Délibération n° 2021-040 du 8 avril 2021 portant avis sur un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement

(demande d'avis n° 21005550)

La Commission nationale de l'informatique et des libertés,

Saisie par le ministère de l'Intérieur d'une demande d'avis concernant un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8 ;

Après avoir entendu le rapport de Mme Sophie LAMBREMON, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

Emet l'avis suivant

1. La loi n° 2015-912 du 24 juillet 2015 a eu pour objet d'établir le cadre juridique applicable aux activités des services de renseignement en déterminant notamment les principes et les finalités de la politique publique en la matière, le régime juridique applicable aux techniques de renseignement ainsi que les différentes garanties qui permettent, effectivement, d'y recourir. La CNIL est saisie d'un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement. Le présent avis ne se prononce pas sur les articles 13 bis et 13 ter du projet de loi, introduits par une saisine rectificative sur laquelle la Commission se prononcera ultérieurement.

2. La préservation d'un strict équilibre entre la sécurité publique, la protection des intérêts fondamentaux de la Nation et le respect de la vie privée a conduit, par la loi de 2015, à confier le contrôle des différentes techniques de renseignement à une autorité administrative indépendante spécialisée (la Commission nationale de contrôle des techniques de renseignement ou CNCTR) ainsi qu'à une juridiction administrative spécialisée relevant du contrôle en cassation du Conseil d'Etat.

3. Les évolutions envisagées par le projet de loi visent principalement à pérenniser et élargir les instruments de prévention de la commission d'actes de terrorisme et à modifier, par ailleurs, certaines dispositions relatives au renseignement introduites notamment par la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (loi « SILT »). En particulier, il s'agit d'étendre la nature des données pouvant être collectées dans le cadre de l'accès aux données de connexion, ainsi que la possibilité de transmission d'informations relatives à une personne faisant l'objet d'une hospitalisation sans consentement, notamment aux services de renseignement, ou encore de permettre aux services de renseignement d'exploiter des données collectées *via* des techniques de renseignement pour d'autres finalités que

celles ayant justifié leur recueil, et de transmettre ces informations à d'autres services ayant des missions de renseignement.

4. Compte tenu des enjeux associés à la mise en œuvre de certains moyens considérés comme particulièrement intrusifs et permettant de recueillir un volume très important de données, la Commission estime indispensable de s'assurer que les atteintes portées au respect de la vie privée soient limitées au strict nécessaire. Elle rappelle que ces atteintes doivent être adéquates et proportionnées au but poursuivi et que des garanties suffisantes doivent être mises en œuvre. A cet égard, la Commission observe que plusieurs des garanties introduites par la loi du 24 juillet 2015 précitée sont reprises par le présent projet de loi, tel que le formalisme strict attaché à la mise en œuvre de ces techniques.

5. La Commission relève que certaines dispositions du projet de loi ont vocation à encadrer les principes régissant la collecte de données à caractère personnel, et concernent dès lors, et pour les dispositions qui s'y rapportent, la protection des données. C'est à ce titre que la Commission a été saisie, sur le fondement de l'article 8- 4°-a) de la loi du 6 janvier 1978, du présent projet de loi.

6. La Commission rappelle que le projet de loi encadre les modalités de collecte des différentes techniques de renseignements prévues par le texte. Les données doivent ensuite être traitées, au sein de différents fichiers mis en œuvre par les services concernés, dans le respect du droit à la protection des données à caractère personnel notamment du titre IV de la loi « Informatique et libertés ». Cependant, la Commission rappelle que la plupart d'entre eux (énumérés au sein du décret n° 2007-914 du 15 mai 2007) bénéficient d'un régime dérogatoire, lequel permet de les exclure du champ de contrôle *a posteriori* de la Commission, conformément à l'article 19-IV de la loi du 6 janvier 1978 modifiée.

7. Au regard des évolutions projetées, tant en matière de données collectées que d'exploitation et de transmission de ces informations, la Commission rappelle, ainsi qu'elle l'a fait par le passé, qu'elle demande à pouvoir exercer ses pouvoirs de contrôle sur ces traitements. Si elle relève que tant la CNCTR (par son avis sur la mise en œuvre des techniques, ainsi que son contrôle de l'exécution des autorisations accordées par le Premier ministre) que le groupement interministériel de contrôle (GIC) disposent de prérogatives visant notamment à assurer la légalité des pratiques mises en œuvre, la Commission estime que son contrôle, qui porterait sur les conditions de mise en œuvre globales desdits fichiers et devrait être assorti de garanties adaptées à leur nature particulière, devrait compléter ceux déjà réalisés par ces deux entités et constituerait une garantie supplémentaire.

