transmission d'informations par le procureur de la République de Paris à celles recueillies dans le cadre de procédures ouvertes en matière de cybercriminalité (art. 706-72-1 du CPP) et d'affaires de criminalité organisée d'une très grande complexité (art. 706-75, 4ème alinéa, du CPP). Dans le premier cas cette transmission s'opère au bénéfice des services de l'Etat mentionnés à l'article L. 2321-2 du code de la défense (services désignés par l'arrêté du 17 juillet 2015 du Premier ministre, pour participer à la caractérisation de l'attaque et prendre les mesures nécessaires de lutte à son encontre) et, dans le second, au bénéfice des services de renseignement.

Le secret de l'enquête et de l'instruction est une garantie donnée aux citoyens pour assurer à la fois la préservation de l'ordre public en permettant la recherche des auteurs d'infractions, mais aussi une garantie du respect de la présomption d'innocence et de la protection de la vie privée (Conseil constitutionnel, Décision n° 2017-693 QPC du 2 mars 2018). Il ne peut subir de restriction que si celle-ci est justifiée par un intérêt général et proportionnée à celui-ci.

29. L'extension de la transmission d'informations aux affaires de cybercriminalité n'appelle pas d'objection du Conseil d'Etat. Dans la mesure où il est le plus souvent très difficile d'appréhender les auteurs de tels faits, et que l'essentiel de la réponse à ces agissements passe par des actions conduites par les services spécialisés pour mettre fin à cette criminalité, cette transmission aux seuls services chargés par le Premier ministre, en application du code de la défense, de lutter contre les atteintes aux systèmes d'information, constitue une dérogation au secret de l'enquête et de l'instruction légitime au regard de son objectif et proportionnée à celui-ci quant à son champ et quant au destinataire de l'information.

30. Sur l'extension à la criminalité et la délinquance organisées de grande complexité, le Conseil d'Etat considère que si la lutte contre ces formes spécifiques de criminalité et de délinquance a déjà été reconnue dans ses particularités par la jurisprudence constitutionnelle comme justifiant de dérogations procédurales (Décision n° 2019-778 DC du 21 mars 2019, loi de programmation de la justice, qui n'admettait l'extension de techniques spéciales de renseignement qu'à la criminalité organisée, et non à toutes formes de délinquance), le champ des informations transmises doit être limité à certaines finalités et certains services pour limiter l'atteinte portée au secret de l'enquête, à la protection de la vie privée et à la

présomption d'innocence. Il propose en conséquence de réduire la liste des infractions concernées à la lutte contre le trafic de stupéfiants, contre la traite des êtres humains et contre les filières d'immigration clandestines et les délits en matière d'armes. Il propose également de préciser que seuls les services du deuxième cercle des services de renseignement dont la liste aura été fixée par un décret en Conseil d'Etat pourront être destinataires de ces informations.

Au bénéfice de ces aménagements, le texte n'appelle pas d'objection.

Autres dispositions

Sur les dispositions de prorogation pour sept jours des mesures individuelles de contrôle et de surveillance (MICAS) expirant le 31 juillet 2021

31. Les dispositions régissant les MICAS des article L. 228-1 et suivants du CSI cesseront d'être en vigueur le 31 juillet 2021, en application du II de l'article 5 de la loi du 30 octobre 2017. Le projet de loi examiné par le Conseil d'Etat le 21 avril 2021 (Avis n° 402562) pérennise ces mesures. Le renouvellement éventuel de MICAS en cours, s'il sera ainsi légalement possible au-delà de la date du 31 juillet, nécessite cependant que soit aménagé un délai pour le cas où le projet de loi pérennisant le dispositif ne serait pas adopté suffisamment à temps avant le 31 juillet 2021 et aboutirait à l'expiration de la mesure en cours sans que son renouvellement ait pu prendre sa suite. Pour éviter cette situation qui conduirait à l'interruption des mesures de contrôle et de surveillance, le projet de loi prévoit une prolongation automatique de sept jours des mesures qui viendraient à échéance le 31 juillet. Dans la rédaction qu'il adopte, le Conseil d'État précise le texte en indiquant d'une part que cette prolongation par la loi ne peut s'appliquer que dans l'hypothèse où la procédure de renouvellement a fait l'objet d'une notification au plus tard le lendemain de la publication de la loi et qu'elle ne s'applique qu'à compter du terme de la mesure initiale.

