Contribution extérieure auprès du Conseil Constitutionnel dans l'affaire n° 2021-822 DC

Loi relative à la prévention d'actes de terrorisme et au renseignement

Produite par l'association « La Quadrature du Net », le 27 juillet 2021

Monsieur le Président,

Mesdames et Messieurs les membres du Conseil constitutionnel,

Par la présente contribution extérieure, l'association La Quadrature du Net entend faire valoir les observations suivantes à l'encontre des dispositions de la loi « *relative à la prévention d'actes de terrorisme et au renseignement* ».

En raison des délais extrêmement courts laissés au Conseil constitutionnel pour se prononcer sur cette loi, dont les conséquences sont pourtant très importantes pour l'exercice des droits et libertés en France, cette contribution extérieure se limite à certaines dispositions du chapitre II de la loi « relatives au renseignement » dont l'inconstitutionnalité est manifeste, particulièrement en ce qu'elles visent à :

- pérenniser et étendre les traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste ainsi qu'à étendre la possibilité de recueil en temps réel de certaines données (**partie 1**, concernant les articles 14, 15 et 16, page 1) ;

- organiser la conservation généralisée des données de connexion par les opérateurs (**partie 2**, concernant l'article 17, page 7) ;

- étendre les obligations de coopération des fournisseurs de services de communications électroniques notamment aux usages d'IMSI catcher et au piratage informatique (**partie 3**, concernant l'article 12, page 10) ;

- allonger la durée de conservation des renseignements à des fins de recherche et de développement (**partie 4**, concernant l'article 10, page 13).

PARTIE 1. Sur la pérennisation et l'extension du recours aux algorithmes de surveillance ainsi que sur l'extension de la possibilité de recueil en temps réel de certaines données (Articles 14, 15 et 16)

Les articles 14 et 15 du projet de loi organisent la pérennisation et l'extension des dispositions prévues à l'article L. 851-3 du code de la sécurité intérieure encadrant le recours aux algorithmes de surveillance. L'article 16 organise l'extension de la possibilité de recueil en temps réel des données de connexion.

Ces articles constituent une atteinte disproportionnée au droit à la vie privée (a) et au secret des correspondances (b) ainsi qu'à l'article 34 de la Constitution (c).

a) Atteinte disproportionnée au droit à la vie privée

<u>En droit :</u>

Au titre notamment du droit au respect de la vie privée protégé par l'article 2 de la Déclaration de 1789, le Conseil constitutionnel a considéré que la « *collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* » (Cons. constit., n°2012-652 DC, 22 mars 2012).

Ce droit au respect de la vie privée est également inscrit aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, que le Conseil constitutionnel se doit de respecter au titre de l'article 88-1 de la Constitution. De manière générale, si le Conseil constitutionnel n'est pas tenu d'appliquer la jurisprudence de la Cour de Justice de l'Union européenne, il peut cependant utilement s'en inspirer afin de garantir un niveau de protection adapté aux droits et libertés constitutionnellement protégés.

Il est vrai que dans sa décision de 2015 sur la loi « relative au renseignement », le Conseil constitutionnel a considéré que le recours aux algorithmes ne constituait pas une atteinte disproportionnée au droit au respect de la vie privée (Cons. constit., n° n°2015-713 DC, § 60).

Néanmoins, depuis cette décision, la Cour de Justice de l'Union européenne a rendu une décision concernant notamment la compatibilité entre le droit de l'Union européenne et un dispositif de traitement automatisé des données relatives au trafic et des données de localisation (CJUE, C-511/18 et s., 6 octobre 2020). Elle y souligne notamment que le recours à l'analyse automatisée doit être limité « *à des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le recours à cette analyse pouvant faire l'objet d'un contrôle effectif* (...) » (CJUE, précité, § 192).

<u>En l'espèce</u> :

En premier lieu, alors que la loi de 2015 « relative au renseignement » ne permettait l'utilisation des algorithmes de surveillance qu'à titre expérimental, la loi examinée par le Conseil constitutionnel prévoit aujourd'hui la pérennisation de ce dispositif. La CNIL rappelle ainsi dans son avis sur le texte 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* » (CNIL, Délibération n°2021-040 du 8 avril 2021, § 24). Elle a souligné ne pas avoir pu analyser la proportionnalité de l'atteinte à la vie privée constituée par cette pérennisation (CNIL, idem, § 31).

