Délibération n° 2021-053 du 3 mai 2021 portant avis sur les articles 11 quinquies, 11 sexies et 11 septies du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement

(demande d'avis n° 21008068)

La Commission nationale de l'informatique et des libertés,

Saisie par le ministère de l'intérieur d'une demande d'avis concernant les articles 11 quinquies, 11 sexies et 11 septies d'un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8-4°-a) ;

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 Commission a été saisie en urgence, le 26 avril 2021, sur le fondement de l'article 8-4°-a) de la loi du 6 janvier 1978 modifiée, des articles 11 quinquies, 11 sexies et 11 septies du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement (ci-après « le projet de loi »).

2. Ces articles visent pour l'essentiel à tenir compte de la décision « French Data Network et autres » rendue par le Conseil d'Etat statuant au contentieux le 21 avril 2021 (n°393099, 394922, 397844, 397851, 424717, 424718). La Commission souligne d'emblée que cette décision, qui fait suite à une saisine par le Conseil d'Etat de la Cour de justice de l'Union européenne (CJUE) d'une question préjudicielle, est porteuse d'enjeux significatifs tant en matière de libertés publiques, et notamment de préservation de la vie privée des personnes, que d'effectivité de l'action publique pour garantir les intérêts fondamentaux de la Nation, la sécurité publique et répression des infractions. Ces décisions et leur mise en œuvre participent à la définition d'un équilibre entre ces impératifs qui constitue un choix de société et un choix politique, qu'il appartient au Parlement de peser, parfaire et préciser.

3. Dans sa décision, le Conseil d'Etat a enjoint au Premier ministre de procéder à l'abrogation dans un délai de six mois, de l'article R. 10-13 du code des postes et des communications électroniques (CPCE) ainsi que du décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant

d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. Le Conseil d'Etat a en outre relevé que les dispositions visant à permettre la mise en œuvre de techniques de renseignement, sans contrôle préalable par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou une juridiction, en dehors des cas d'urgence dûment justifiés, devaient être annulées.

4. Dans ce contexte, si la Commission souligne qu'il appartiendra au législateur d'apprécier la conformité des dispositions projetées au regard des exigences tant constitutionnelles qu'européennes, elle souligne que les modalités d'application d'une partie de ces dispositions devront être précisées par voie réglementaire et précise à cet égard qu'elle entend faire un examen circonstancié du présent dispositif sans que cela préjuge de son appréciation du respect des principes relatifs à la protection des données à caractère personnel s'agissant des conditions de mise en œuvre effectives de ces dispositions.

5. Elle regrette néanmoins d'avoir à se prononcer dans des conditions d'urgence extrême sur de telles évolutions, compte tenu des enjeux associés à la collecte généralisée et indifférenciée des données relatives aux communications électroniques et les impacts substantiels s'agissant de la vie privée des personnes concernées qui en résultent.

Sur la modification des dispositions relatives au régime de conservation des données relatives aux communications électroniques par les opérateurs (article 11 quinquies du projet de loi)

6. Le projet de loi prévoit de modifier l'article 34-1 du CPCE qui organise le régime de conservation des données relatives aux communications électroniques par les opérateurs, pour prévoir, par dérogation au principe selon lequel ces opérateurs effacent ou rendent anonymes sans délai les données de connexion afférentes aux communications de leurs abonnés, les hypothèses dans lesquelles il peut être dérogé à cette obligation.

En ce qui concerne la conservation des données relatives à l'identité des utilisateurs, ainsi que des données techniques permettant de les identifier, ou relatives aux équipements terminaux de connexion utilisés

7. Le projet de loi prévoit que « *les opérateurs de communication 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 d'un 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* ».

8. Si la Commission relève que la Cour de justice et le Conseil d'Etat ont admis la possibilité de conserver de manière généralisée et indifférenciée les données relatives aux communications portant sur l'identité des personnes concernées, notamment en ce que leur conservation est considérée comme susceptible de porter une atteinte

moindre à la vie privée de ces personnes, les dispositions projetées appellent les observations suivantes.

