91 rue de Charenton
75012 Paris
Tel 01 48 05 47 88
Mail : contact@syndicat-magistrature.org
site : syndicat-magistrature.fr
Twitter : @Smagistrature

Paris, le 18 mai 2021,

Observations du Syndicat de la magistrature sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement

Dispositions relatives au renseignement (articles 7 et suivants)

L'exposé des motifs du projet de loi est très clair. Il *« vise à apporter au livre VIII du code de sécurité intérieure les ajustements nécessaires pour que les services de renseignement continuent de disposer de moyens d'action adéquats et proportionnés face aux menaces persistantes qui pèsent sur les intérêts fondamentaux de la Nation. »*

Pourtant, l'adéquation et la proportionnalité sont difficiles à trouver quand on regarde dans le détail les dispositions prévues.

Qu'il s'agisse en effet de la transmission d'informations par les autorités administratives même couvertes par le secret professionnel, de l'augmentation de la durée de conservation des renseignements pour les besoins de la recherche et du développement, de l'expérimentation des interceptions de correspondances par voie satellitaire, de la pérennisation des boîtes noires, ou encore de l'extension aux adresses complètes de ressources sur internet pour le recueil de données en temps réel et le recueil de données au moyen d'un traitement algorithmique - pour ne citer que ces exemples - ces dispositions illustrent en réalité la consécration de ce qui émergeait dès la loi du 24 juillet 2015 relative au renseignement, à savoir l'extension du champ des activités de renseignement et la légalisation de techniques de surveillance intrusives, alimentant de surcroît un brouillage des compétences administratives et judiciaires.

Dans ces observations formulées à propos de la loi du 24 juillet 2015, le Syndicat de la magistrature formulait un certain nombre de recommandations et notamment la principale : un véritable encadrement *a priori* des activités par une instance indépendante et qui n'exclut pas le juge judiciaire. Six ans plus tard, cette revendication est malheureusement toujours d'actualité alors que l'autorité judiciaire n'a aucune visibilité sur les affaires traitées par les services du renseignement, et aucun levier pour s'en saisir, bien qu'elle soit la gardienne de la liberté individuelle aux termes de la Constitution.

Ces questionnements relatifs, au fond, au fonctionnement d'un Etat de droit auraient mérité un examen approfondi du texte, seul à même de créer les conditions d'un débat serein, s'agissant de la protection des libertés individuelles. C'est hélas la procédure accélérée qui a - encore une fois - été choisie. Le Syndicat de la magistrature, malgré ce calendrier très

restreint, a sollicité une audition devant la commission des lois et souhaité faire une analyse détaillée du contenu de ce projet de loi.

Article 7

L'ouverture de la possibilité de transmission de données et l'atténuation de la règle de « la finalité » en matière de renseignements

Actuellement l'article L. 822-3 du code de la sécurité intérieure dispose que :

« Les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles mentionnées à l'article L. 811-3. Ces opérations sont soumises au contrôle de la Commission nationale de contrôle des techniques de renseignement. »

Cet article est toutefois à mettre en lien avec l'article L. 863-2 du code de la sécurité intérieure (CSI) qui dispose que :

« Les services spécialisés de renseignement mentionnés à l'article L. 811-2 et les services désignés par le décret en Conseil d'Etat prévu à l'article L. 811-4 peuvent partager toutes les informations utiles à l'accomplissement de leurs missions définies au titre Ier du présent livre. » dont le contenu imprécis, du fait de l'absence de décret, a pu être dénoncé à plusieurs reprises tant par des associations telles que La Quadrature du Net que par la CNIL qui indique :« *l'absence de décret pris pour l'application des dispositions prévues au premier alinéa du même article L. 863-2 fait peser un risque juridique sur les échanges entre services et la conservation éventuelle de ces informations. En particulier, toute conservation systématique dans un traitement de données de telles informations devrait faire l'objet d'un décret en Conseil d'État pris après avis de la CNIL* ».

L'article 7 du projet de loi complète l'article L. 822-3 du code de sécurité intérieure pour encadrer les conditions dans lesquelles les services de renseignement peuvent, d'une part, exploiter les renseignements qu'ils ont obtenus pour une finalité différente de celle qui en a justifié le recueil et, d'autre part, se transmettre les renseignements qu'ils ont collectés par la mise en œuvre des techniques autorisées par le livre VIII du code de la sécurité intérieure.

En premier lieu, lorsqu'un service de renseignement obtient, après la mise en œuvre régulière d'une technique de renseignement pour une finalité donnée, des renseignements utiles à la poursuite d'une finalité différente de celle qui en a justifié le recueil, il peut les transcrire ou les extraire pour le seul exercice de ses missions.

En deuxième lieu, les renseignements collectés, extraits ou transcrits peuvent être transmis à d'autres services de renseignement si cette transmission est strictement nécessaire à l'exercice des missions du service destinataire. Une telle transmission devra néanmoins être subordonnée à l'autorisation du Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR), dans deux hypothèses :

- lorsque cette transmission concerne des renseignements à l'état brut – c'est-à-dire ni extraits, ni transcrits – et poursuit une finalité différente de celle ayant justifié leur recueil ;

- lorsque cette transmission concerne des renseignements, qu'ils soient à l'état brut, extraits ou transcrits, recueillis par la mise en œuvre d'une technique à laquelle le service de renseignement destinataire n'aurait pu recourir au titre de la finalité motivant la transmission.

L'exposé des motifs du projet de loi prétend que *« ces deux verrous permettent ainsi de s'assurer de la pertinence de la transmission entre services, en particulier lorsqu'elle procède d'une technique limitée à une finalité donnée ou réservée à un nombre restreint de services de renseignement. »*

Pourtant, cet article constitue un changement de paradigme majeur dès lors qu'il ouvre la voie à l'utilisation de renseignements collectés pour un autre but. Il remet ainsi en cause la logique de « finalisation » inhérente au fonctionnement du renseignement et accroît de façon importante les possibilités d'intrusions dans la vie privée des citoyens, du fait que la condition de finalité va diminuer et partant les possibilités de contrôle liés à ce critère.