En second lieu, aucune disposition ne vient répondre aux exigences de la Cour de Justice de l'Union européenne sur les limitations à apporter à l'utilisation des algorithmes de surveillance. Ainsi, l'article 14 ne mentionne aucune limitation du dispositif à l'existence d'une « *menace grave pour la sécurité nationale* » qui serait « *actuelle ou prévisible* ». Il ne prévoit encore moins aucun « contrôle effectif » d'une telle analyse. Le législateur n'a donc tiré aucune conséquence des récents arrêts de la Cour de Justice sur la question du recours aux algorithmes.

Il est particulièrement significatif que la loi déférée prévoit un régime spécifique pour la conservation des données de connexion, avec décision du Premier ministre relative à l'existence de « motifs tenant à la sauvegarde de la sécurité nationale », mais qu'aucun régime parallèle ne soit prévu pour le recours aux algorithmes.

Il en résulte que la pérennisation et l'extension du recours aux algorithmes prévues aux articles 14 et 15 de la loi déférée sont contraires à l'article 2 de la Déclaration de 1789 et à l'article 88-1 de la Constitution.

b) Atteinte disproportionnée au secret des correspondances

<u>En droit :</u>

Le Conseil constitutionnel a admis la valeur constitutionnelle du droit au secret des correspondances, rattaché aux articles 2 et 4 de la Déclaration de 1789 (Cons. constit., n°2004-492 DC, 2 mars 2004).

Dans sa décision de 2015 concernant la loi « relative au renseignement », il a conditionné la constitutionnalité des dispositions relatives au recours à l'algorithme au fait que, notamment, ces traitements ne pouvaient porter que sur des informations ou documents mentionnés à l'article L. 851-1 du CSI, c'est-à-dire des données dites de « connexion » ou « métadonnées » (Cons. constit., n°2015-713 DC, § 60). Dans cette même décision, le Conseil constitutionnel précise que les données faisant l'objet du traitement « *ne peuvent en aucun cas porter sur le contenu des*

correspondances échangées ou des informations consultées, sous quelque forme que ce soit » (Cons. constit., n°2015-713 DC, § 55).

À ce titre, si le Conseil constitutionnel a admis dans sa décision de 2015 certaines techniques de renseignement portant atteinte au secret du contenu des correspondances, il ne l'a fait qu'en raison de leur caractère ciblé, différent d'une surveillance généralisée (voir notamment Cons. constit., n°2015-713 DC, § 25).

En l'espèce :

Les articles 15 et 16 étendent le recours aux algorithmes et la possibilité de recueil en temps-réel des données de connexion aux « adresses complètes de ressources utilisées sur internet ».

Comme le rappelle la CNIL dans son avis sur le texte, ce type de données « *sont susceptibles de faire apparaître des informations relatives au contenu des éléments consultés ou aux correspondances échangées* » (CNIL, Délibération n°2021-040 du 8 avril 2021, § 35). Les « adresses complètes de ressources utilisées sur internet » peuvent, en effet, être extrêmement parlantes sur le contenu consulté par l'utilisateur, et indiquer par exemple le titre d'un article complet.

Dans son rapport sur le projet de loi, la commission des lois du Sénat rappelle ainsi qu'aussi bien la CNIL que la Commission nationale de contrôle des techniques de renseignement (CNCTR) ont, dans leur avis sur le projet de décret relatif aux techniques de renseignement « ***exclu la possibilité que la technique de l'algorithme puisse permettre un accès complet aux URL*** » du fait que les URL « *constituent des données mixtes, comprenant à la fois des données de connexion, c'est-à-dire des éléments relatifs à l'acheminement de la communication internet, et des données de communication, c'est-à-dire des éléments fournissant des précisions sur l'objet ou le contenu du site internet consulté* » (Commission des lois du Sénat, Rapport n°694 sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement, 16 juin 2021).