9. **En premier lieu**, le projet de loi prévoit qu'un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, selon l'activité des opérateurs et la nature des communications, les informations et catégories de données conservées en application de cet article. La Commission relève que le renvoi aux « *données techniques permettant d'identifier l'utilisateur ou relatives aux équipements terminaux de connexion utilisés* » est particulièrement large. Si elle relève que l'adresse IP pourra notamment être conservée à ce titre, elle rappelle que seules les données nécessaires aux finalités poursuivies par une telle conservation devront être conservées par les opérateurs.

10. A cet égard, elle rappelle en outre que la CJUE a considéré que la conservation de ces données devait notamment, pour des finalités autres que celles relevant de la sécurité nationale, être temporellement limitée au strict nécessaire.

11. Elle souligne en outre que la conservation de ce type de données ne saurait être justifiée pour un spectre large de finalités et notamment la poursuite et la recherche de toute infraction pénale. A ce titre, si le Conseil d'Etat a considéré que le législateur n'était pas tenu d'énumérer les infractions relevant du champ de la criminalité grave et pour lesquelles une conservation de ces données serait justifiée (qui sera en tout état de cause contrôlé par le juge pénal), la Commission estime que le projet de loi devrait préciser les finalités premières pour lesquelles ces données devraient être conservées par les opérateurs.

12. **En second lieu,** le projet de loi prévoit que « *les données conservées et traitées dans les conditions définies aux II bis à V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux* ».

13. A cet égard, la Commission relève que compte tenu des finalités pour lesquelles elles sont traitées, les données conservées dans les conditions définies au II bis de l'article 34-1 du CPCE ne pourront porter sur la localisation des équipements terminaux. Elle invite dès lors le ministère à préciser la disposition précitée en ce sens.

Sur la conservation de données relatives aux communications électroniques en cas de menace grave, actuelle ou prévisible pour la sécurité nationale

14. L'article 11 quinquies prévoit qu'« en *cas de menace grave, actuelle ou prévisible, pour la sécurité nationale, le Premier ministre peut enjoindre aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données relatives aux communications électroniques, en complément de celles mentionnées au II bis* ».

15. Le projet de loi précise en outre que « *l'injonction du Premier ministre, qui prend la forme d'un décret dont la durée d'application ne peut excéder un an, peut être renouvelée si les conditions prévues pour son édiction continuent d'être réunies* ».

16. A cet égard, la Commission rappelle que la Commission nationale de contrôle des techniques de renseignement (CNCTR) est compétente s'agissant de la mise en œuvre de techniques de renseignement et constitue à ce titre un des maillons de la chaîne opérationnelle conduisant au recueil de renseignements. Dès lors, elle estime, dans la mesure où le principe même de la conservation de données de trafic et de localisation constitue une atteinte à la vie privée, que l'injonction du Premier ministre imposant aux opérateurs la conservation de ces données devrait être soumise pour avis à la CNCTR. La Commission relève qu'une telle modalité est notamment de nature à garantir un strict équilibre entre l'atteinte à la vie privée portée par cette collecte et la protection de la sécurité nationale.

17. A cet égard, la Commission rappelle que le juge européen a subordonné la collecte généralisée et indifférenciée des données de trafic et de localisation à la seule hypothèse d'une « *menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible* », cette collecte devant également être limitée dans le temps. Dans ce contexte, le Conseil d'Etat a estimé que la durée de cette injonction de conservation faite aux opérateurs, ne « *saurait raisonnablement excéder un an* ».

18. La Commission estime que l'article 11 quinquies, en ce qu'il prévoit que la durée d'application de cette injonction ne peut excéder un an, vise à répondre aux exigences posées par le Conseil d'Etat.

Sur la conservation et l'accès aux données relatives aux communications électroniques pour les besoins de la recherche, de la constatation et la poursuite d'infractions pénales

19. Le projet de loi prévoit de supprimer les dispositions figurant actuellement au III de l'article L. 34-1 du CPCE, qui encadrent la conservation de certaines catégories de données, pour les besoins notamment, de la recherche, de la constatation et de la poursuite d'infractions pénales notamment.

20. La Commission relève que cette modification vise à tenir compte, tant des exigences européennes rappelées par la CJUE que de la décision du Conseil d'Etat du 21 avril 2021.