En effet, l'article L. 822-3 du CSI limitait jusque-là de façon très nette les possibilités d'échange de renseignements en cloisonnant les services et aboutissait, de fait, à ce qu'un service utilise une technique de renseignement pour une seule finalité, l'exploite dans ce but et la supprime une fois la finalité exploitée. Désormais, une voie est créée de transmission des renseignements à des services qui n'auraient pas pu les obtenir, donc éventuellement à des services de renseignements *lambda*, non habilités à les requérir.

Ces échanges dans un sens ou dans un autre se feront librement, l'étude d'impact indiquant que : « *Ces échanges d'informations n'ont en principe pas à faire l'objet d'une procédure spécifique d'autorisation, sauf à alourdir inutilement et à freiner les échanges entre services, alors que leurs missions et leurs méthodes de travail supposent une coopération étroite*. »

Toutefois, dans deux hypothèses, il faudra l'autorisation du Premier ministre et le contrôle de la CNCTR : lorsque la transmission de A vers B des renseignements collectés « *bruts* » poursuit une finalité différente de celle qui en a justifié le recueil et lorsque les transmissions des renseignements collectés, extraits ou transcrits sont le fruit d'un outil de surveillance auquel le service destinataire n'aurait pu recourir au titre de la finalité motivant la transmission.

Le risque est ainsi grand qu'en réalité, ces services demandent à des services habilités d'utiliser une technique de renseignement à laquelle ils n'ont pas accès pour obtenir des informations. Il sera en effet très difficile de pouvoir vérifier ensuite que la technique de renseignement a été utilisée pour une autre fin et a permis la découverte de tels renseignements et non qu'il s'agit de l'inverse.

Le contrôle de la CNCTR semble en effet très restreint, s'agissant uniquement d'une transmission à la CNCTR lorsque *« les transcriptions, extractions ou les transmissions poursuivent une finalité différente de celle au titre de laquelle les renseignements ont été recueillis »,* sans pour autant que la CNCTR puisse exercer une réelle vérification sur les conditions d'obtention de ces renseignements et le risque de demande expresse par d'autres services évoqué plus haut.

Le Syndicat de la magistrature lors du vote de la loi relative au renseignement du 24 juillet 2015 avait déjà pu critiquer le fait que le Premier ministre soit l'autorité décisionnaire et argumenter sur le fait qu'il était possible de donner à la CNCTR un pouvoir de décision, ou *a minima* d'avis conforme (c'est-à-dire d'avis liant sans exception le Premier ministre). Compte tenu du caractère extrêmement attentatoire aux libertés et à la vie privée des pouvoirs qui seraient donnés aux services, il est légitime que l'exécutif ne puisse en disposer. Le Syndicat de la magistrature estime toujours que la décision devrait ainsi être confiée à une autorité indépendante, assurant la séparation des pouvoirs, la possibilité pour la CNCTR de faire des recommandations ou de saisir le Conseil d'Etat n'étant pas suffisante.

La transmission d'information par les autorités administratives même couvertes par le secret professionnel

Actuellement, l'article L. 863-2 du CSI dispose que *« 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 peuvent transmettre aux services mentionnés au premier alinéa du présent article, de leur propre initiative ou sur requête de ces derniers, des informations utiles à l'accomplissement des missions de ces derniers ».*

Avec ce projet de loi, pourront désormais être transmises par ces autorités administratives *« 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 »*

Cette disposition interroge fortement quant à la traçabilité et à la durée de conservation de ces informations une fois transmises, la seule précision faite étant que les informations sont détruites dès lors qu'elles ne sont plus nécessaires à l'accomplissement des missions du service auquel elles ont été transmises, le critère du « plus nécessaire » n'étant alors aucunement borné dans le temps.

Le Conseil d'Etat partage cette interrogation sur la durée de conservation de ces informations. Il préconise ainsi qu'il soit précisé que *« les informations transmises sont immédiatement détruites par le service destinataire lorsque celui-ci constate qu'elles ne sont pas ou plus strictement nécessaires à l'exercice de ses missions et de prévoir qu'un décret fixera les conditions dans lesquelles est assurée la traçabilité des transmissions depuis les traitements de données à caractère personnel des autorités administratives concernées vers les services de renseignement »*. Des précisions et des limitations en la matière sont donc absolument nécessaires.

Par ailleurs, la précision selon laquelle *« Les conditions dans lesquelles la traçabilité des transmissions mentionnées au premier alinéa est mise en œuvre dans les traitements de données à caractère personnel des autorités administratives mentionnées au même alinéa sont, le cas échéant, fixées par décret»* n'est pas de nature à rassurer compte tenu de l'absence de décret qui a déjà pu être observée dans le champ du renseignement. Cette disposition questionne également sur le droit d'accès aux informations dès lors qu'il modifie l'article 49

de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin de rendre inapplicable le droit d'accès de la personne concernée par un traitement de données personnelles entrant dans le champ du règlement (UE) 2016/679 du 27 avril 2016 (« RGPD ») à l'information selon laquelle des renseignements ont été transmis par les autorités administratives responsables de ces traitements aux services de renseignement. Si le Conseil d'Etat dans son avis ne s'émeut nullement de cette inapplication du droit d'accès, considérant que *« la cohérence du dispositif »* justifie de l'écarter ainsi que l'objectif de la sécurité nationale, il ne répond nullement à la question qui peut également se poser de disposer éventuellement de la connaissance de ces transmissions *a posteriori* et d'une réouverture du droit d'accès par la suite. Enfin, cette disposition ne comprend nullement de définitions des autorités concernées. L'on peut alors s'interroger sur le fait que cela puisse concerner par exemple les services sociaux ou encore d'autres autorités en lien direct avec des usagers, ces derniers n'ayant alors aucun élément sur le contenu et la destination des informations qu'ils communiquent.

La CNIL de son côté questionne également dans son avis cette disposition s'interrogeant notamment 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. Elle rappelle en outre que de de telles transmissions devront être précisées et encadrées par voie réglementaire, ainsi que le prévoit déjà l'article L. 863-2 du CSI et 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 CNIL 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.

Le Syndicat de la magistrature s'oppose ainsi fermement à cette disposition extrêmement vague, ne posant aucune condition à la nature des informations susceptibles d'être transmises. Avec l'article 6 de la loi, ces dispositions font sauter les digues relatives aux secrets particulièrement protégés, notamment le secret médical.