La commission des lois du Sénat y ajoute que, selon la Délégation Parlementaire au Renseignement (ci-après « DPR ») « *l'élargissement de la technique de l'algorithme souhaité par les services à l'analyse de la totalité des informations contenues dans les URL reviendrait, de fait,* ***à autoriser un traitement automatisé de données révélant, pour partie, le contenu de communications*** ». En effet, elle précise que si le Conseil constitutionnel n'interdit pas par principe que des services du renseignement accèdent au contenu des communications, cela n'a été autorisé pour l'instant que pour une collecte individualisée et non pour « *un traitement en masse des données de communication* » (Commission des lois du Sénat, Rapport sur le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement n° 694, 16 juin 2021).

Il en résulte que les articles 15 et 16 autorisent la surveillance en masse de données portant sur le contenu des correspondances, en contradiction avec le secret des correspondances protégées par la Constitution.

c) Incompétence négative du législateur

En droit :

Il ressort de l'article 34 de la Constitution que la loi fixe les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques.

Dans sa décision de 2015 sur la loi « relative au renseignement », le Conseil constitutionnel a ainsi considéré qu'il y avait eu violation de l'article 34 du fait de l'absence de définition dans la loi des « *conditions d'exploitation, de conservation et de destruction des renseignements collectés en application de l'article L. 854-1* » en matière de surveillance internationale. Le législateur n'avait ainsi pas déterminé « *les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » (Cons. constit., n°2015-713 DC, § 78).

En l'espèce :

L'article 15 la loi déférée modifie l'article L851-3 du CSI. Désormais, cet article ne prévoit plus que « *peut être imposé aux opérateurs [...] la mise en œuvre sur leurs réseaux* » du dispositif de détection automatisée, mais que ce dispositif sera désormais directement mis en œuvre par les services de renseignement « *sur les données transitant par les réseaux des opérateurs* ». Cette modification implique une architecture radicalement différentes que la loi échoue entièrement à décrire et à encadrer.

En effet, dans son avis sur le texte, la CNIL précise que « *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'État pour être soumis à des dispositifs de détection centralisés* ». Elle considère ainsi que cela implique de « *dupliquer, au bénéfice d'un service administratif du Premier ministre, l'ensemble de ces données, qui concernent tous les appels téléphoniques et accès internet réalisés sur le territoire français, constitue une évolution particulièrement significative* » (CNIL, Délibération n°2021-040 du 8 avril 2021, § 16 et s.).

À ce titre, la CNIL considère donc « *indispensable que le texte soit précisé* » sur ce sujet et que le principe de cette architecture « *devrait (...) figurer dans la loi* » (idem).

Cette architecture facilite en effet grandement la surveillance réalisée par les services de renseignement et est susceptible d'être dévoyée à d'autres fins que celles définies par le texte, et ce d'autant plus que les dispositifs de l'article 10 de cette même loi permettent *de facto* de conserver les données analysées par l'algorithme pour la recherche et développement pendant 5 ans. Cela pourrait

potentiellement être l'intégralité du trafic internet qui peut donc se retrouver dupliqué et mis de côté par les services de renseignement.

La loi déférée n'apporte aucune précision sur les modalités de mise en œuvre de la technique de recours aux algorithmes ni sur l'architecture précise du traitement automatisé. Le législateur n'a donc pas précisé les conditions réelles de collecte, d'exploitation et de conservation des renseignements lié à la particularité de la duplication et de la centralisation des données de connexion concernant potentiellement l'ensemble des personnes vivant en France.

Il en résulte que l'article 15 est en contradiction avec l'article 34 de la Constitution.

PARTIE 2. Sur l'organisation de la conservation des données de connexion par les opérateurs (Article 17)

L'article 17 refond le cadre de conservation généralisée des données de connexion par les opérateurs en réaction à la décision de la Cour de Justice de l'Union européenne du 6 octobre 2020.

Il constitue une atteinte disproportionnée aussi bien au droit à la vie privée protégé par l'article 2 de la Déclaration de 1789 qu'à l'article 88-1 de la Constitution en ce qu'il représente une violation directe du droit de l'Union européenne tel qu'interprété par la Cour de Justice de l'Union européenne.

