Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

COMMISSION NATIONALE DE CONTRÔLE DES TECHNIQUES DE RENSEIGNEMENT

Délibération n° 4/2021 du 30 avril 2021

La Commission nationale de contrôle des techniques de renseignement (CNCTR) a été saisie pour avis par le Premier ministre le 26 avril 2021 d'une lettre rectificative au projet de loi relatif à la prévention d'actes de terrorisme et au renseignement [1]. Cette lettre contient deux articles additionnels destinés à tirer les conséquences de la décision « French data network et autres » rendue par l'assemblée du contentieux du Conseil d'Etat le 21 avril 2021[2] après que la Cour de justice de l'Union européenne (CJUE) a répondu, dans un arrêt du 6 octobre 2020[3], aux questions préjudicielles que le Conseil d'Etat lui avait posées dans une décision avant-dire droit du 26 juillet 2018[4].

L'article 11 *quinquies* du projet de loi est relatif au régime de conservation des données relatives aux communications électroniques par les opérateurs de communications électroniques.

L'article 11 *sexies* modifie le dispositif de contrôle préalable des demandes de mise en œuvre des techniques de renseignement.

Les observations qui suivent constituent l'avis de la CNCTR.

---

[1] La saisine initiale du 8 mars 2021 a été complétée par une première saisine rectificative le 7 avril 2021. Les délibérations de la CNCTR n° 2/2021 du 7 avril 2021 et n° 3/2021 du 14 avril 2021 constituent les avis rendus par la commission sur les dispositions soumises à son examen. Elles sont disponibles sur le site internet de la commission.

[2] Il s'agit de la décision rendue sur les requêtes n[os] 393099, 39492, 397844, 397851, 424717 et 424718.

[3] Il s'agit de l'arrêt « La Quadrature du Net et autres » rendue sur les requêtes C-511/18, C-512/18 et C-520/18.

[4] Voir les requêtes n[os] 394922, 397844, 397851 et 399099.

1. Sur le régime de conservation des données de connexion (article 11 *quinquies* du projet de loi)

L'article L. 34-1 du code des postes et des télécommunications (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.

Dans sa décision du 21 avril 2021, le Conseil d'Etat a jugé que le Gouvernement ne pouvait, 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 à l'identité civile, aux adresses IP et aux informations relatives aux comptes et aux paiements, aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public. Il a, en revanche, admis qu'une telle obligation de conservation généralisée et indifférenciée peut être fondée sur la sauvegarde de la sécurité nationale et il a estimé que toutes les finalités énumérées à l'article L. 811-3 du code de la sécurité intérieure doivent être regardées comme relevant de la sécurité nationale. Il a, cependant, jugé que cette obligation doit être subordonnée au constat, à échéance régulière qui ne saurait raisonnablement excéder un an, de la persistance d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

L'article 11 *quinquies* tire les conséquences de l'arrêt du 21 avril 2021 en modifiant l'article L. 34-1 du CPCE pour y préciser :

- que les opérateurs de communications électroniques sont tenus de conserver jusqu'à l'expiration d'un délai de cinq ans après la fin de validité de leur contrat les informations relatives à l'identité civile de l'utilisateur et, pour une durée d'un an, les autres informations fournies par l'utilisateur lors de la souscription de son contrat, les informations de paiement et les données techniques permettant d'identifier l'utilisateur ou relatives aux « *équipements terminaux de connexion* » utilisés parmi lesquelles figurent notamment les adresses IP attribuées à la source d'une connexion ;
- qu'ils sont également tenus, aux seules fins de sauvegarde de la sécurité nationale, d'opérer une conservation généralisée et indifférenciée, pendant une durée d'un an, de certaines catégories de données de connexion, y compris les données de trafic et de localisation, sous réserve qu'une injonction du Premier ministre, qui prend la forme d'un décret dont la durée d'application ne peut excéder un an et peut être renouvelée, constate l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

L'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique est également modifié pour prévoir les mêmes obligations pour les fournisseurs d'accès à internet et les hébergeurs de contenus.