Article 8

Une augmentation de la durée de conservation des renseignements pour les besoins de la recherche et du développement qui questionne quant aux modalités de stockage et à sa durée

L'article L. 822-2 du CSI dispose que les renseignements collectés par la mise en œuvre d'une technique de recueil de renseignement sont détruits à l'issue d'une durée de :

1° Trente jours à compter de leur recueil pour les correspondances interceptées en application des articles L. 852-1 (interceptions de sécurité) et L. 852-2 (surveillance en temps réel de toutes les données de connexion d'une personne susceptible d'être une menace) et pour les paroles captées en application de l'article L. 853-1 (sonorisation et captation d'images et de données informatiques) ;

2° Cent vingt jours à compter de leur recueil pour les renseignements collectés par la mise en œuvre des techniques mentionnées au chapitre III du titre V du présent livre, à l'exception des informations ou documents mentionnés à l'article L. 851-1 . (Cela vise la sonorisation et captation d'images et de données informatiques) ;

3° Quatre ans à compter de leur recueil pour les informations ou documents mentionnés à l'article L. 851-1 (à savoir le recueil des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications).

Pour ceux des renseignements qui sont chiffrés, le délai court à compter de leur déchiffrement. Ils ne peuvent être conservés plus de six ans à compter de leur recueil.

Dans une mesure strictement nécessaire aux besoins de l'analyse technique et à l'exclusion de toute utilisation pour la surveillance des personnes concernées, les renseignements collectés qui contiennent des éléments de cyberattaque ou qui sont chiffrés, ainsi que les renseignements déchiffrés associés à ces derniers, peuvent être conservés au-delà des durées mentionnées au présent I (soit au-delà de 30 jours, 120 jours, 4 ans et 6 ans).

L'article 8 du projet de loi vise à instaurer un régime autonome de conservation de renseignements pour les seuls besoins de la recherche et du développement en matière de capacités techniques de recueil et d'exploitation des renseignements. Il est argumenté en faveur de cette disposition qu'il est indispensable pour les services de renseignement de disposer d'un stock important de données, captées par telle ou telle technique de renseignement, leur permettant d'acquérir des connaissances suffisantes pour développer, améliorer et valider ces capacités.

Le nouveau III de l'article L. 822-2 permet donc une conservation de renseignements au-delà de la durée normalement applicable, dans la mesure - est-il dit - strictement nécessaire à ces travaux de recherche et de développement et à l'exclusion de toute utilisation pour la surveillance des personnes concernées, sous réserve que ces renseignements soient expurgés des motifs et des finalités ayant justifié leur recueil et conservés dans des conditions ne permettant pas de rechercher l'identité des personnes concernées.

À cette fin, les paramètres techniques applicables à chaque programme de recherche destinés à garantir le respect de ces conditions sont préalablement soumis à une autorisation préalable du Premier ministre, délivrée après avis de la CNCTR. Ces renseignements sont, en outre, uniquement accessibles aux agents spécialement habilités à cet effet et exclusivement affectés à cette mission puis détruits dès qu'ils ne sont plus utiles aux besoins précités et au plus tard cinq ans après leur recueil. Le II de l'article 11 prévoit que le service du Premier ministre qui assure la centralisation de certains renseignements collectés par les services de

renseignements pourra également les conserver, aux mêmes fins et dans les mêmes conditions, après accord des services à l'origine de leur recueil.

L'étude d'impact précise que : *« La mise en œuvre des techniques de renseignement et le travail de transcription et d'extraction des renseignements pertinents nécessitent le recours à des dispositifs techniques ou informatiques particuliers. L'amélioration de ces dispositifs de collecte, d'extraction ou de transcription requiert souvent un travail de recherche et de développement conduit sur des données étroitement comparables à celles qui sont collectées via les techniques de renseignement : traitement d'enregistrement vocaux opérationnels, couverts volontairement ou non par des bruits de fond, d'images captées par un dispositif vidéo camouflé par exemple. Or, les modèles d'apprentissage ont besoin de données pour s'entraîner avant d'être confrontés à des données inconnues. Plus les réseaux de neurones qui constituent ces modèles d'apprentissage disposent de données pertinentes, c'est-à-dire aussi proches que possible de celles obtenues dans un contexte opérationnel, pour apprendre, plus ils sont performants et précis, la quantité de données nécessaires à leur entraînement étant directement proportionnelle à la complexité du problème à résoudre. Ceci s'applique au traitement de l'image, de la parole, du texte, ou bien d'autres types de données plus ou moins structurées et hétérogènes, extraction des informations d'intérêt telles qu'un son, une conversation dans un environnement bruyant, l'accélération du traitement de la vidéo par l'élimination ou sélection de scènes sur requête sémantique. »*

Si cet article vise à permettre une avancée de la recherche et développement en conservant plus longtemps un ensemble de données, la limite étant alors de 5 ans et cette conservation étant 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, cela signifie toutefois que, de fait, les extractions de données vont devoir être conservées pendant cette durée, donc stockées quelque part et rester exploitables, ce qui questionne sur la possibilité de les utiliser également pour faire de la surveillance indirecte. La durée de 5 ans paraît en conséquence excessive au vu des risques encourus. Le Conseil d'Etat s'est inquiété lui-même du stockage de ces données dans son avis, estimant que cela devait faire l'objet d'un stockage *« matériellement et informatiquement cloisonné »* afin d'éviter *« tout risque de détournement à des fins de surveillance »*.

Outre, la question de la conservation de ces données, le principe même de la validation de la conservation massive de données à des fins de recherche et de développement pose difficulté sur le fond. Ceci d'autant plus que le mécanisme de contrôle prévu paraît largement insuffisant, la CNCTR ayant uniquement la possibilité d'adresser une recommandation au Premier ministre tendant à la suspension d'un programme de recherche quand elle estime qu'il ne respecte plus les conditions posées dans le texte.

La possibilité prévue au II de l'article 11 que le service du Premier ministre assure la centralisation de certains renseignements collectés par les services de renseignements puisse également les conserver, aux mêmes fins et dans les mêmes conditions, après accord des services à l'origine de leur recueil, interroge fortement sur l'objectif d'une telle conservation sous des délais excessifs, la recherche et développement ne pouvant alors être utilisés comme argument pour justifier ultérieurement que de telles données, conservées, soient ressorties et réutilisées.