8. Enfin, la Commission relève que la Cour de justice de l'Union européenne s'est prononcée le 6 octobre 2020 (Privacy international (aff. C-623/17), et La Quadrature du Net, French Data Network, Ordre des barreaux francophones et germanophone (aff. jointes C-511/18, C-512/18, C-520-18)), dans le cadre d'une question préjudicielle, sur la conformité de certaines des dispositions visées par le projet de loi. Si elle n'entend pas apprécier, dans son avis, la régularité des dispositions déjà en vigueur et non modifiées par le projet au regard du droit de l'Union européenne, pour lesquelles le Gouvernement a indiqué attendre l'issue des contentieux en cours, la Commission rappelle néanmoins que le juge européen s'est prononcé sur les conditions de licéité de mise en œuvre des techniques de renseignement de recueil en temps réel et d'analyse

automatisée des données de trafic et des données techniques relatives à la localisation des équipements. Or plusieurs dispositions du projet de loi examiné sont relatives à ces techniques. Le juge européen a admis le recours à ces méthodes pour l'objectif de lutte contre le terrorisme. Les garanties exigées par le juge européen ont notamment trait à l'existence d'une « *menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible* » et qui justifie la surveillance, et à l'existence d'un contrôle effectif du traitement algorithmique de criblage, soit par une juridiction, soit par une entité administrative indépendante dont la décision est dotée d'un effet contraignant. A cet égard, la Commission relève que la législation française a institué une autorité administrative indépendante, la CNCTR, qui est saisie pour avis de toute autorisation de mise en œuvre de ces techniques de renseignement, dispose de pouvoirs de contrôle sur leur mise en œuvre, peut adresser au Premier ministre toute recommandation jugée nécessaire et peut saisir, lorsque ses avis ou recommandations ne sont pas suivis d'effet, une juridiction spécialisée dont la décision s'impose aux services de renseignement.

9. En revanche, si l'article L. 801-1 du code de la sécurité intérieure prévoit que l'autorisation de ces techniques doit être justifiée « *par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation* », la Commission recommande que la rédaction du projet de loi explicite qu'il rentre dans l'office de la CNCTR de vérifier l'existence de cette menace de nature terroriste. Un tel contrôle, rappelle la CJUE, doit en effet être réalisé lors de la décision de procéder au traitement d'analyse automatisée de données de connexion, ou lors du renouvellement de son autorisation. La Commission relève que, s'agissant du recueil en temps réel des données de connexion de certaines personnes, la Cour a exigé qu'elle soit limitée aux « *personnes pour lesquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme* », ce qu'il conviendrait de préciser. Enfin, la Cour a également insisté sur la nécessité d'apporter sur ces mesures une information appropriée, générale et parfois individuelle, sans nuire à leur efficacité. La loi ou les dispositions réglementaires devront intégrer ces exigences.

10. Compte tenu des fortes incidences que pourraient avoir les choix du Parlement sur la mise en œuvre de certaines techniques de renseignement, la Commission rappelle qu'elle se montrera particulièrement vigilante quant aux évolutions qui pourraient être apportées aux dispositifs en question (et notamment les mesures de nécessité et de proportionnalité qui s'imposeront en toute hypothèse). Elle souligne en tout état de cause qu'elle devra être consultée sur les aspects relevant de sa compétence.

Sur la pérennisation de la technique de renseignement visée à l'article L. 851-3 du code de la sécurité intérieure, dite de « l'algorithme » (articles 1, 7 et 8 du projet de loi)

11. L'article L. 851-3 du code de la sécurité intérieure (CSI) dans sa rédaction issue de la loi de 2015 précitée prévoit la possibilité de mettre en œuvre sur les réseaux de communication électroniques des opérateurs et de certaines autres personnes morales, des traitements automatisés destinés à détecter au moyen d'un « algorithme », des connexions susceptibles de révéler une menace terroriste.

12. A titre liminaire, la Commission relève la différence entre les caractéristiques du premier traitement mis en œuvre en 2017, qui portait uniquement sur la téléphonie, et celles de ceux envisagés en application du même texte qui, en raison de l'évolution des pratiques en la matière ainsi que du type d'informations concernées, soulèvent des enjeux particuliers.

13. Elle relève à cet égard que l'article L. 851-3 du CSI encadre aussi bien le traitement des données de téléphonie que celles issues des connexions sur Internet. A cet égard, la Commission souligne que l'expérimentation dont il est envisagé la pérennisation porte sur ces deux types de données, de manière indifférenciée et ce, alors même que sa mise en œuvre n'a jusqu'à présent porté que sur les données de téléphonie. Elle estime que l'atteinte portée à la vie privée par le criblage algorithmique des données de connexion sur internet est cependant plus forte que celui de données de connexion téléphonique et que le contrôle de proportionnalité doit être différencié.

En ce qui concerne les modalités de mise en œuvre de cette technique

14. L'article 8 du projet de loi prévoit que ces algorithmes « *peuvent être autorisés, à la demande des services spécialisés de renseignement mentionnés à l'article L. 811- 2, sur les données transitant par les réseaux des opérateurs et des personnes mentionnées à l'article L. 851-1* (…) ». Il précise en outre que, « *un service du Premier ministre est seul habilité à exécuter les traitements et opérations mis en œuvre sur le fondement du I et du IV, sous le contrôle de la Commission nationale de contrôle des techniques de renseignement* ».