Les dispositions de l'article 11 *quinquies* du projet de loi ont donc pour objet de mettre les dispositions législatives qui viennent d'être évoquées en conformité avec le droit de l'Union européenne. Elles n'appellent pas d'observations de la part de la CNCTR.

2. Sur le contrôle préalable des demandes de techniques de renseignement (article 11 *sexies* du projet de loi)

2.1 Dans sa décision « French data network et autres » du 21 avril 2021, le Conseil d'Etat a jugé que la mise en œuvre des techniques de renseignement prévues aux articles L. 851-1 à L. 851-4 du code de la sécurité intérieure devait être soumise au contrôle préalable d'une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou d'une juridiction, en dehors des cas d'urgence dûment justifiée, et que les dispositions en vigueur du code de la sécurité intérieure ne répondaient pas à cette exigence. Il tire ainsi les conséquences des arrêts du 21 décembre 2016[5] et du 6 octobre 2020 de la Cour de justice de l'Union européenne qui ont jugé que le droit de l'Union européenne imposait, sauf en cas d'urgence dûment justifiée, un contrôle préalable par une juridiction ou une autorité administrative indépendante dotée d'un pouvoir contraignant.

L'article 11 *sexies* du projet de loi propose, pour adapter le dispositif actuel aux exigences du droit de l'Union européenne, plusieurs modifications aux dispositions du livre huitième du code de la sécurité intérieure relatives au renseignement :

- il prévoit, à l'article L. 821-1 de ce code, que lorsque le Premier ministre délivre une autorisation de mise en œuvre d'une technique de renseignement après avis défavorable de la CNCTR, le Conseil d'Etat est immédiatement saisi et doit statuer sur la légalité de la décision du Premier ministre dans un délai de vingt-quatre heures. La décision du Premier ministre ne peut être exécutée avant que le Conseil d'Etat ait statué « sauf en cas d'urgence dûment justifiée et si le Premier ministre a ordonné sa mise en œuvre immédiate » ;

- il exclut la possibilité d'invoquer l'urgence pour autoriser la mise en œuvre initiale ou le renouvellement de la technique de l'« algorithme » prévue à l'article L. 851-3 de ce code ;

- il limite à certaines finalités la possibilité d'invoquer le caractère d'urgence pour autoriser la captation de paroles prononcées à titre privé ou confidentiel ou d'images dans un lieu privé et le recueil et la captation de données informatiques par des dispositifs techniques, ainsi que pour autoriser la pénétration dans un lieu privé afin d'y mettre en œuvre une technique de renseignement ;

- il abroge, enfin, l'article L. 821-5 de ce code qui permet au Premier ministre, en cas d'« urgence absolue » et pour un nombre limité de finalités, de délivrer une autorisation de mise en œuvre d'une technique de renseignement sans avis préalable de la CNCTR.

---

[5] Il s'agit de l'arrêt dit « Tele 2 Sverige AB » rendu par la CJUE réunie en grande chambre le 21 décembre 2016 sur les requêtes C-203/15 et C-698/15.

2.2 La CNCTR rappelle que, jusqu'à présent, le Premier ministre n'a jamais autorisé la mise en œuvre d'une technique de renseignement après qu'elle a émis un avis défavorable. Ce constat, qui témoigne de la solidité du dispositif légal de contrôle préalable issu de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, ne prive, cependant, pas de pertinence les modifications proposées par l'article 11 *sexies* du projet de loi.