La CNIL partage ces interrogations dans son avis soulignant que le régime de réutilisation des données, dans son ensemble, devrait être encadré par un décret d'application et que des garanties complémentaires devraient être prévues dans l'hypothèse où cette recherche serait mise en œuvre au moyen d'un traitement algorithmique.

Article 9

Un alignement à la hausse de la durée d'autorisation de la technique de recueil de données informatiques sur celle de la technique de captation des données informatiques

L'article L. 853-2 du CSI prévoit que peut être admise, lorsque les renseignements ne peuvent être recueillis par un autre moyen légalement autorisé, l'utilisation de dispositifs techniques permettant :

1° D'accéder à des données informatiques stockées dans un système informatique, de les enregistrer, de les conserver et de les transmettre pour une durée maximum de 30 jours ;

2° D'accéder à des données informatiques, de les enregistrer, de les conserver et de les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données, telles qu'il les y introduit par saisie de caractères ou telles qu'elles sont reçues et émises par des périphériques, pour une durée maximum de deux mois.

Il est rendu compte à la Commission nationale de contrôle des techniques de renseignement de sa mise en œuvre. La commission peut à tout moment adresser une recommandation tendant à ce que cette opération soit interrompue et que les renseignements collectés soient détruits.

L'article 9 vise à modifier l'article L. 853-2 en alignant la durée maximum à deux mois pour les deux techniques.

Si cette modification a le mérite de placer sur le même régime l'exploitation des données stockées sur un périphérique informatique et celles réalisées par extraction du flux, cela aboutit cependant indéniablement à augmenter le temps d'exploitation possible des données informatiques stockées par un alignement vers le haut sur les 2 mois.

Un alignement vers le bas, compte tenu des enjeux en termes de protection de la vie privée eut été préférable.

Article 10

L'élargissement de la possibilité donnée au Premier ministre de requérir la coopération des opérateurs de communications électroniques pour la mise en œuvre de certaines techniques de renseignement en y ajoutant les recueils de données techniques de connexion par dispositifs de proximité dit « IMSI catcher » et les techniques de recueil et de captation de données informatiques

L'article 10 modifie l'article L. 871-6 du code de la sécurité intérieure pour compléter

la liste des techniques de renseignement pour lesquelles la coopération des opérateurs de communications électroniques peut être requise afin qu'ils réalisent sur leurs réseaux des opérations matérielles nécessaires à leur mise en œuvre et de garantir qu'elles ne porteront pas atteinte au fonctionnement et à la sécurité des réseaux, ni à la qualité du service rendu par les opérateurs.
L'article 10 ajoute au champ de cette disposition les techniques de recueil ou de captation des données informatiques, prévues à l'article L. 853-2 du code de la sécurité intérieure, qui peuvent être mise en œuvre de deux manières :

- soit par accès direct au support informatique concerné,

- soit par les réseaux des opérateurs de communications électroniques.

La seconde extension concerne la technique de renseignement visée à l'article L. 851-6 du même code, soit celle qui permet le recueil au moyen d'un appareil de type « IMSI–catcher » de données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés.

En 2015, le législateur avait limité les possibilités de réquisitions, pour les besoins des services de renseignement, à cinq techniques de renseignement :
− les demandes d'accès différé aux données de connexion, prévues à l'article L. 851-1 du CSI ;
− la technique de l'accès en temps réel aux données de connexion prévue par l'article L. 851-2 du CSI ;
− la technique de détection d'une menace terroriste sur la base de traitements automatisés, dite technique de l'algorithme, prévue par l'article L. 851-3 du CSI ;
- les géolocalisation en temps réel ;
− les interceptions de sécurité prévues à l'article L. 852-1 du CSI y compris par IMSI-catcher.

Ces opérations matérielles nécessaires à la mise en place de certaines techniques de recueil de renseignement ne sont faites que sur ordre du Premier ministre. Une fois l'autorisation donnée, les agents peuvent installer *« dans les locaux et installations »* des opérateurs, fournisseurs d'accès à internet et hébergeurs accessibles en France, les outils nécessaires à ces opérations de surveillance.

Le projet de loi ajoute à la liste précédente, d'autres outils :

- L. 851-6 : les IMSI catcher, pour le recueil des données de connexion
- L. 853-2 : le recueil des données informatiques et leur captation

Cette adjonction devrait permettre la possibilité pour les services d'installer des IMSI catcher, sur les stations de base des opérateurs ou bien dans les infrastructures d'un prestataire de services en ligne basé en France.

Le Syndicat de la magistrature a déjà pu dénoncer le procédé de l'IMSI catching qui est si intrusif qu'il n'a vocation à être utilisé qu'exceptionnellement dans le cadre de

procédures judiciaires concernant des infractions graves à la loi pénale de sorte que son utilisation dans le cadre du renseignement est extrêmement attentatoire aux libertés.

Si la question de l'IMSI catching est ici posée en lien avec l'introduction de la 5G qui – du fait que les identifiants des terminaux mobiles deviendront temporaires - va en quelque sorte rendre plus dépendants les services de renseignement des opérateurs de télécommunication (dès lors que seuls les opérateurs pourront faire le lien entre les identifiants temporaires) et vise ainsi à anticiper cette mise en place pour pouvoir continuer à utiliser de tels procédés d'investigations malgré la 5G, il n'en demeure pas moins que l'extension de cette technique en dehors du champ judiciaire est problématique en termes de libertés et de droit à la vie privée.

L'extension de l'IMSI catching pour le recueil de données de connexion et la possibilité de réquisitions pour le recueil de données informatiques et leur captation constituent ainsi une amplification continue de ces atteintes aux libertés fondées sur des critères très vagues, sans contrôle judiciaire et sans contrôle réel de la CNCTR notamment.

Le recueil de données informatiques et leur captation pose également un certain nombre de difficultés majeures dès lors qu'il s'agit d'un procédé visant à permettre d'entrer dans des systèmes et d'exploiter absolument toutes les données contenues dans un téléphone, un ordinateur ou même des serveurs. En outre, de nombreuses interrogations demeurent à la lecture du texte sur les opérateurs qui pourraient être concernés par de telles dispositions.