15. Le ministère a précisé que la modalité initialement envisagée pour mettre en œuvre cette technique, consistait à placer physiquement les dispositifs de détection en plusieurs points des réseaux des opérateurs. La Commission relève que cette modalité correspondait à l'interprétation la plus naturelle de l'article L. 851-3 du CSI, issu de la loi de 2015 et aurait constitué une forme de garantie technique apportée au dispositif.

16. Le ministère a néanmoins indiqué que placer physiquement les dispositifs de détection en plusieurs points des réseaux des opérateurs présente des difficultés techniques, tant en matière de sécurité des réseaux des opérateurs, que de détection d'évènements communs à plusieurs dispositifs installés sur ces réseaux. En outre, certains des paramètres de détection revêtant une sensibilité particulière, ils ne peuvent être rendus accessibles ou divulgués lors de l'exécution de l'algorithme par les opérateurs. En conséquence, le ministère a retenu une architecture selon laquelle les flux de données ne sont pas analysés au moyen d'algorithmes installés sur les réseaux des opérateurs mais dupliqués puis acheminés au sein d'une infrastructure dépendant de l'Etat pour être soumis à des dispositifs de détection centralisés. La CNCTR a donné son accord à ces modalités techniques, qu'elle a estimées conformes à la loi autorisant l'expérimentation, en exigeant certaines garanties, notamment le fait que l'algorithme soit mis en œuvre par le GIC et non par les services de renseignement.

17. S'agissant de ces modalités, la Commission formule, en l'état des informations mises à sa disposition, les observations suivantes.

18. La Commission considère que les modifications apportées par le projet de loi à l'article L. 851-3 du CSI ne permettent pas d'appréhender de manière claire et précise les évolutions envisagées et ainsi la manière dont cette technique de renseignement sera mise en œuvre. Elle estime indispensable que le texte soit précisé. Elle considère notamment que le fait que la mise en œuvre de l'algorithme implique de dupliquer, au bénéfice d'un service administratif du Premier ministre, l'ensemble de ces données, qui concernent tous les appels téléphoniques et accès internet réalisés sur le territoire français, constitue une évolution particulièrement significative. La centralisation et la duplication modifient la portée de l'atteinte à la vie privée, par les risques qu'elles portent en elle-même. Le principe même de cette architecture technique devrait donc, à ses yeux, figurer dans la loi.

19. La Commission considère, *a fortiori*, que des garanties spécifiques, prévues par les textes, doivent nécessairement entourer la mise en œuvre d'une telle architecture technique. Ces garanties doivent permettre que la mise à disposition du GIC de l'ensemble de ces données, en dehors de toute mesure de surveillance ciblée, ne puisse s'analyser en une forme de recueil en temps réel des données de connexion, qui serait prohibée par la jurisprudence européenne. A cet égard, si les données de connexion elles-mêmes ne sont pas mises à disposition des services de renseignement et ne peuvent, sous le contrôle de la CNCTR, être utilisées par le GIC que pour la mise en œuvre de l'algorithme, la Commission estime qu'il est également nécessaire que les données ne soient conservées que le temps strictement nécessaire à leur analyse, puis immédiatement détruites, et que le GIC ne garde que le strict minimum nécessaire au fonctionnement de l'algorithme sur la période d'analyse considérée. A cet égard, elle prend acte des précisions apportées par le ministère selon lesquelles ces données sont conservées sous forme pseudonyme pour une durée de vingt-quatre heures (sauf dans l'hypothèse d'un hit), avant d'être détruites. Cette précision devrait expressément figurer dans le projet de loi, qui devrait également préciser les modalités de recueil et d'accès à ces données.

En ce qui concerne le recours à un algorithme

20. Le recours à cette technique de renseignement très particulière, selon les modalités décrites ci-dessus, ne saurait être admise que s'il est nécessaire et proportionné à l'objectif de lutte contre le terrorisme.

21. D'une part, la Commission relève que la mise en œuvre de ce type de dispositifs doit permettre de doter les services de renseignement de moyens d'action adéquats face aux menaces persistantes qui pèsent sur les intérêts fondamentaux de la Nation et, plus particulièrement, permettre la détection de manière précoce de menaces terroristes. Le Gouvernement estime que cette nouvelle technique de renseignement est rendue nécessaire par l'évolution de la menace terroriste, qui proviendrait d'individus n'appartenant pas à des groupes ou organisations structurées et identifiables, dont la radicalisation et le passage à l'acte sont mal appréhendés par les techniques de renseignement ciblées.