<u>En droit :</u>

Comme vu précédemment, le Conseil constitutionnel a reconnu que la collecte, l'enregistrement et la conservation de données personnelles étaient constitutives d'une atteinte à la vie privée et devaient donc être justifiées par un motif d'intérêt général et proportionné à cet objectif (Cons. constit., n°2012-652 DC, 22 mars 2012).

La Cour de justice de l'Union européenne rappelle de façon constante que [les données de connexion] « s*ont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées (...). [qui] peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées (...). En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications* » (*Digital Rights*, 8 avril 2014, C-293/12 et C-594/12, § 27*;Tele2*, 21 décembre 2016, C-203/15 et C-698/15, § 99 ; *La Quadrature du Ne*t, 6 octobre 2020, C-511/18 et s., § 117).

Dans sa décision du 6 octobre 2020 « La Quadrature du Net », la Cour de Justice de l'Union européenne définit les limitations et garanties permettant aux régimes de conservation généralisée des données de connexion de se conformer aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne et à l'article 15 paragraphe 1 de la directive 2002/58 (CJUE, C-511/18 et s., 6 octobre 2020). Il convient à ce titre de rappeler que l'article 88-1 de la Constitution impose au législateur de respecter le droit de l'Union européenne.

Dans cette décision, la Cour de Justice de l'Union européenne a réaffirmé sa jurisprudence selon laquelle le droit de l'Union européenne s'opposait « *à des mesures législatives prévoyant (...) à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation* ».

À titre exceptionnel, et étant mis de côté les cas particuliers des données relatives à l'état civil et des adresses IP, la Cour de Justice a considéré que seul était permis « l*e* ***recours à une injonction*** *faite*

aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à ***une menace grave pour la sécurité nationale*** *qui s'avère* ***réelle et actuelle ou prévisible*** », précision étant faite que cette décision doit pouvoir faire l'objet d'un contrôle effectif : « *soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant (...)* » (CJUE, La Quadrature du Net, 6 octobre 2020, § 168). La Cour insiste bien sur le fait que « *cette conservation ne saurait présenter un caractère systématique* » (même arrêt, § 138).

Il en résulte qu'une conservation généralisée des données de connexion n'est possible qu'à travers une injonction spécifique limitée dans le temps adressée à des opérateurs dans le cas d'une menace grave pour la sécurité nationale d'un État et soumise au contrôle effectif d'une autorité dont la décision est dotée d'un effet contraignant.

<u>En l'espèce :</u>

Il est précisé au 3° du I de l'article 17 que le Premier ministre peut enjoindre « *pour des motifs tenant à la sauvegarde de la sécurité nationale* », quand il a constaté « *une menace grave, actuelle ou prévisible* », « *par décret aux opérateurs (...) de conserver pendant une durée d'un an* » certaines données de connexion.

Ce régime d'organisation de conservation des données de connexion ne respecte aucune des garanties–imposées par la Cour de Justice de l'Union européenne, aussi bien sur la nature de l'injonction (1), sur les motifs tenant à la sauvegarde de la sécurité nationale (2) que sur l'absence de contrôle effectif (3).

1. Sur la nature de l'injonction

Le fait que le Premier ministre puisse enjoindre cette conservation des données par un décret ne remplit pas les conditions exigées par la Cour de Justice de l'Union européenne. En effet, un acte administratif réglementaire ne saurait constituer une injonction : cette dernière doit nécessairement être spécifique et ne peut prendre la forme que d'un acte individuel. De plus, la durée d'un an prévue pour l'application du décret est excessive au regard de la nécessité de circonscrire cette collecte au strict nécessaire, d'autant qu'aucune limite du nombre de reconduction n'est prévue dans la loi, permettant alors un caractère systématique de la collecte des données de connexion.

2. Sur les motifs tenant à la sauvegarde de la sécurité nationale

La notion de sécurité nationale telle qu'interprétée par le Conseil d'État et à laquelle renvoie la loi déférée ne correspond en aucun cas à celle, restreinte et devant répondre à un critère d'exception, retenue par la Cour de Justice de l'Union européenne comme pouvant seule légitimer la conservation généralisée et indifférenciée des données de connexion.