Au bénéfice de ces modifications, le Conseil d'État admet la nécessité de cette mesure. Il attire toutefois l'attention du Gouvernement sur le fait que si la loi devait être publiée au-delà du 31 juillet, une inévitable solution de continuité en résulterait avant tout renouvellement de MICAS, risquant ainsi de préjudicier gravement à la défense des intérêts que ces mesures ont vocation à préserver.

Sur les dispositions relatives aux archives

32. L'article L. 213-1 du code du patrimoine, dans sa rédaction issue de l'article 17 de la loi n° 2008-696 du 15 juillet 2008 relative aux archives, prévoit la communicabilité de plein droit des archives publiques sous réserve des délais prévus à l'article L. 213-2. Ce dernier article dispose que sont communicables de plein droit à l'expiration d'un délai de « (…) *3° cinquante ans à compter de la date du document ou du document le plus récent inclus dans le dossier (…) les documents dont la communication porte atteinte au secret de la défense nationale, aux intérêts fondamentaux de l'Etat dans la conduite de la politique extérieure, à la sûreté de l'Etat, à la sécurité publique (…)* ». Ces dispositions doivent être rapprochées de celles de l'article 413-9 du code pénal selon lequel « *Présentent un caractère de secret de la défense nationale (…) les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de classification destinées à restreindre leur diffusion ou leur accès* ». Estimant nécessaire l'articulation des dispositions de ces deux codes, une instruction interministérielle de 2011, révisée en 2020, a prévu de mettre en place une procédure

systématique de déclassification des documents revêtant la nature d'archives publiques au sens du code du patrimoine, dès lors que leur communication était demandée après le délai de cinquante ans. Cette procédure a, au plan matériel, conduit à des lenteurs dans les délais de communication.

33. Afin de lever les ambiguïtés ou les difficultés d'application qui auraient pu résulter de l'article L. 213-2 du code du patrimoine, le projet de loi prévoit que toute mesure de classification mentionnée à l'article 413-9 du code pénal prend automatiquement fin à la date à laquelle le document qui en fait l'objet devient communicable de plein droit.

Pour éviter toutefois que le caractère automatique de cette communicabilité ne porte atteinte aux intérêts fondamentaux de la Nation, le projet énumère quatre catégories de documents pour lesquels, par dérogation, la communication n'est possible qu'à l'expiration d'un terme plus éloigné que le délai de cinquante ans, que les documents concernés aient ou non fait l'objet d'une mesure de classification. Ces dérogations visent les documents relatifs :

- à un nombre restreint d'infrastructures, militaires ou civiles, dont la diffusion des plans, tant qu'elles sont en service, affecterait significativement la sécurité nationale. Dans ce cas, les documents ne sont pas communicables jusqu'au terme de leur affectation à l'usage justifiant de cette protection. La communication peut être refusée pour des documents concernant des installations de « *caractéristiques semblables* » ;

- aux plans opérationnels et à la conception technique et aux procédures d'emploi des matériels de guerre et matériels assimilés, susceptibles d'être exportés avec une autorisation préalable, selon la procédure définie à l'article L. 2335-2 du code de la défense, et figurant sur une liste arrêtée par le ministre de la défense, jusqu'à la fin de leur emploi par les formations armées et les formations rattachées ;

- aux procédures opérationnelles et aux capacités techniques des services de renseignement, jusqu'à la date de la perte de leur valeur opérationnelle ;

- à l'organisation, la mise en œuvre et la protection des moyens de la dissuasion nucléaire, jusqu'à la perte de leur valeur opérationnelle.

En outre, la protection particulière des documents nominatifs est désormais restreinte à ceux concernant les seuls agents des services de renseignement.