22. Le Gouvernement a par ailleurs souligné que ces traitements algorithmiques sont utilisés pour repérer des personnes dont les services de renseignement déterminent ensuite, sous le contrôle de la CNCTR, s'il est nécessaire de les soumettre à une mesure de surveillance ciblée en cas de suspicion de menace terroriste. Cet équilibre répond à une exigence de la CJUE qui demande que l'utilisation de l'algorithme ne conduise pas à une décision automatisée de surveillance ciblée. Le traitement de l'ensemble des données de connexion auprès des acteurs concernés permet de détecter les individus dont la radicalisation serait repérable par leur activité numérique, au moyen notamment d'un mécanisme de hit/no hit, afin dans un second temps de de déclencher une surveillance ciblée.

23. Enfin, la mise en œuvre de cette technique est entourée d'une série de garanties et de contrôle, consistant notamment à subordonner la mise en œuvre d'une telle technique à une autorisation du Premier ministre après avis de la CNCTR, celle-ci disposant d'un pouvoir de recommandation et de saisine d'une juridiction spécialisée dont les décisions sont contraignantes. En outre, le Gouvernement prévoit dans le projet de loi que cette technique ne pourra plus être exercée directement par les services de renseignement mais par un service distinct du Premier ministre (le GIC), sous le contrôle de la CNCTR. Le projet de loi propose également de supprimer la possibilité de proroger la durée de conservation des données issues de cette technique.

24. D'autre part, la Commission ne peut que rappeler que l'utilisation d'une telle technique porte une atteinte particulièrement forte à la vie privée des individus et au droit à la protection des données à caractère personnel, garantis notamment par la Constitution et la charte des droits fondamentaux de l'Union européenne, puisqu'elle ne présente pas de caractère ciblé mais procède de l'analyse de l'ensemble des données de connexion de la population. La mise en œuvre d'une surveillance poussée de l'intégralité des données de connexion pourrait, à elle seule, entraîner des effets dissuasifs sur l'exercice de leur liberté d'information et d'expression par les utilisateurs d'Internet et des réseaux de communications électroniques. En outre les modalités particulières de mise en œuvre de ces algorithmes accentuent l'atteinte portée au respect de la vie privée des personnes et à la protection de leurs données personnelles.

25. S'agissant des informations pouvant être exploitées en application de cet article, la Commission rappelle que les traitements mis en œuvre au moyen de traitements algorithmiques consistant à analyser les données de connexion et de localisation constituent des traitements de données à caractère personnel. Dans la décision précitée de la CJUE, il a été rappelé que les informations visées (données relatives au trafic et de localisation) fournissent les moyens d'établir le profil des personnes concernées en ce qu'elles concernent « *un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles (…)* ». A cet égard, la Commission estime que la formulation de l'article L. 851-3 du CSI, qui mentionne que les données concernées sont recueillies « *sans permettre l'identification des personnes auxquelles les informations se rapportent* », devrait être modifié dans la mesure où ces données sont susceptibles de permettre l'identification des personnes.

26. La Commission observe en particulier que cette technique de repérage automatique est susceptible d'entraîner le recueil et l'analyse de données de connexion de toute personne, y compris celles dont les communications sont soumises, selon les règles nationales, au secret professionnel.

27. Enfin, la Commission rappelle le risque lié à l'inclusion de biais dans les algorithmes déployés, lors de la conception ou de l'entraînement des modèles, qui peut conduire à des faux positifs ou à des faux négatifs nuisant notamment à l'efficacité opérationnelle du dispositif et entraîner des conséquences dommageables pour les personnes concernées. La Commission estime que le ministère devrait initier des travaux sur le sujet et rappelle la nécessité de se montrer particulièrement vigilant dans le cadre de ces différentes phases d'élaboration des modèles algorithmiques.

28. La Commission prend d'ailleurs acte des précisions du ministère qui a indiqué que les algorithmes reposent en principe sur des modèles générant les signaux de « hit »/ « no hit » à partir de « sélecteurs » stricts, provenant souvent des méthodes traditionnelles de renseignement. Cette solution contribue non seulement à l'efficacité opérationnelle de la mesure de renseignement mais constitue aussi une solution plus protectrice de la vie privée et contribuant à assurer la proportionnalité du dispositif. Elle encourage donc le ministère à se construire une doctrine d'usage qui favorise ce type d'algorithme.

29. En conséquence de ce qui précède, la Commission estime que l'introduction de telles techniques de surveillance dans le droit français ne peut être justifiée qu'à des conditions très strictes. Elle relève que le projet de loi maintient la limitation de cette technique au seul objectif de détection des menaces terroristes. Il était nécessaire de procéder par expérimentation, comme l'a fait la loi de 2015, et la pérennisation de cette technique n'est envisageable que si, d'une part, la protection de la population contre les menaces terroristes ne peut être assurée de façon satisfaisante par les moyens traditionnels de surveillance ciblée, ce qu'il appartient au Gouvernement d'établir, et si d'autre part, cette technique est assortie des garanties suffisantes pour en limiter l'usage au strict nécessaire et assurer que les abus soient repérés et sanctionnés.