En effet, la notion de sécurité nationale telle qu'entendue en droit français doit aujourd'hui, selon le Conseil d'État « *être appréciée au regard de l'ensemble des intérêts fondamentaux de la Nation listés à l'article L. 811-3 du code de la sécurité intérieure* », notion extrêmement large concernant notamment « *les intérêts majeurs de la politique étrangère* », les « *intérêts économiques, industriels et scientifiques majeurs de la France* » ou les risques tenant aux « *violences collectives* » que le Conseil constitutionnel a notamment rattaché, dans sa décision sur la loi renseignement de 2015, à l'organisation de manifestation non déclarées. Ainsi, dans sa récente décision, le Conseil d'État souligne ainsi que la menace pour la sécurité nationale n'est pas seulement liée au risque terroriste mais aussi au « *risque d'espionnage et d'ingérence étrangère* », à « *l'activité de groupes radicaux* » (Conseil d'État, 21 avril 2021, n° 393099 et s., § 44)

Une telle notion est donc très éloignée de la notion de menace grave pour la sécurité nationale telle qu'entendue par la Cour de Justice de l'Union européenne, qui ciblait spécifiquement « *des activités de terrorisme* », et ce dans les seuls cas où ces activités représenteraient une menace réelle et immédiate. Il revenait donc au législateur de limiter la conservation généralisée des données de connexion à des situations beaucoup plus restreintes, exceptionnelles et proportionnées que celles dégagées par le Conseil d'État autour de son interprétation dévoyée de la notion de sécurité nationale.

3. Sur l'absence de contrôle effectif

Le dispositif tel que prévu par le législateur ne prévoit pas de contrôle effectif répondant aux exigences de la Cour de Justice de l'Union européenne.

Aucun contrôle de la CNCTR n'est prévu sur l'injonction du Premier ministre, alors que cette institution est un des maillons essentiel de la chaîne opérationnelle encadrant le recueil des renseignements. C'est d'ailleurs un des regrets exprimé par la CNIL dans son avis sur le projet de loi qui considère que l'injonction du Premier ministre « *devrait être soumis pour avis à la CNCTR* » (CNIL, Délibération n° 2021-053, § 16).

Le seul contrôle possible de la conservation généralisée des données de connexion n'est finalement pas dans la loi, mais est dévolu à la potentialité du recours à un juge. Comme le rappelle la commission des lois du Sénat, ce contrôle correspondrait en *réalité à la possibilité que le Conseil d'État soit « éventuellement saisi en référé du décret du Premier ministre* » (Commission des lois du Sénat, Rapport n°694 sur le projet de loi du « relatif à la prévention d'actes de terrorisme et au renseignement, 16 juin 2021). Il ne s'agit en aucun cas d'un contrôle effectif tel que demandé par la Cour de Justice de l'Union européenne mais d'un contrôle dépendant de la volonté de possible requérants qui ne pourrait être réalisé qu'a posteriori, soit une fois que la mesure portant atteinte à la vie privée ait été réalisée.

Il en résulte que l'article 17 de la loi déférée ne respecte pas les articles 2 de la Déclaration de 1789 et 88-1 de la Constitution.

PARTIE 3. Sur l'extension des obligations de coopération des opérateurs de communications électroniques et des fournisseurs de services (Article 12)

L'article 12 prévoit la coopération forcée des opérateurs et fournisseurs de communications électroniques avec les services de renseignement afin de mettre en œuvre des techniques d'intrusion informatique directement sur des terminaux.

En droit :

Le Conseil constitutionnel censure depuis longtemps l'incompétence négative du législateur (cf. Cons. constit., 26 janv. 1967, *Loi organique modifiant l'ordonnance du 22 décembre 1958*, 67-31 DC), même d'office lorsque les auteurs de la saisine ne l'ont pas invoqué (cf. Cons. constit., 20 janv. 1984, *Loi relative à l'enseignement supérieur*, 83-165 DC). Le Conseil constitutionnel analyse ainsi régulièrement la méconnaissance, par le législateur, de l'étendue de sa propre compétence en lien avec le principe de clarté de la loi, d'une part, et l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi, d'autre part (voir notamment Conseil constit., 12 août 2004, *Loi relative aux libertés et responsabilités locales*, 2004-503 DC, cons. 29).