Le fait que le Conseil d'État n'ait pas jugé utile de se prononcer sur cet article nous semble très problématique, eu égard aux enjeux, notamment vis-à-vis des opérateurs de télécommunications. Ceux-ci pourront désormais être tenus de mettre en place des dispositifs de piratage informatique, procédés extrêmement intrusifs, sans pour autant que leurs clients n'en soient informés ni que le Conseil d'État estime que des enjeux en termes de libertés ne se posent ou nécessitent a minima un avis.

Article 11

L'expérimentation des interceptions de correspondances par voie satellitaire

L'article 11 autorise, à titre expérimental pour une durée de 4 ans, les services de renseignement à intercepter, par le biais d'un dispositif de captation de proximité, les correspondances transitant par la voie satellitaire. L'interception de ce type de communications représenterait selon l'exposé des motifs du texte un *« enjeu opérationnel majeur pour les services de renseignement, en raison du déploiement de nouvelles constellations satellitaires et du développement à venir d'une offre alternative de télécommunications de nature à concurrencer des opérateurs de communications électroniques traditionnels. »*

Ces nouvelles techniques aboutiraient à rendre inadapté le cadre légal car les réseaux en cours de déploiement seraient exploités par des opérateurs étrangers donc non atteignables par des réquisitions dans le cadre de la loi renseignement. Il est en outre évoqué l'instabilité des

communications satellitaires qui rendrait complexe un ciblage des interceptions au stade de la captation. Le dispositif vise donc à expérimenter un nouveau cas d'interception de correspondances par le biais d'un dispositif de proximité, restreint à certaines des finalités prévues à l'article L. 811-3 du code de la sécurité intérieure.

L'autorisation sera prévue pour une durée de 30 jours, renouvelable. La CNCTR disposera d'un accès permanent, complet, direct et immédiat aux opérations de transcription et d'extraction. Le nombre maximal d'autorisations d'interception est arrêté par le Premier ministre après avis de la CNCTR.

Le texte autorise donc l'usage « *d'un appareil ou d'un dispositif technique* » pour intercepter des correspondances émises ou reçues par la voie satellitaire, quand des raisons techniques ou de confidentialité (secret défense) font obstacle « *au concours des opérateurs* » de sorte qu'il existerait un principe de subsidiarité.

Cette possibilité sera ainsi ouverte pour certaines des finalités prévues par le code :

- L'indépendance nationale, l'intégrité du territoire et la défense nationale ;
- Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;
- La prévention du terrorisme ;
- La prévention de la criminalité et de la délinquance organisées.

Le Conseil d'Etat a estimé que l'étude d'impact n'était pas assez précise quant aux modalités d'évaluation de l'expérimentation ni sur les critères d'appréciation aux regards desquels elle sera jugée. Il propose notamment que parmi ces critères puissent figurer le nombre de communications interceptées sans rapport avec la cible visée ou encore l'évaluation précise des obstacles juridiques, techniques ou opérationnels ayant empêché le recours au régime des interceptions de sécurité de droit commun du I de l'article L. 852-1 et nécessité le recours au dispositif expérimental. Nous partageons ces remarques sur l'évaluation de l'expérimentation,en nous interrogeant par ailleurs sur le caractère véritablement expérimental de cette disposition au vu de sa durée : elle est prévue jusqu'au 31 juillet 2025, avec la fourniture d'un rapport d'évaluation 6 mois avant la fin de son effet..Il semblerait en outre plus pertinent que l'expérimentation puisse se faire dans un cadre judiciaire, plus protecteur.

La CNIL interroge de son côté le fait que ce type de technique de renseignement est susceptible de permettre la collecte systématique et automatique des données relatives à des personnes pouvant n'avoir aucun lien autre qu' une simple proximité géographique avec l'individu effectivement surveillé de sorte qu'elle *« invite le Gouvernement, lors de l'expérimentation, et si cela est techniquement réalisable, à mettre en œuvre de telles mesures de filtrage le plus en amont possible »*. En outre, elle insiste sur le fait que la loi pourrait préciser que l'utilisation effective de cette nouvelle technique ne sera possible que tant que l'utilité opérationnelle n'en sera pas démentie, parce que ce type de transmissions satellitaires ne connaîtrait pas le développement escompté, ou que les modalités techniques d'interception

s'avéreraient insatisfaisantes. Elle sollicite qu'un bilan intermédiaire soit réalisé et adressé au Parlement, dans les mêmes conditions que celui qui devra être effectué avant la fin de l'expérimentation. Elle souligne enfin que le bilan visé à l'article précité devra *« a minima porter sur un certain nombre de caractéristiques, notamment opérationnelles, relatives à cette technique »*. La CNIL incite plus particulièrement à quantifier le volume de données collectées, et notamment celles concernant des personnes ne faisant pas l'objet de l'autorisation. Elle estime par ailleurs que des éléments quantitatifs sur l'efficience de cette technique, ainsi que la durée de l'utilisation de ces dispositifs de captation, devront également figurer dans le bilan remis au Parlement.

Outre que ce texte apparait ainsi insuffisamment cadrant, il est indiqué que les correspondances interceptées seront détruites dès qu'il apparaît qu'elles sont sans lien avec la personne concernée par l'autorisation et au plus tard au terme du délai prévu à l'article L. 822-2 1° du I soit 30 jours. Pourtant, rien ne détermine de façon précise ce que le critère de l'absence de lien comprend. En outre, les finalités prévues pour permettre l'utilisation de cette expérimentation sont extrêmement larges et permettent de recouvrir une part majeure des situations visées par les demandes de renseignements. La fixation d'un nombre maximal d'autorisations d'interceptions n'est pas non plus suffisamment protectrice, cette décision étant du seul ressort du Premier ministre sans avis de la CNCTR qui est seulement informée.

Article 12

La pérennisation des boîtes noires

L'article 12 de ce projet de loi a pour objet de pérenniser cette technique de renseignements en abrogeant l'article 25 de la loi du 24 juillet 2015 qui avait fixé une durée limitée à l'utilisation de cette technique.

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 le 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.