Le mécanisme de contrôle proposé est déjà prévu au III de l'article L.853-3 du code de la sécurité intérieure dans le cas précis et limité de l'introduction dans un lieu privé à usage d'habitation. La CNCTR estime que son extension, par la modification proposée de l'article L. 821-1 du même code, à l'ensemble des techniques de renseignement répond à l'exigence, posée par le Conseil d'Etat statuant au contentieux, d'un contrôle préalable de la mise en œuvre des techniques de renseignement par une autorité administrative indépendante dotée d'un pouvoir d'avis conforme ou par une juridiction. Elle permet de combiner le contrôle préalable de la CNCTR, autorité administrative indépendante, et le contrôle juridictionnel du Conseil d'Etat. En application de ce mécanisme, lorsque la CNCTR émet un avis défavorable à une demande de mise en œuvre d'une technique de renseignement, le Premier ministre ne peut passer outre à cet avis défavorable en délivrant une autorisation sans que le Conseil d'Etat statuant au contentieux soit saisi et, sauf en cas d'urgence dûment justifiée, sans qu'il ait préalablement statué sur la légalité de sa décision. Ce mécanisme de contrôle préalable laisse entier le pouvoir du Premier ministre de ne pas autoriser une technique de renseignement qui aurait pourtant recueilli l'assentiment de la CNCTR. Outre que cette décision ne porte pas atteinte au droit au respect de la vie privée, il appartient en effet au Premier ministre, en vertu de ses prérogatives constitutionnelles, d'apprécier, lorsqu'il se prononce sur une demande de surveillance, les risques liés à la réalisation de l'opération envisagée.

2.3 La commission approuve le choix opéré par l'article 11 *sexies* du projet de loi d'appliquer le mécanisme de contrôle préalable à l'ensemble des techniques de renseignement, sans le limiter à celles relatives aux accès aux données de connexion qui étaient l'objet du litige porté devant le Conseil d'Etat. Ce choix conforte la cohérence du cadre légal de contrôle des techniques de renseignement.

Le projet de loi omet, cependant, d'étendre l'application du mécanisme proposé à la surveillance des communications électroniques internationales. Depuis la loi n° 2018-17 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, la CNCTR exerce un contrôle préalable sur les demandes d'autorisation d'exploitation des communications électroniques internationales (III de l'article L. 854-2 du code de la sécurité intérieure) ainsi que sur les demandes d'autorisation d'exploitation de communications d'identifiants techniques rattachables au territoire national dont l'utilisateur communique depuis ce territoire (V du même article). La CNCTR estime, dès lors, que le mécanisme d'avis conforme ci-dessus décrit doit également s'appliquer, pour des raisons de cohérence, dans le domaine de la surveillance des communications électroniques internationales. Elle recommande en conséquence que des dispositions similaires à celles prévues par le 1° du I de l'article 11 *sexies* du projet de loi soient introduites dans l'article L. 854-2 du code de la sécurité intérieure.

2.4 La CNCTR approuve l'abrogation de l'article L. 821-5 du code de la sécurité intérieure. Bien que cet article n'ait été utilisé qu'une seule fois[6], quelques mois après l'entrée

[6] Alors que la CNCTR était pourtant en mesure de rendre son avis dans un délai compatible avec l'urgence invoquée.

en vigueur de la loi du 24 juillet 2015, il n'en constitue pas moins une exception au principe du contrôle préalable exercé par la CNCTR sur toutes les demandes de techniques de renseignement. Or, la commission a démontré qu'elle était en mesure d'exercer son contrôle préalable à tout moment, dans des délais extrêmement courts lorsque cela est nécessaire pour répondre aux exigences opérationnelles propres à l'activité des services de renseignement. Le maintien d'une disposition dérogatoire au principe du contrôle préalable n'est donc pas justifié.

2.5 Le mécanisme d'avis conforme proposé doit cependant prendre en compte les cas d'urgence dûment justifiée dans lesquels la mise en œuvre de l'autorisation ne peut attendre la décision de la formation spécialisée du Conseil d'Etat, même si elle est rendue dans le délai de vingt-quatre heures prévu par l'article 11 *sexies* du projet de loi. Ce texte envisage quatre situations :

a) celle de l'autorisation de la mise en œuvre ou du renouvellement d'un algorithme (I et II de l'article L. 851-3 du code de la sécurité intérieure), dans laquelle le caractère d'urgence ne peut être invoqué. La CNCTR estime que cette disposition est justifiée par la nature particulière de la technique de l'algorithme qui nécessite un contrôle approfondi.