En ce qui concerne le principe de la pérennisation

30. L'article 1er du projet de loi prévoit de pérenniser la mise en œuvre de la technique de renseignement dite de « l'algorithme », jusqu'alors expérimentale et arrivant à échéance au 31 décembre 2021. Les garanties apportées sont principalement celles précédemment présentées.

31. Afin de pouvoir se prononcer sur la pérennisation, il est nécessaire d'évaluer précisément les bénéfices retirés de ce dispositif durant les années d'expérimentation, pour les comparer à l'atteinte à la vie privée que représente cette forme de surveillance très particulière. A cet égard, la loi prévoit que le Gouvernement remet au Parlement un rapport sur l'application de cette disposition au plus tard le 30 juin 2021. La Commission a pris connaissance d'un bilan général de l'expérimentation mais estime que le ministère ne lui a pas transmis d'éléments suffisamment précis lui permettant d'apprécier l'efficacité opérationnelle et l'efficience de cette technique (tel qu'un bilan comprenant des éléments quantitatifs sur le nombre de cas identifiés, de faux positifs,

de levée de pseudonymat, de durée d'utilisation des ces algorithmes, etc.). Il a été indiqué que des éléments protégés par le secret de la défense nationale seraient fournis à d'autres autorités, notamment la délégation parlementaire au renseignement. Dans ces conditions elle estime ne pas être en mesure d'évaluer les bénéfices de cette technique de renseignement et, par voie de conséquence, d'apprécier la proportionnalité de l'atteinte qu'elle porte au respect de la vie privée.

Sur la collecte de données relatives aux « adresses complètes de ressources sur Internet » (articles 8 et 9 du projet de loi)

32. Les articles 8 et 9 du projet de loi prévoient d'ajouter aux informations pouvant faire l'objet d'un recueil et d'une surveillance automatisés les « *adresses complètes de ressources sur Internet* ». Cette modification intervient pour les deux techniques de recueil administratif de données que sont le recueil de données en temps réel et le recueil au moyen d'un traitement algorithmique (prévus respectivement aux articles L. 851-2 et L. 851-3 du CSI).

33. **A titre liminaire**, la Commission estime que la notion d'« *adresses complètes de ressources sur Internet* », ajoutée aux articles L. 851-2 et L. 851-3 du CSI n'est pas strictement identique à la notion « d'URL », souvent utilisée dans les documents transmis par le ministère dans le cadre de l'instruction de la demande d'avis. En effet, si le mécanisme des URL peut servir à désigner des ressources stockées sur un serveur, de nombreux services l'utilisent également pour transmettre des informations à un serveur ou pour conserver des éléments relatifs à la session en cours. C'est par exemple le cas des paramètres des requêtes « *query strings* » et des informations des formulaires HTML remplis par les usagers, ces données étant agrégées à la fin des URL et transmises avec elles. Elle invite donc le gouvernement à s'interroger sur le périmètre précis qu'il entend définir et à affiner la formule. Si l'expérimentation devait concerner toutes les URL, une formule du type « « adresse de ressource sur internet et paramètres associés à cette adresse » pourrait être envisagée.

34. Par ailleurs, elle rappelle que s'il est techniquement possible d'identifier le nom de domaine d'une URL consultée par un internaute en obtenant le détail des résolutions DNS qu'il aurait effectuées auprès de son fournisseur d'accès à Internet, il en va autrement du chemin complet de la ressource. En effet, l'URL n'est pas lisible en clair par l'opérateur dès lors que la transmission de données concernée est chiffrée entre le terminal de l'utilisateur et les serveurs concernés (*via* le protocole HTTPS par exemple, qui est utilisé aujourd'hui pour la quasi-totalité des connexions sur le web). La Commission prend acte que la collecte auprès des opérateurs vise uniquement les URL non chiffrées, le déchiffrement n'étant à ce stade pas envisagé par les services de renseignement.

35. **S'agissant de l'admissibilité de l'extension** de ces deux techniques de renseignements aux URL, la Commission rappelle que ces données ont une nature particulière. Comme souligné par le Comité européen de la protection des données (CEPD), les URL sont susceptibles de faire apparaître des informations relatives au contenu des éléments consultés ou aux correspondances échangées. La Commission rappelle que la protection particulière dont bénéficient les données de contenu ainsi

que les correspondances représente une garantie essentielle pour assurer le respect de la vie privée et des autres libertés afférentes.

36. Le Conseil constitutionnel a, dans sa décision n°2015-713 DC du 23 juillet 2015 concernant la loi relative au renseignement, relevé (pt 55), au titre des garanties appliquées aux méthodes de recueil ou de traitement en cause, l'impossibilité de recueil de données portant sur « *le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications* ». C'est notamment au regard de cette garantie et, conformément à l'analyse du Gouvernement, qui avait alors précisé que le dispositif des algorithmes ne porterait que sur des données de connexion (ou méta données) et non sur le contenu des communications, qu'il a déclaré conformes les techniques de renseignement précitées.