21. Le Conseil d'Etat a enjoint au Premier ministre de procéder à l'abrogation de sa décision refusant d'abroger l'article R. 10-13 du CPCE ainsi que le décret du 25 février 2011, notamment en ce que ces dispositions ne limitent pas les finalités de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation à la sauvegarde de la sécurité nationale. Cette censure est justifiée par le fait que la CJUE a jugé que la conservation généralisée de ces données pour les besoins de la poursuite des infractions pénales était contraire au droit de l'Union européenne.

22. Cependant, la haute juridiction administrative a considéré que les critères posés par la CJUE pour permettre une conservation de ces données à cette fin (conservation ciblée, prédétermination des personnes susceptibles d'être impliquées dans une infraction pénale) n'étaient matériellement pas réalisables. Elle a en revanche estimé qu'une conservation dite rapide des données pour permettre de faire obstacle à la disparition des informations nécessaires aux enquêtes pénales était permise par le droit européen. Concrètement, elle a estimé que cette conservation dite rapide pouvait se traduire par une injonction de l'autorité judiciaire, faite aux opérateurs de

communications électroniques, aux fournisseurs d'accès internet et aux hébergeurs de sites internet, de procéder à la conservation (pour une durée de quatre-vingt-dix jours maximum) des données de connexion qu'ils détiennent, y compris parmi celles conservées au titre de la conservation imposée aux fins de sauvegarde de la sécurité nationale. C'est sur cette conservation rapide que se greffe la possibilité pour les autorités judiciaires d'accéder à ces données pour des enquêtes pénales relatives à des cas avérés ou suspectés de criminalité grave.

23. A cet égard, la Commission comprend du dispositif tel qu'il lui a été soumis par le ministère, que l'accès aux données, notamment de trafic et de localisation, pourra être rendu possible au moyen de réquisitions judicaires.

24. Elle rappelle que le Conseil d'Etat a subordonné la possibilité pour l'autorité judiciaire d'accéder aux données nécessaires à la poursuite et à la recherche des auteurs d'infractions pénales, à celles dont la gravité le justifie. Si à cet égard, l'article préliminaire du code de procédure pénale (CPP) prévoit que « *les mesures de contraintes dont la personne suspectée ou poursuivie peut faire l'objet sont prises sur décision ou sous le contrôle effectif de l'autorité judiciaire* » et qu'elles « *doivent être strictement limitées aux nécessités de la procédure, proportionnées à la gravité de l'infraction reprochée et ne pas porter atteinte à la dignité de la personne* », la Commission rappelle, en tout état de cause, qu'un contrôle strict de l'application de ces dispositions, compte tenu de l'atteinte portée à la vie privée des personnes concernées induite par la conservation de ces données, devra être réalisé, tant par les services d'enquête que par les autorités judiciaires.

25. La Commission relève en outre que le projet de loi, en ce qu'il modifie l'article L. 34-1 du CPCE et l'article 6 de la loi pour une confiance dans l'économie numérique, conduit à ce qu'aucune disposition spécifique n'encadre désormais l'accès à ces données pour les finalités de recherche, de constatation et de poursuite d'infractions pénales. Dès lors, elle s'interroge, eu égard à la spécificité des données auxquelles il pourra être accédé, et afin d'assurer la stricte proportionnalité de cet usage, sur le caractère suffisant des dispositions actuelles, notamment eu égard au champ d'application de l'article 60-2 du code de procédure pénale, pour encadrer les modalités de conservation dite rapide de ces données ainsi que leur accès (par exemple pour fixer la durée maximale de « conservation rapide »). En tout état de cause, la Commission souligne que, dans la mesure où seules les infractions considérées comme graves pourront justifier un tel accès, et comme l'a souligné dans ses conclusions le rapporteur public, les contraventions devraient, par principe, être exclues de ce périmètre.

Sur la modification des dispositions relatives aux obligations faites aux fournisseurs d'accès

26. Le projet de loi modifie l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique afin de prévoir que les fournisseurs d'accès à des services de communication au public en ligne, conservent les données d'identification dans les mêmes conditions que celles prévues à l'article L. 34-1 du CPCE.