L'exposé des motifs explique que *« la pérennisation de ce dispositif se justifie ainsi, en premier lieu, par sa pertinence opérationnelle, cette capacité de détection ne pouvant être remplie par aucun des moyens traditionnels des services de renseignement »*. Il est estimé par ailleurs que cette technique est entourée de garanties « spécifiques et substantielles » à savoir le fait que les traitements automatisés ne peuvent recueillir d'autres données que celles répondant à leurs paramètres de conception ni ne peuvent, par eux-mêmes, permettre l'identification des personnes auxquelles les données traitées se rapportent. Enfin, il est précisé que le fait que la mise en œuvre repose sur une double autorisation, du Premier ministre, précédée d'un avis de la CNCTR est suffisant.

S'agissant de la pérennisation, le Conseil d'Etat considère que le projet prévoyant que seuls les services de renseignement du premier cercle pourront demander à mettre en œuvre des algorithmes et 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 ainsi que la suppression de la possibilité de conserver les données exploitées dans le cadre d'une identification faisant suite à un signalement au-delà de soixante jours, apportent assez de garanties pour encadrer ce dispositif.

La CNIL de son côté rappelle 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. »*

Elle 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 modifiée dans la mesure où ces données sont susceptibles de permettre l'identification des personnes. Elle ajoute 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 et que 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 nuit notamment à l'efficacité opérationnelle du dispositif et peut entraîner des conséquences dommageables pour les personnes concernées.

Ainsi, pendant que les interceptions dans le cadre judiciaire, pourtant plus protecteur, sont actuellement l'objet, dans le cadre du projet de loi « confiance » dans la justice, d'une réforme

tendant à en exclure totalement les données liées à l'activité d'avocat, les services de renseignement auraient de leur côté carte blanche pour traiter de manière indifférenciée la masse des données numériques. Il apparaît donc que le gouvernement considère qu'il est plus légitime de faire confiance à lui-même, ou à l'administration de manière générale, qu'à la justice. Ce constat inquiétant au regard du principe de séparation des pouvoirs n'en est pas moins réel.

La CNIL recommande donc que la rédaction du projet de loi explicite clairement qu'il rentre dans l'office de la CNCTR de vérifier l'existence de cette menace de nature terroriste. Un tel contrôle devant 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, d'après la CJUE.

La CNIL relève en outre que l'expérimentation dont il est envisagé la pérennisation porte sur deux types de données (traitement des données de téléphonie et connexions sur Internet) 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. Elle ajoute que 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. Pourtant, par la suite, 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.

Si 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, la CNIL de son côté formule des observations :

- que l'article L. 851-3 du CSI soit précisé pour appréhender de manière claire et précise les évolutions envisagées et la manière dont cette technique de renseignement sera mise en œuvre (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 notamment) ;

- qu'il est 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. Le fait que ces données sont conservées sous forme pseudonyme pour une durée de vingt-quatre heures avant d'être détruites devrait expressément figurer dans le projet de loi, qui devrait également préciser les modalités de recueil et d'accès à ces données.

Du point de vue du Syndicat de la magistrature, ce texte en pérennisant les boîtes noires accentue et perpétue les capacités de surveillance généralisée des services de renseignement et des prestataires privés chargés de la mise en œuvre de la technique. Confirmer dans le temps l'utilisation d'algorithmes pour passer au tamis l'ensemble des flux internet, contenus et données de connexion est d'autant plus inquiétant que le cadre fixé est insuffisamment protecteur. Non seulement les conditions du contrôle *a priori* pêchent par leur faiblesse, mais les conditions de recours à ces techniques sont loin d'être restrictives. Ces articles contreviennent ainsi au principe de proportionnalité. Le Syndicat de la magistrature rappelle son opposition à ces formes de surveillance généralisée et partage les inquiétudes formulées et détaillées par la CNIL.

Article 13 et 14

L'extension aux adresses complètes de ressources sur internet pour le recueil de données en temps réel et le recueil au moyen d'un traitement algorithmique

Les articles 13 et 14 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).

L'article 13 décline les modalités de pérennisation de ce dispositif au sein de l'article L. 851-3. Désormais, tous les types d'URL sont inclus parmi les données pouvant faire l'objet des traitements automatisés prévus par l'article L. 851-3. Il peut s'agir, comme la loi le permet aujourd'hui, des données permettant l'accès des équipements terminaux aux services de communication au public en ligne qui relèvent, par nature, de la catégorie des données de connexion ; il peut également s'agir des « adresses complètes de ressources sur internet » pouvant faire référence au contenu des informations consultées.

L'article 14 procède à l'inclusion des adresses complètes de ressources sur internet utilisées par une personne, dans le champ des données pouvant faire l'objet d'une détection en temps réel sur les réseaux de communications électroniques, au titre de la technique prévue à l'article L. 851-2 du code de la sécurité intérieure.
Cette détection est effectuée pour les seuls besoins de la prévention du terrorisme, à l'encontre de personnes préalablement identifiées comme étant susceptibles d'être en lien avec une menace terroriste, ou de personnes de leur entourage lorsqu'il existe des raisons sérieuses de penser qu'elles « *sont susceptibles de fournir des informations* » en relation avec la menace.

Cette technique est autorisée pour une durée de quatre mois renouvelable. Par voie de conséquence, la durée de conservation des URL recueillies au moyen de la technique de détection en temps réel (article L. 851-2) est alignée sur celle fixée au 2° de l'article L. 822-2 (120 jours) déjà applicable à des données de même nature.

Il est selon l'exposé des motifs *« déterminant que les traitements automatisés prévus à l'article L. 851-3 puissent également s'appliquer à ce type d'URL pour que soient détectées les consultations d'informations présentant un lien avéré avec les activités terroristes et, in fine, après autorisation, pour que soient identifiés les individus à l'origine de ces connexions ».*

Dans le détail, il est argumenté sur le fait que :
- la mise en œuvre des traitements ne pourra plus être sollicitée que par les seuls services spécialisés de renseignement,

- la possibilité de proroger la durée de conservation (de 60 jours au départ jusqu'à 4 ans en cas d'éléments sérieux confirmant l'existence d'une menace terroriste) des données correspondant aux paramètres de détection et dont le Premier ministre autorise le recueil est supprimée,

- la mission d'exécuter les traitements automatisés sera exclusivement confiée à un service du Premier ministre, le groupement interministériel de contrôle, service à compétence nationale distinct des services de renseignement,

- les données qui ne sont pas susceptibles de révéler une menace terroriste sont par ailleurs immédiatement détruites.