37. De manière générale, la Commission, qui ne remet pas en cause l'utilité, notamment opérationnelle, que représenterait la possibilité d'étendre la nature des données actuellement collectées, dans un contexte au sein duquel les techniques de communication comme la menace terroriste évoluent fortement, estime qu'il ne lui est pas possible de se prononcer sur la proportionnalité d'une telle atteinte *ex ante*. Elle estime donc que, comme pour le principe de la technique de surveillance par traitement algorithmique, le législateur devrait dans un premier temps, et y compris s'il choisissait de pérenniser la technique de renseignement algorithmique, passer à nouveau, sur ce point, par une expérimentation avant de l'étendre définitivement à ces nouvelles catégories de de données. Cette expérimentation pourrait permettre, plus généralement, d'évaluer finement l'utilité de cette technique de renseignement pour toutes les données de connexion liées à l'usage d'internet puisque, selon la compréhension de la Commission, les seuls algorithmes utilisés jusqu'ici l'ont été pour des données de connexion téléphoniques.

Sur la conservation de données à des fins de recherche et de développements des techniques de renseignement (article 11 du projet de loi)

38. L'article 11 du projet de loi envisage de compléter l'article L. 822-2 du CSI afin de prévoir une conservation ainsi qu'une réutilisation des données collectés par le biais des techniques de renseignement aux seules fins de recherche et développement en matière de renseignement. La conservation à cette fin ne peut excéder cinq années après le recueil des données.

39. La Commission, qui se prononce pour la première fois sur une telle disposition, prend acte de ce que la mise en œuvre d'un tel dispositif n'a pas vocation à permettre d'assurer le suivi et/ou l'identification de personnes, au même titre que les techniques de renseignement, mais à exploiter ces données à des fins de recherche, pour permettre le développement et l'amélioration des capacités de techniques de recueil et d'exploitation.

40. Elle souligne que si les finalités de conservation et d'exploitation de ces informations, légitimes, sont bien distinctes de celles ayant justifié leur collecte, il n'en demeure pas moins que le traitement de ces données, et en l'absence de toute mesure permettant l'anonymisation totale de ces informations, constitue un traitement de données à caractère personnel au sens de la réglementation applicable. A cet égard, et

compte tenu des finalités pour lesquelles un tel traitement serait mis en œuvre, la Commission considère, que la loi du 6 janvier 1978 modifiée, et plus particulièrement son titre IV, a vocation à s'appliquer au traitement projeté, sous réserve de dispositions spéciales du CSI y dérogeant. Sur ce dernier point, elle relève en particulier que les programmes de recherches n'auraient pas à être autorisés par des actes réglementaires en application des articles 31 et suivants de la loi du 6 janvier 1978 dès lors que le projet de loi prévoit déjà un mécanisme d'autorisation spécifique.

41. Elle rappelle que, s'agissant de la loi précitée, son article 4-2° prévoit que le traitement ultérieur de données à des fins de recherche est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des dispositions applicables en matière de protection de données.

42. La Commission relève que le ministère, afin d'assurer comme le prévoit le projet de loi, que cette « *conservation est opérée dans la mesure strictement nécessaire à l'acquisition des connaissances suffisantes pour développer, améliorer et valider les capacités techniques de recueil et d'exploitation* » a assorti de garanties la mise en œuvre de ce dispositif. A cet égard, seuls les agents spécialement habilités à cet effet et exclusivement affectés à cette mission pourront accéder aux données, les motifs et finalités pour lesquels les informations ont été collectées ne seront pas conservées, et enfin, il ne sera pas possible de rechercher l'identité d'une personne par l'intermédiaire de ce dispositif. Les paramètres techniques de chaque programme de recherche seront autorisés par le Premier ministre, après avis de la CNCTR, laquelle sera en mesure d'user de ses pouvoirs de contrôle, de recommandation et de saisine du juge.

43. La Commission accueille favorablement la mise en œuvre de ces garanties. Elle estime néanmoins que le régime de réutilisation des données, dans son ensemble, devrait être encadré par un décret d'application et que des garanties complémentaires soient prévues dans l'hypothèse où ce traitement serait mis en œuvre au moyen d'un traitement algorithmique.

44. En effet, les modalités ainsi que les critères pris en compte par le traitement algorithmique devront être clairement définis avant toute mise en œuvre du traitement projeté et une attention particulière devra être portée aux principes cardinaux de vigilance et de loyauté tout au long du développement de ce traitement. D'une part, compte tenu de la particulière sensibilité des informations susceptibles d'être traitées ainsi que du volume de données ayant vocation à être exploité, une attention particulière devra être portée aux évolutions envisagées des traitements algorithmiques et plus particulièrement à la présence d'éventuels biais. Elle appelle également à être vigilant sur le traitement d'éventuelles données sensibles lors de l'entraînement des algorithmes.