Précisément, le commentaire autorisé du Conseil constitutionnel sous la décision 2004-503DC, explique que : «*le principe de clarté, qui résulte de l'article 34 de la Constitution, et l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi, qui découle des articles4,5,6 et 16 de la Déclaration de 1789 (...), imposent au législateur d'adopter des dispositions suffisamment précises et des formules non équivoques. A défaut, il renverrait à d'autres (administrations, juridictions) des choix que la Constitution lui a confiés en propre ».*

De plus, le Conseil constitutionnel a pu censurer des dispositions au regard de leur complexité excessive, qui se traduisait notamment par censurer une disposition sur le fondement du « *caractère imbriqué, incompréhensible pour le contribuable, et parfois ambigu pour le professionnel, de ses dispositions, ainsi que par les très nombreux renvois qu'il comporte à d'autres dispositions elles-mêmes imbriquées ;* [...] *les incertitudes qui en résulteraient seraient source d'insécurité juridique, notamment de malentendus, de réclamations et de contentieux* » (Décision n° 2005-530 DC du 29 décembre 2005, cons. 84)

Enfin, le Conseil constitutionnel a déjà jugé que ne sont pas conformes à la Constitution en ce qu'elles portent une atteinte manifestement disproportionnée au droit au respect de la vie privée des dispositions prévoyant des mesures de surveillance et de contrôle qui peuvent « ê*tre utilisées à des fins plus larges que la seule mise en œuvre* » des exigences constitutionnelles et qui ne « *définissent pas la nature des mesures de surveillance et de contrôle que les pouvoirs publics sont autorisés à prendre* » (cons. 7 et 8, 2016-590 QPC du 21 octobre 2016).

En l'espèce :

Par le jeu de multiples renvois, l'article 12 étend le champ d'application des articles L.871-3 et L.871-6 du Code de sécurité intérieure qui permettent de contraindre les opérateurs et les fournisseurs d'accès à collaborer à la mise en œuvre des mesures de renseignement directement sur les réseaux et terminaux. L'article 12 aboutit ainsi *in fine* à permettre aux services de renseignement de solliciter ces acteurs pour la mise en œuvre de nouvelles mesures extrêmement intrusives, qui étaient circonscrites auparavant aux seuls acteurs du renseignement.

En premier lieu, le législateur n'a pas pris le soin de viser explicitement le contenu des mesures de surveillance et de contrôle visées par cette extension et s'est contenté de viser, par renvoi, plusieurs articles du code de sécurité intérieure et même des sections entières du code de procédure pénale. En élargissant de façon substantielle le nombre des situations pour lesquelles les services de renseignement peuvent requérir la contribution des fournisseurs et opérateurs et en ne listant pas précisément dans quelle mesures et sous quelles conditions cette contrainte pourrait être justifiée, le législateur a empêché les destinataires et personnes concernées par ces dispositions de comprendre et appréhender les situations concrètes prévues par ces dispositions.

L'analyse réelle de ces dispositions étaient par ailleurs totalement absente de l'exposé des motifs et de l'étude d'impact du Gouvernement ainsi que de l'avis du Conseil d'État et des rapports des différentes commissions.

Par cette absence de précision et par la complexité excessive de la rédaction de cet article, le législateur a incontestablement créé une situation d'insécurité juridique et méconnu l'étendue de sa compétence en manquant à remplir l'objectif de valeur constitutionnelle d'intelligibilité et d'accessibilité de la loi.

En second lieu, l'élargissement des techniques de renseignement pour lesquelles les opérateurs et fournisseurs peuvent être contraints de collaborer crée une atteinte manifestement disproportionnée au droit au respect de la vie privée.