Le Conseil d'État estime de son côté - tout comme la CNCTR - que les adresses complètes de ressources sur internet aux données sont assimilées aux « URL » (« *Uniform Ressource Locator* »), et revêtent la nature de données à caractère mixte dès lors qu'elles sont 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.

Il 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.

La CNIL rappelle que *« ces données ont une nature particulière »*, *« les URL sont susceptibles de faire apparaître des informations relatives au contenu des éléments consultés ou aux correspondances échangées* » devant faire l'objet d'une protection particulière.

Elle estime qu'il faudra procéder à une expérimentation permettant d'évaluer 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.

Du côté du Syndicat de la magistrature, 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, met en place un domaine nouveau d'investigation plus attentatoire à la protection de la vie privée et des données personnelles.

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*».

Il est donc permis de douter que l'inclusion des données traitées par les algorithmes aux adresses complètes internet puissent, de ce point de vue, être validées dans la mesure où elles portent potentiellement sur les informations consultées visées par le Conseil constitutionnel.

Le Syndicat de la magistrature qui a déjà dénoncé le recours à la technique du IMSI catching dès 2015 considère que 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 renforce les risques de surveillance généralisée et ne peut être acceptée.

Le projet de loi aboutit au final à la fois à une pérennisation de ces techniques mais également à une extension des données pouvant faire l'objet de cette technique de surveillance sans pour autant qu'un réel contrôle sur l'expérimentation ait pu être fait et que les enjeux d'une telle extension soient suffisamment connus et contrôlés.

Article 15

De nouvelles règles en matière de conservation des données

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.

La décision *French Data Network et autres* dispose 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).

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).

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 pour les besoins de la lutte contre la criminalité grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale ;

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, 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.

Le Conseil d'État dans son avis 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. Il 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.

La CNIL dans son avis 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 note 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. 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. 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), elle estime que le projet de loi devrait préciser les finalités premières pour lesquelles ces données devraient être conservées par les opérateurs.

S'agissant de l'hypothèse selon laquelle *«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 »,* la CNIL estime que dans la mesure où le principe même de la conservation de données de trafic et de localisation constitue une atteinte à la vie privée, l'injonction du Premier ministre imposant aux opérateurs la conservation de ces données devrait être soumise pour avis à la CNCTR.

S'agissant de la conservation dite rapide qui pourrait 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, la CNIL 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 CNIL 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.

Le Syndicat de la magistrature relève que les critères de la *« menace grave, actuelle ou prévisible pour la sécurité nationale »* sont trop imprécis pour permettre au Premier ministre

d'enjoindre aux opérateurs de communications électroniques de conserver certaines catégories de données. Le même constat peut être fait s'agissant des *« besoins de la lutte contre la criminalité grave »* dont les contours en matière d'infractions concernées sont très flous et nécessitent des précisions. En outre, nous notons que la durée d'application du décret, d'un an, semble excessive au vu des enjeux. Par ailleurs, l'absence d'intervention de la CNCTR sur ce point, qui n'émet même pas d'avis est problématique. Enfin, une question demeure sur les possibilités et conséquences pour les opérateurs de communications électroniques du refus de communiquer ces informations et sur l'information auprès des usagers de telles possibilités afin qu'ils puissent consentir de façon éclairée à la transmission de telles données en recourant à ces opérateurs.

Article 16

Le contrôle préalable par une juridiction ou une autorité indépendante

L'article 16 tire également les conséquences des décisions précitées de la Cour de justice de l'Union européenne et du Conseil d'État, selon lesquelles la mise en œuvre des techniques de renseignement prévues aux articles L. 851-1 à L. 851-4 doit, sauf cas d'urgence dûment justifiée, être subordonnée à un contrôle préalable par une juridiction ou une autorité indépendante dont la décision est dotée d'un effet contraignant.

Cet article modifie donc les dispositions de l'article L. 821-1 du code de la sécurité intérieure pour étendre à toute technique de renseignement autorisée après avis défavorable de la commission nationale de contrôle des techniques de renseignement le mécanisme, actuellement prévu au III de l'article L. 853-3 du code de la sécurité intérieure en ce qui concerne l'introduction dans un lieu privé à usage d'habitation, de saisine obligatoire de la formation spécialisée du Conseil d'État par la commission. La formation spécialisée du Conseil d'État dispose alors d'un délai de vingt-quatre heures pour statuer, délai pendant lequel la technique de renseignement en cause ne peut pas être mise en œuvre.

Toutefois, en cas d'urgence dûment justifiée et si le Premier ministre a ordonné la mise en œuvre immédiate de la technique ainsi autorisée, il est possible de passer outre ce caractère suspensif. Cette faculté n'est en revanche pas possible s'agissant des autorisations délivrées pour la mise en œuvre de la technique de l'algorithme, en application des I et II de l'article L. 851-3 du code de la sécurité intérieure, ou concernant des personnes exerçant les professions protégées mentionnées à l'article L. 821-7. Elle par ailleurs est limitée aux seules finalités prévues aux 1°, 4° ou a) du 5° de l'article L. 811-3, s'agissant de la mise en œuvre des techniques de recueil de renseignement prévues aux articles L. 853-1, L. 853-2 et L. 853-3, seule la finalité de prévention du terrorisme justifiant cette procédure lorsque l'introduction dans un lieu privé concerne une habitation.

Compte tenu de la création de cette nouvelle procédure d'urgence, la procédure d'urgence absolue prévue à l'article L. 821-5 du code de la sécurité intérieure est supprimée.

Le Conseil d'État n'a pas émis d'observation sur cet article.

La CNIL de son côté, 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 ou le président de celle-ci 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 s'il a précédemment précisé qu'il avait ordonné la mise en œuvre immédiate de la technique de renseignement. La CNIL 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.

En troisième lieu, le projet de loi abroge l'article L. 821-5 du CSI qui prévoit que dans certaines situations d'urgence absolue 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. 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. 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) 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. La CNIL 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 CNIL 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.