27. Sous les réserves précédemment formulées, la Commission estime que la modification de cet article n'appelle pas d'observation complémentaire.

Sur le contrôle préalable de la mise en œuvre des techniques de renseignement (article 11 sexies du projet de loi)

28. Le projet de loi modifie les dispositions de l'article L. 821-1 du code de la sécurité intérieure (CSI) afin de prévoir que pour l'ensemble des techniques de renseignement, leur mise en œuvre, en cas d'avis défavorable de la CNCTR, implique obligatoirement une saisine de la formation spécialisée du Conseil d'Etat par la CNCTR. Dans cette hypothèse, le Conseil d'Etat dispose d'un délai de vingt-quatre heures pour statuer, délai pendant lequel la technique de renseignement en cause ne peut être mise en œuvre, sauf en cas d'urgence dûment justifiée et si le Premier ministre a ordonné sa mise en œuvre immédiate.

29. A cet égard, la Commission relève que ces dispositions visent à tenir compte des observations formulées par le Conseil d'Etat dans sa décision du 21 avril précité, éclairée par les exigences européennes rappelées par la CJUE. La mise en œuvre de l'ensemble de ces techniques est subordonnée à une décision dotée d'effet contraignant, prise par une juridiction ou une entité administrative indépendante. La réforme revient donc à soumettre la mise en œuvre d'une technique de renseignement, hors cas d'urgence, à l'avis conforme de la CNCTR, sauf à ce qu'une décision de justice en décide autrement. La Commission accueille favorablement le principe d'une telle évolution.

30. Elle considère cependant que le projet de loi appelle les observations suivantes.

31. **En premier lieu**, la Commission estime que le dispositif est inutilement complexe en ce qu'au lieu de prévoir un avis conforme de la CNCTR, il prévoit une saisine du Conseil d'Etat, par des membres de la CNCTR et non le Premier ministre, dans l'hypothèse où un avis défavorable serait rendu. Elle relève en outre que les dispositions projetées permettent formellement au Premier ministre d'autoriser la mise en œuvre immédiate d'une technique de renseignement après l'avis défavorable de la CNCTR et avant que le Conseil d'Etat ait statué. La Commission invite le Gouvernement à prévoir un dispositif plus simple et plus protecteur en prévoyant un avis conforme de la CNCTR. Elle recommande donc qu'il soit, sauf dans certains cas d'urgence, interdit au premier ministre d'autoriser la mise en œuvre d'une technique de renseignement après avis défavorable de la CNCTR. Il reviendrait alors au Premier ministre soit de renoncer à la mise en œuvre de la technique, soit de saisir lui-même le Conseil d'Etat.

32. **En deuxième lieu**, si la Commission comprend qu'il soit nécessaire, au regard des enjeux, que la formation du Conseil d'Etat statue dans les plus brefs délais, elle estime possible qu'un délai de vingt-quatre heures ne soit pas toujours suffisant pour juger des cas les plus complexes. Dans l'hypothèse où le juge ne parviendrait pas, malgré sa diligence, à trancher le litige dans ce délai, elle estime qu'il résulte du texte que la mesure de renseignement ne pourra pas être mis en œuvre tant qu'elle n'aura pas été autorisée par la décision de justice.

33. **En troisième lieu**, le projet de loi abroge l'article L. 821-5 du CSI qui prévoit que dans certaines situations d'urgence et pour des finalités limitées, le Premier ministre peut autoriser la mise en œuvre d'une technique de renseignement sans avis préalable de la CNCTR.

34. La Commission relève que les dispositions introduites par le projet de loi constituent une évolution positive dans la mesure où l'avis de la CNCTR sera systématiquement sollicité, sans dérogation possible. Elle souligne néanmoins que dans l'hypothèse où la CNCTR rendrait un avis défavorable, le Premier ministre peut, en cas d'urgence dûment justifiée, ordonner la mise en œuvre immédiate de la technique, et ce, avant que le Conseil d'Etat se soit prononcé.