Sur la communication d'informations relatives à l'admission d'une personne faisant l'objet d'une mesure d'hospitalisation sans consentement (article 6 du projet de loi)

45. L'article 6 du projet de loi prévoit d'introduire un article L. 3211-12-7 au code de la santé publique afin de permettre la communication d'informations relatives à l'admission d'une personne en soins psychiatriques sans consentement, au représentant de l'Etat dans le département, et à Paris, au préfet de police, ainsi qu'aux services de renseignement mentionnés aux articles L. 811-2 et L. 811-4 du CSI afin

d'assurer le suivi de cette personne qui représente une menace grave pour la sécurité et l'ordre publics à raison de sa radicalisation à caractère terroriste. De telles informations sont aujourd'hui uniquement communiquées au préfet du département d'hospitalisation de la personne concernée.

46. Le ministère entend notamment, par une telle évolution, permettre de pallier l'absence d'information du préfet qui se situe hors du département d'hospitalisation de la personne concernée. Si le principe de la dérogation au secret médical relève de la loi, la Commission rappelle que les conditions de mise en œuvre de cette possibilité devront être strictement encadrées par voie réglementaire, (et notamment les dispositions relatives aux fichiers concernés).

47. A cet égard, le ministère envisage de mettre en œuvre cette possibilité au moyen d'une mise en relation entre le Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) et les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement dénommés « HOPSYWEB ».

48. Dans l'hypothèse où les dispositions introduites par le projet de loi auraient uniquement vocation à permettre une telle possibilité, et ainsi se limiter à la seule mise en relation entre ces deux fichiers, la Commission rappelle les observations formulées dans sa délibération n° 2018-354 du 13 décembre 2018 dans laquelle, sans remettre en cause la légitimité d'une telle transmission, elle s'était fortement interrogée sur les conditions de sa mise en œuvre.

49. Plus particulièrement, et au regard de la sensibilité particulière des informations relatives à une admission en soins psychiatriques couverte par le secret médical et aux risques pour les personnes concernées, elle appelle à un encadrement strict des conditions de mise en œuvre de cette transmission, notamment un renforcement de la sécurisation des procédures de vérification d'identité et de recueil d'informations complémentaires. La Commission rappelle en outre que les informations communiquées devront être strictement nécessaires à l'accomplissement des missions du représentant de l'Etat et des services de renseignement et se limiter à ce qui est prévu aux articles L. 3212-5, L. 3212-8 et L. 3213-9 du code de la santé publique et à l'article 706-135 du code de procédure pénale.

Sur la transmission d'informations couvertes par un secret protégé par la loi aux services de renseignement (article 10 du projet de loi)

50. Les modifications de l'article L. 863-2 du CSI par l'article 10 du projet de loi visent à autoriser les autorités administratives mentionnées à l'article 1er de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, à transmettre aux services de renseignement mentionnés aux articles L. 811-2 et L. 811- 4 du CSI, de leur propre initiative ou sur requête de ces derniers, toute information même couverte par un secret protégé par la loi, « strictement nécessaire » à l'accomplissement des missions de ces services et susceptible de concourir à la défense et la promotion des intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 du même code. Ces dispositions modifient l'actuel article L. 863-2 du CSI qui autorise ces transmissions lorsqu'elles sont seulement « utiles » aux missions de ces services.

51. La Commission prend acte des éléments apportés par le ministère selon lesquels de telles transmissions d'informations peuvent s'avérer indispensables aux services de renseignement pour leur permettre de mener à bien leurs missions et accueille favorablement le resserrement des conditions posées par la loi.

52. Elle s'interroge sur la portée des atteintes aux secrets protégés par la loi, au regard de la nature de certains d'entre eux. Elle estime que le texte ne couvre pas l'hypothèse d'un professionnel médical exerçant dans une structure publique. La Commission rappelle que les conditions de mise en œuvre de telles transmissions devront être précisées et encadrées par voie réglementaire, ainsi que le prévoit déjà l'article L. 863-2 du CSI. Elle insiste tout particulièrement sur la vigilance devant être portée aux transmissions d'informations réalisées à l'initiative des autorités administratives, ainsi qu'aux garanties entourant les dérogations au secret médical. En tout état de cause, la Commission estime que l'article L. 863-2 du CSI devrait être modifié afin de garantir que de telles atteintes ne peuvent être que nécessaires et proportionnées aux intérêts poursuivis.

Sur l'exploitation à d'autres fins, de renseignements collectés *via* des techniques de renseignement, et leur transmission à d'autres services de renseignement (article 10 du projet de loi)

53. L'article 10 du projet de loi prévoit que « *lorsqu'un service spécialisé de renseignement mentionné à l'article L. 811-2 ou un service désigné par le décret en Conseil d'Etat prévu à l'article L. 811-4 obtient, à la suite de la mise en œuvre d'une technique mentionnée au titre V du présent livre, des renseignements utiles à la poursuite d'une finalité différente de celle qui a en a justifié le recueil, il peut les transcrire ou les extraire pour le seul exercice de ses missions* ».