Le Syndicat de la magistrature est favorable dans le principe à ce nouvel article et notamment à l'abrogation de l'article L 821-5 du CSI, qui ne va cependant pas assez loin. Nous en déplorons les modalités et notamment les exceptions au principe d'un contrôle par le Conseil d'Etat. Ainsi, le fait de maintenir une exception et notamment que le nouveau dispositif permette 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 en cas d'urgence dûment justifiée, est très problématique. Si le projet de loi prévoit 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) concernant la sonorisation de certains lieux et véhicules ainsi que la captation d'images et de données informatiques et si 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, il n'en demeure pas moins que le projet de loi ne prévoit pas de limitation particulière quant aux conditions dans lesquelles l'urgence pourrait être utilisée. Par ailleurs, l'absence de mise en œuvre d'un avis conforme de la CNCTR risque d'aboutir à ce que le champ des exceptions soit extrêmement utilisé en ayant notamment davantage recours à la demande de mise en œuvre immédiate notamment de la part du Premier ministre.

Nous déplorons par ailleurs le fait qu'aucun contrôle *a posteriori* de l'urgence justifiée et des conditions ayant justifié d'intervenir avant la décision du Conseil d'État ne soit prévue.

Article 17

La transmission par l'autorité judiciaire d'éléments de toute nature figurant dans les procédures judiciaires

L'article 17 qui introduit un nouvel article 706-105-1 au sein du chapitre II du titre XXV du livre IV du code de procédure pénale, étend, par dérogation à l'article 11 du code de procédure pénale, les possibilités de transmission par l'autorité judiciaire, d'éléments de toute nature figurant dans des procédures judiciaires, pour deux types de finalités : d'une part, l'autorité judiciaire peut transmettre à certains services visés à l'article L. 2321-2 du code de la défense, de sa propre initiative ou à la demande de ces services, des éléments nécessaires à l'exercice de leur mission en matière de sécurité et de défense des systèmes d'information ; d'autre part, elle peut également transmettre à certains des services de renseignement visés aux articles L. 811-2 et L. 811-4 du code de la sécurité intérieure, des éléments de toute nature figurant dans des procédures en matière de trafic de stupéfiants, traite des êtres humain, lutte contre les filières d'immigration clandestines ou en matière d'armes lorsque ces éléments sont nécessaires à l'exercice des missions des services concernés au titre de la prévention de la criminalité et de la délinquance organisées.

Ces transmissions sont assurées par le Procureur de la République de Paris, qui dispose d'une compétence territoriale spéciale dans ces deux matières. Si la procédure fait l'objet d'une information judiciaire, cette communication ne peut intervenir qu'avec l'avis favorable du juge d'instruction. Celui-ci peut également procéder à cette communication pour les procédures d'information dont il est saisi après avoir recueilli l'avis du procureur de la République de Paris. Les informations communiquées ne peuvent être transmises à des services étrangers ou à des organismes internationaux compétents dans le domaine du renseignement. Toute personne qui en est destinataire est tenue au secret professionnel.

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 Conseil d'État dans son avis considère que ces dispositions n'appellent pas d'avis de sa part s'agissant des affaires de cybercriminalité. En revanche, sur l'extension à la criminalité et la délinquance organisées de grande complexité, le Conseil d'Etat considère que 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 qu'outre les services du premier cercle, 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.

La CNIL de son côté estime que le périmètre infractionnel visé par le projet de loi apparaît très large. En outre, elle estime que le projet de loi devrait être précisé afin de mentionner expressément le caractère facultatif, pour les autorités judiciaires, de transmettre de telles données en indiquant qu'il revient à l'autorité judiciaire d'apprécier si cette transmission est de nature à nuire à la bonne administration de la justice. Elle s'interroge sur le fait que 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, se questionnant sur les raisons ayant conduit le ministère à étendre cette possibilité aux services dits du « second cercle ».

Le Syndicat de la magistrature rejoint ces interrogations quant au périmètre des infractions visées, le trafic de stupéfiants ainsi que les délits en matière d'armes semblant par

exemple extrêmement larges pour pouvoir être visés de façon respectueuses des droits des justiciables concernés.

Plus largement, le principe même selon lequel une des finalités justifiant l'intervention des services de renseignement est la lutte contre la criminalité organisée devrait poser question au législateur, au sens où cette lutte, définie par la référence à la commission d'infractions pénales, est intégralement de la compétence de l'autorité judiciaire. Aucune réflexion n'a été engagée sur la frontière, en cette matière, entre les cadres d'intervention des services relevant du ministère de l'intérieur (judiciaire ou administratif), la CNCTR étant finalement la seule à tracer la ligne entre ces champs, en considérant par exemple, à l'occasion d'un contrôle sur une technique de renseignement, que l'affaire devrait être judiciarisée en raison de la présence d'indices de la commission d'une infraction. Cette frontière est juridiquement ténue (du fait notamment de l'existence de l'infraction d'association de malfaiteurs, qui pourraient finalement conduire à judiciariser tous les dossiers actuellement traités par les services du renseignement). Ce qui est particulièrement problématique dans un Etat de droit, c'est que l'autorité judiciaire n'a aucune visibilité sur les affaires traitées par les services du renseignement, et aucun levier pour s'en saisir, alors même qu'elle est la gardienne de la liberté individuelle aux termes de la Constitution. On assiste ainsi à un double mouvement : des techniques de plus en plus intrusives peuvent être mises en oeuvre par les services du renseignement, s'apparentant à celles dont dispose l'autorité judiciaire pendant une enquête, mais sans aucune des garanties du code de procédure pénale. Il devient plus « confortable » pour les services relevant du ministère de l'Intérieur de travailler dans le cadre administratif, pour mener ce qu'il convient de considérer comme de véritables enquêtes, la seule question étant par la suite de « blanchir » les renseignements obtenus lorsque des éléments paraissent justifier des suites judiciaires. C'est cette évolution qui vient ici être parachevée par le principe selon lequel l'autorité judiciaire devrait aussi, lorsqu'une enquête est ouverte, donner ses propres informations à l'administration. Cette partie du projet de loi montre, comme d'autres, que les principes de l'Etat de droit ont été totalement perdus de vue. Il ne sera bientôt plus utile de s'interroger sur les équilibres de la procédure pénale, le contradictoire, l'accès au dossier, quand les services relevant du ministère de l'Intérieur travailleront principalement sous l'égide de ce code de procédure pénale bis que devient le code de la sécurité intérieure.

Nous partageons subsidiairement le constat fait par d'autres autorités que le caractère facultatif de transmission de ces renseignements doit être exprimé clairement du point de vue de l'autorité judiciaire.