34. Le Conseil d'Etat rappelle que le droit d'accès aux documents d'archives publiques est une des garanties mettant en œuvre les exigences constitutionnelles issues de l'article 15 de la Déclaration des droits de l'homme et du citoyen de 1789. Si des limitations liées à des exigences constitutionnelles ou justifiées par l'intérêt général peuvent y être apportées, c'est à la condition qu'il n'en résulte pas d'atteintes disproportionnées au regard de l'objectif poursuivi (Conseil constitutionnel, Décision n° 2017-655 QPC du 15 septembre 2017). Le secret de la défense nationale participe de la sauvegarde des intérêts fondamentaux de la Nation, au nombre desquels figurent l'indépendance de la Nation et l'intégrité du territoire mentionnées à l'article 5 de la Constitution (Conseil constitutionnel, Décision n° 2011-192 QPC du 10 novembre 2011).

Le Conseil d'Etat constate que le projet de loi recherche une logique renouvelée ou précisée de l'accès aux archives publiques en organisant, sauf exceptions, un système de droit d'accès au-delà de cinquante ans des documents couverts par le secret de la défense nationale

par perte automatique de la classification. Cette explicitation est de nature à remédier aux difficultés de communication nées de la situation actuelle.

35. Il relève ensuite que les limitations apportées par le projet à la communicabilité de plein droit au-delà de cinquante ans, sont justifiées par la nature des intérêts fondamentaux à protéger, qu'il s'agisse de la souveraineté nationale, de la défense ou de la sécurité nationale.

Dans la liste des limitations, le Conseil d'État rappelle que le degré de précision du champ et des modalités des exceptions apportées doit être d'autant plus grand que, outre les exigences constitutionnelles ci-dessus rappelées, il incombe à la loi d'assurer la mise en œuvre du principe de légalité des délits et des peines, puisque la méconnaissance des dispositions en cause est pénalement sanctionnée. Dans ce cadre, il propose donc plusieurs aménagements afin de restreindre la communication différée des archives à ce qui est strictement nécessaire à la protection de ces intérêts fondamentaux. A cet effet :

- il précise que la fin de l'affectation des infrastructures concernées doit être constatée par un acte publié, qui, s'il n'existe pas déjà pour certaines d'entre elles, devra être prévu par un acte réglementaire à intervenir ;

- il ne retient pas d'exception au-delà de 50 ans pour les plans opérationnels des armées, dont il estime que, s'ils n'ont fait l'objet d'une actualisation permettant la computation d'un nouveau délai, il ne peut sérieusement être soutenu que leur communication porterait atteinte aux intérêts de la défense nationale. Cette actualisation peut résulter du simple examen régulier de la valeur opérationnelle des documents concernés. Il ajoute que la liste des matériels de guerre soumis à une autorisation d'exportation non communicables avant la fin de leur emploi fait l'objet d'une actualisation annuelle par arrêté publié du ministre de la défense ;

- il précise que la dérogation relative aux documents se rapportant aux procédures opérationnelles et aux capacités techniques des services de renseignement est limitée à ceux concernant les services du premier cercle et certains de ceux du second cercle désignés par décret en Conseil d'Etat.

Le Conseil d'Etat estime que le projet opère dans ces conditions une conciliation équilibrée entre le droit d'accès aux documents d'archives publiques et la protection des intérêts fondamentaux de la Nation.

Ces dispositions entreront en vigueur dès la publication de la loi. Alors même qu'avant son intervention des documents auraient pu être communicables au titre des anciennes dispositions, il est loisible au législateur de modifier pour l'avenir le régime de communicabilité pourvu que ce soit, comme le Conseil d'Etat l'estime ici, dans le respect des exigences constitutionnelles.

36. Par une saisine rectificative, le texte prévoit de ne pas appliquer le nouveau régime aux archives non classifiées qui seraient devenues communicables avant l'intervention de ces nouvelles dispositions. Le Conseil d'Etat prend acte de ce choix qui, au terme du très bref délai d'examen dont il a disposé, n'appelle pas d'objection de nature juridique.

Cet avis a été délibéré par l'assemblée générale du Conseil d'Etat dans sa séance du jeudi 6 mai 2021.