54. Cet article prévoit en outre que, « *sous réserve des dispositions des deuxième à quatrième alinéas du présent II, un service spécialisé de renseignement mentionné à l'article L. 811-2 ou un service désigné par le décret en Conseil d'Etat prévu à l'article L. 811-4 peut transmettre à un autre de ces services les renseignements collectés, extraits ou transcrits dont il dispose, si cette transmission est strictement nécessaire à l'exercice des missions du service destinataire* ».

55. A titre liminaire, la Commission relève que le projet de loi vise à encadrer de manière plus stricte que par l'actuel article L. 863-2 du CSI, les modalités selon lesquelles les données collectées *via* des techniques de renseignement pourront être exploitées et transmises à d'autres services exerçant des missions de renseignement. Elle souligne que des garanties fortes sont par ailleurs prévues par le texte, au titre desquelles figurent une autorisation préalable du Premier ministre après avis de la CNCTR pour certaines de ces transmissions, ainsi que la désignation d'un agent, au sein de chaque service spécialisé de renseignement, chargé de veiller au respect de l'application des dispositions précitées. Ces garanties sont de nature à permettre d'assurer un juste équilibre entre la possibilité d'exploiter ces informations à des fins de renseignement et la protection des données ainsi visées.

56. La Commission rappelle tout d'abord que l'article L. 811-3 du CSI limite les finalités pouvant justifier le recours à l'usage d'une technique de renseignement, et rappelle en outre que l'article 4-2° de la loi du 6 janvier 1978 prévoit que les données à caractère personnel doivent être « *collectées pour des finalités déterminées, explicites et*

légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ».

57. La Commission insiste sur le fait que les renseignements ne pourront être transmis à un autre service que pour l'exécution des missions définies par ses textes constitutifs. Ces missions sont, pour les services de renseignement dits « du premier cercle », limitativement énumérées à l'article L. 811-3 du CSI. Elle souligne qu'il reviendra à la CNCTR de s'assurer, au cas par cas, que l'utilisation ultérieure d'un renseignement obtenu par des techniques particulièrement intrusives, en principe interdites aux administrations, n'est pas disproportionnée au regard de l'utilité que représente le renseignement pour le service destinataire et des objectifs poursuivis. Ce contrôle est particulièrement nécessaire lorsque le renseignement sera transmis à un des services dits « du second cercle », prévus à l'article L. 811-4 du CSI, pour une mission ne relevant pas des finalités listées à l'article L. 811-3 du même code. Elle souhaiterait que le projet de loi mentionne ce contrôle de compatibilité incombant au service transmetteur et à la CNCTR. En outre, si la Commission prend acte de ce que les renseignements transmis aux services de renseignement du second cercle le seront nécessairement au regard de l'une des finalités mentionnées à l'article L. 811-3 du CSI et sous réserve qu'elle corresponde aux missions confiées par voie réglementaire au service destinataire, elle estime que le texte présente une ambiguïté sur ce point et devrait être précisé.

Sur les autres dispositions du projet de loi

58. Indépendamment des observations formulées précédemment, la Commission souligne que le projet de loi introduit des évolutions de nature à avoir un impact sur la réglementation relative à la protection des données à caractère personnel ou qui, à tout le moins, pourraient être analysées au regard des principes fixés par la loi du 6 janvier 1978 modifiée.

59. De manière générale, si la Commission estime que ces différentes modifications n'appellent pas d'observation substantielle, elle relève néanmoins les points suivants.

60. L'article 4 du projet de loi vise à permettre la saisie d'un support informatique présent sur les lieux d'une visite domiciliaire ordonnée aux fins de prévention de la commission d'actes de terrorisme, lorsque celle-ci a révélé des éléments en lien avec la menace et que la personne fait obstacle à l'accès aux données informatiques qu'il contient. La Commission relève que la saisie ainsi que le traitement de ces données seront réalisées dans les mêmes conditions que celles actuellement prévues par l'article L. 229-5 du CSI, ce qui n'appelle pas d'observation.

61. L'article 10 du projet de loi modifie l'article 49 de la loi du 6 janvier 1978 afin de prévoir que le droit d'accès des personnes concernées ne s'applique pas « *s'agissant de l'information suivant laquelle des données à caractère personnel ont été transmises en application du premier alinéa de l'article L. 863-2 du CSI* ». La Commission rappelle que l'article 23 du RGPD susvisé prévoit que le droit de l'Etat membre peut, par voie législative, limiter la portée des droits des personnes concernées, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir notamment la sécurité et la défense nationale.

62. L'article 12 du projet de loi harmonie les durées d'autorisation pour les techniques de recueil et de captation de données informatiques. Ainsi la durée d'autorisation de la technique de recueil des données informatiques est alignée sur celle de la captation. Enfin, l'article 14 modifie l'article L. 213-2 du code du patrimoine pour clarifier le régime de communicabilité des archives classifiées.

La Présidente

Marie-Laure DENIS