35. Le projet de loi prévoit toutefois des limitations à cette hypothèse, qui ne pourra être mobilisée que pour certaines finalités (l'indépendance nationale, l'intégrité du territoire et la défense nationale, la prévention du terrorisme, et les atteintes à la forme républicaine des institutions, conformément à l'article L. 811-3 du CSI) concernant la sonorisation de certains lieux et véhicules ainsi que la captation d'images et de données informatiques. En outre, le caractère d'urgence ne pourra être invoqué s'agissant de la technique dite de « l'algorithme » encadrée à l'article L. 851-3 du CSI.

36. La Commission considère que cet encadrement constitue une garantie importante pour s'assurer que les situations dans lesquelles l'urgence peut être mobilisée soient limitées à des cas précisément définis. Elle relève néanmoins que pour la majorité des techniques de renseignement encadrées par le CSI, le projet de loi ne prévoit pas de limitation particulière quant aux conditions dans lesquelles l'urgence pourrait être mobilisée. A cet égard, la Commission estime qu'une réflexion pourrait être engagée sur l'opportunité de limiter à certaines finalités considérées comme les plus graves, et ce pour l'ensemble des techniques de renseignement, le recours à cette procédure d'urgence.

Sur la transmission d'informations par l'autorité judiciaire aux services de renseignement et à l'Agence nationale de la sécurité des systèmes d'information (article 11 septies)

37. L'article 11 septies du projet de loi encadre, pour certaines procédures d'enquêtes ou d'instruction et par dérogation au secret de l'instruction, la possibilité pour le procureur de la République de Paris (ou le cas échéant le juge d'instruction), de communiquer aux services de renseignement, ainsi qu'à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) des éléments de toute nature figurant dans ces procédures et nécessaires à l'exercice de leurs missions.

38. A titre liminaire, la Commission souligne qu'elle s'est prononcée dans sa délibération n° 2021-045 du 15 avril 2021 relative à certains articles du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, sur des dispositions de nature similaire. Dans ce contexte, les observations développées ci-après portent principalement sur les évolutions envisagées par le ministère, et ce, sans préjudice des remarques formulées dans la délibération précitée.

39. De manière générale, la Commission rappelle que si que les enjeux associés à cette modification dépassent les seules considérations « Informatique et Libertés », elle souligne néanmoins que les dispositions visées, en ce qu'elles permettent la transmission de données à caractère personnel, doivent s'effectuer dans le respect des principes relatifs à la protection de ces données, et plus spécifiquement ceux relatifs à la proportionnalité et la licéité des traitements.

40. **En premier lieu**, la Commission relève que le périmètre infractionnel visé par le projet de loi, s'il est limité aux affaires qui sont ou apparaîtraient d'une très grande complexité, semble néanmoins large du fait de certaines des infractions pénales auxquelles il est renvoyé (par exemple s'agissant des délits de trafic de stupéfiants), sans pour autant que les cas d'usage correspondant à une telle possibilité soient particulièrement identifiés et aient été portés à sa connaissance à ce stade. Dès lors, comme formulé dans sa délibération précitée, la Commission s'interroge sur le périmètre précisément visé par l'article 11 septies du projet de loi.

41. **En deuxième lieu,** le projet de loi prévoit que ces informations peuvent, dans cette nouvelle version du projet, être transmises aux services de renseignement dits du « premier » et du « second cercle », pour les seules missions relevant de la prévention de la criminalité et de la délinquance organisée. A cet égard, la Commission s'interroge sur les raisons ayant conduit le ministère à étendre cette possibilité aux services dits du « second cercle ».

42. **En troisième lieu**, le projet de loi précise que cette communication peut intervenir à l'initiative du procureur de la République ou du juge d'instruction, ou à la demande des services de renseignement. A cet égard, si le projet de texte précise que dans le cadre d'une information judiciaire, cette communication ne pourra intervenir qu'avec l'avis favorable du juge d'instruction, la Commission estime que le projet de loi devrait être précisé afin de mentionner expressément le caractère facultatif, pour les autorités judiciaires, de la transmission de telles données, en indiquant qu'il revient à l'autorité judiciaire d'apprécier si celle-ci est de nature à nuire à la bonne administration de la justice.

La Présidente

Marie-Laure DENIS