La commission recommande également d'exclure la possibilité d'invoquer le caractère d'urgence pour la mise en œuvre de techniques concernant un parlementaire, un magistrat, un avocat ou un journaliste. Elle rappelle que l'article L. 821-7 du code de la sécurité intérieure prohibe la surveillance de ces personnes à raison de l'exercice de leur mandat ou de leur profession et qu'il écarte la procédure d'urgence absolue de l'article L. 821-5 du code de la sécurité intérieure pour la délivrance d'une autorisation de mise en œuvre d'une technique de renseignement, quelle qu'elle soit. Elle estime, dès lors, qu'en cas de désaccord entre la Commission et le Premier ministre il est préférable qu'avant toute mise en œuvre d'une mesure de surveillance le Conseil d'Etat statuant au contentieux ait pu se prononcer.

b) celle de l'autorisation de pénétrer dans un lieu privé à usage d'habitation pour y mettre en œuvre certaines techniques de renseignement (article L. 853-3 du code de la sécurité intérieure), dans laquelle le caractère d'urgence ne peut être invoqué que si l'autorisation a été délivrée au titre de la prévention du terrorisme. Le projet de loi propose de conserver les dispositions déjà prévues dans un tel cas par l'article L. 853-3, comme cela a été dit plus haut. La CNCTR estime que ces dispositions sont justifiées par le caractère particulièrement attentatoire à la vie privée de la pénétration dans un lieu d'habitation.

c) celle, propre à plusieurs techniques, dont la mise en œuvre porte une atteinte substantielle au droit au respect de la vie privée, dans laquelle le caractère d'urgence ne peut être invoqué que pour un nombre limité de finalités. Les techniques sont celles de l'article L. 853-1 du code de la sécurité intérieure (recueil de paroles prononcées à titre privé ou confidentiel et d'images dans un lieu privé) et de l'article L. 853-2 du même code (recueil de données informatiques par un dispositif technique). Est également concernée l'autorisation de pénétrer dans un lieu privé qui n'est pas un lieu d'habitation (article L. 853-3 de ce code). Les finalités sont celles prévues aux 1°, 4° et a du 5° de l'article L. 811-3 de ce code, qui concernent respectivement la défense de l'indépendance nationale, de l'intégrité du territoire et de la défense nationale, la prévention du terrorisme et la prévention des atteintes à la forme républicaine des institutions.

Ni la liste des finalités proposées, ni celle des techniques concernées n'appellent d'objections de la part de la CNCTR. La commission recommande, cependant, que pour d'autres techniques, qu'elle regarde comme portant également une atteinte substantielle au droit au respect de la vie privée le caractère d'urgence ne puisse être invoqué que pour ce nombre limité de finalités. Il s'agit des interceptions de sécurité réalisées avec le concours d'un opérateur (I de l'article L. 852-1 du code de la sécurité intérieure), par l'utilisation d'un *IMSI catcher*[7] (II du même article) et au sein d'un réseau de communications électroniques empruntant exclusivement la voie hertzienne (article L. 852-2 du même code) ainsi que du recueil de données de connexion au moyen d'un *IMSI catcher* (article L. 851-6 de ce code). Il est également souhaitable, à son avis, de faire de même pour la nouvelle technique d'interception de correspondances émises ou reçues par la voie satellitaire prévue, à titre expérimental, par l'article 13 *bis* du projet de loi.

d) celle, applicable aux autres techniques, dans laquelle le caractère d'urgence peut être invoqué sans limitation à certaines finalités.

Sous réserve des recommandations formulées ci-dessus aux points a et c, la CNCTR n'a pas d'objections sur ce point. Elle relève que, dans certains cas, les techniques de renseignement concernées ne sont autorisées que pour la finalité de prévention du terrorisme. Il s'agit du recueil de données de connexion en temps réel prévu par l'article L. 851-2 du code de la sécurité intérieure et de l'autorisation d'identification des personnes dont les données de connexion ont été détectées par un algorithme comme susceptibles de révéler une menace terroriste (IV de l'article L. 851-3 du même code).

Délibéré en formation plénière le 30 avril 2021

Francis DELON

Président de la Commission nationale
de contrôle des techniques de renseignement

[7] Dont la mise en œuvre ne peut d'ailleurs être autorisée que pour les mêmes finalités prévues au 1°, 4° et a du 5° de l'article L. 811-3 du code de la sécurité intérieure.