À titre d'exemple, l'article L.853-2 du code de sécurité intérieure permettrait de contraindre des opérateurs de messagerie ou de téléphonie chiffrée à déployer des failles de sécurité sur des terminaux préalablement identifiés. Will Cathcart, dirigeant de la société Whatsapp, exprimait ces inquiétudes dans le journal Le Monde : *« Ce serait une bonne chose que les implications de cet article soient clarifiées. »*, le journaliste indiquant que *« la formulation actuelle évoque la mise en place de mesures de contournement du chiffrement de bout en bout » (*Le Monde, « Vie privée, sécurité, e-commerce… Le patron de WhatsApp s'explique », 28 juin 2021).

De la même manière, les opérateurs pourraient être contraint de collaborer aux interceptions de données de connexions et interceptions de correspondances par "IMSI-catching" prévues par les article L. 852-1 et L. 851-6 du code de sécurité intérieure ainsi que par l'article 706-95-20 du code de procédure pénale. Pour rappel, l'IMSI-catcher est un outil permettant de capter toutes les données de communication dans un rayon donné.

De manière pratique, cela peut correspondre aussi à, par exemple, contraindre un opérateur de téléphonie ou d'Internet d'envoyer un SMS contenant un lien vérolé en son nom ou de le contraindre à déployer une mise à jour frauduleuse du code d'une box Internet pour en donner le contrôle aux services de renseignement, ou même encore de profiter de l'action d'un technicien pour conduire une attaque contre un périphérique informatique d'un abonné.

De même, le ministre de l'intérieur expliquait ainsi sur France Inter, avant le dépôt de la loi déféré, que « nous discutons avec les grands majors d'Internet, on leur demande de nous laisser entrer via des failles de sécurité, certains l'acceptent, d'autres pas. Il faut sans doute **une loi pour contraindre des services étrangers, elle arrive** » (France Inter, 28 avril 2021, L'invité de 8h20). Cherchant à détailler ce point, le ministre a expliqué en hémicycle lors de l'examen de la loi à l'Assemblée nationale le 17 mai 2021 : « Pour ce qui est des messageries cryptées, comme Telegram, WhatsApp ou Signal, elles ont précisément bâti leur modèle économique sur la garantie de ne pas pouvoir être écouté. [...] le recueil des données informatiques permettra d'**accéder au terminal informatique de la personne qui utilise ces messageries pour recueillir les données qui sont stockées dans ces messageries.** »

Si les précédentes possibilités de requérir l'aide de ces acteurs se limitaient à donner accès aux données et contenus déjà produits dans l'utilisation de leurs services et auxquels ils pouvaient accéder, il s'agirait ici de les rendre directement acteurs de la compromissions des outils des utilisateurs de leurs services les mettant en position de conduire ou de participer à une intrusion informatique sur demande des services sans pouvoir s'y opposer.

La modification des dispositions du code de sécurité intérieure change considérablement la nature, l'échelle et les circonstances permettant l'utilisation des techniques visées par l'article 12. Pourtant, le législateur n'a prévu aucune garantie ou limitation supplémentaires spécifiques aux nouvelles situations créées par cette disposition propres à empêcher l'atteinte manifestement disproportionnée au droit à la vie privée générée par cette extension.

Il en résulte que l'article 12 de la loi déférée est contraire aux articles 2 et 34 de la Constitution.

PARTIE 4. Sur la conservation à des fins de recherche - (Article 10)

L'article 10 allonge la durée de conservation des renseignements à des fins de recherche et de développement.

En droit :

Comme vu précédemment, le Conseil constitutionnel a reconnu que la collecte, l'enregistrement et la conservation de données personnelles étaient constitutives d'une atteinte à la vie privée et devaient donc être justifiées par un motif d'intérêt général et proportionné à cet objectif (Cons. constit., n°2012-652 DC, 22 mars 2012).

Par ailleurs, l'article 34 de la Constitution oblige le législateur à fixer les règles concernant les garanties fondamentales accordées au citoyen et, notamment à ce titre, de définir en cas d'atteinte à ces libertés, les conditions d'exploitation, de conservation et de destruction des données collectées. Le Conseil constitutionnel a ainsi considéré que ne sont pas conformes à la Constitution des dispositions prévoyant des mesures de surveillance qui peuvent « *être utilisées à des fins plus larges que la seule mise en œuvre [des exigences de sauvegarde des intérêts fondamentaux de la Nation]* » (Cons. 7 et 8, 2016-590 QPC du 21 octobre 2016).

Enfin, si le Conseil constitutionnel a admis, notamment dans sa décision de 2015, la légalité de certaines techniques de renseignement conduisant au recueil et à la collecte de certaines données à caractère personnel, il ne l'a admis que pour des finalités précisément détaillées et liées notamment à la sécurité nationale, la prévention du terrorisme ou les intérêts majeurs de la politique étrangère (voir Décision n° 2015-713 du 23 juillet 2015). De la même manière, comme rappelé précédemment, la Cour de Justice a limité la possibilité d'une conservation des données de connexion à l'existence de considérations liées à des menaces graves pouvant porter atteinte à la sécurité nationale d'un État membre (voir CJUE, La Quadrature du Net, 6 octobre 2020, tel que cité précédemment).

En l'espèce :

L'atteinte à la vie privée constituée par ce dispositif est particulièrement grave et disproportionnée.

En premier lieu, l'article 10 concerne l'intégralité des renseignements qui sont obtenus dans le cadre des activités de renseignement (factures téléphoniques détaillées, écoutes téléphoniques, surveillance et analyse du réseau de télécommunication...). Cela pourrait donc être potentiellement la totalité du trafic téléphonique et Internet français (et a minima de très nombreuses données de personnes qui n'ont pas été directement la cible d'une technique de renseignement) qui pourraient être récupérées, par les services dédiés de recherche et développement, et conservées pour une très longue durée. Une fois stockées au prétexte de la recherche et développement, il faut redouter que,

par l’autorisation d’une loi future, ces informations puissent être exploitées pour les nombreux et larges objectifs du renseignement (surveillance économique, répression des opposants politiques…).

À ce titre, la conservation de l'ensemble de ces données n'est justifiée que par un objectif de « recherche et de développement en matière de capacités techniques de recueil et d'exploitation des renseignement ». C'est une finalité particulièrement large et libre d'interprétation qui ne correspond en aucun cas aux exigences du Conseil constitutionnel ou à celles édictées par la Cour de Justice de l'Union européenne.

En second lieu, la Défenseure des droits a considéré que la loi manquait de précision sur les conditions exactes de traitement et d'anonymisation des données et que, au minimum, un décret était nécessaire pour préciser l'anonymisation de ces données et les modalités d'élaboration des algorithmes utilisés (Avis du défenseur des droits n° 21-07 du 18 mai 2021, p. 16). C'est également l'avis de la CNIL qui estime que « *le régime de réutilisation des données (...) devrait être encadré par un décret d'application et que des garanties complémentaires soient prévues dans l'hypothèse où ce traitement serait mis en œuvre au moyen d'un traitement algorithmique* » (CNIL, Délibération n° 2021-040, § 43).

Aucune précision n'a pourtant été apportée sur ces différents points par le législateur qui n'a prévu aucun report à un décret permettant au minimum de préciser ces différents points. Le seul encadrement réside en amont dans l'autorisation préalable du Premier ministre et l'existence d'avis non contraignants rendus par la CNCTR, ce qui est largement insuffisant au vu des dangers de cette disposition et ne répond pas aux critères d'exigence d'un contrôle effectif.

Il en résulte que l'article 10 est contraire aux articles 2 de la Déclaration de 1789 ainsi qu'aux articles 24 et 88-1 de la Constitution.

CONCLUSION

En raison des délais extrêmement courts laissés au Conseil constitutionnel pour se prononcer sur cette loi, et donc de la même manière pour les organisations souhaitant déposer des contributions extérieures sur cette loi, l'association La Quadrature du Net a restreint son analyse aux dispositions qui lui paraissaient les plus graves.

Néanmoins, d'autres dispositions de cette loi nous paraissent particulièrement dangereuses pour les droits et libertés protégés par la Constitution française, notamment la surveillance des communications satellitaires (Article 13), l'absence de contrôle effectif de la CNCTR sur les techniques de renseignement (Article 18) et la facilitation des échanges entre services de renseignement et autres services de l'administration (Article 9).