Noémie Levain
La Quadrature du Net
115, rue de Ménilmontant
75020 Paris
contact@laquadrature.net

Monsieur le président du Conseil constitutionnel,
Mesdames et Messieurs les membres du Conseil constitutionnel

Paris, le 27 mai 2025.

Objet : Contribution extérieure sur la loi « visant à sortir la France du piège du narcotrafic » (affaire 2025-885 DC)

Monsieur le président du Conseil constitutionnel,
Mesdames et Messieurs les membres du Conseil constitutionnel,

La Quadrature du Net est une association de défense des droits et libertés à l'ère du numérique. Elle promeut un usage des nouvelles technologies respectueux des droits fondamentaux, notamment sur Internet.

La loi « visant à sortir la France du piège du narcotrafic » dont vous êtes saisis introduit de nombreuses mesures de surveillance qui vont bien au-delà du seul trafic de stupéfiants. Lors des travaux parlementaires sur ce texte, La Quadrature du Net a alerté le législateur concernant l'inconstitutionnalité de certains points de cette loi.

Par la présente contribution extérieure, La Quadrature du Net souhaite attirer l'attention du Conseil constitutionnel sur l'inconstitutionnalité des dispositions du II de article 1er, de celles de l'article 13, 15, 28, 29, 38, 39, 40 et de celles du I de l'article 54 et III de l'article 56.

I. Sur l'échange d'informations entre les services de renseignement (II de l'article 1er)

Les dispositions du II de l'article 1er de la loi déférée sont contraires à l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 en ce qu'elles suppriment l'obligation d'obtenir une autorisation explicite avant la transmission d'informations entre services de renseignement.

En droit, il incombe au législateur d'assurer la conciliation entre, d'une part, les exigences constitutionnelles inhérentes à la sauvegarde des intérêts fondamentaux de la Nation et, d'autre part, le droit au respect de la vie privée protégée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789.

Par ailleurs, il incombe également au législateur d'exercer pleinement la compétence que lui confie la Constitution et, en particulier, son article 34 (*cf.* Cons. const., 26 janvier 1967, *Loi organique modifiant et complétant l'ordonnance n° 58-1270 du 22 décembre 1958 portant loi organique relative au statut de la magistrature*, n° 67-31 DC, cons. 4 ; Cons. const., 1er août 2013, *Loi tendant à modifier la loi n° 2011-814 du 7 juillet 2011 relative à la bioéthique en autorisant sous certaines conditions la recherche sur l'embryon et les cellules souches embryonnaires*, n° 2013-674 DC, cons. 8). En particulier, il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques, dont le droit au respect de la vie privée (*cf.* Cons. const., 20 mai 2021, *Loi pour une sécurité globale préservant les libertés*, n° 2021-817 DC, § 77).

Enfin, il ressort de l'article 45 de la Constitution que, pour être recevable, un amendement en première lecture doit avoir un lien, même indirect, avec le texte en discussion (*cf.* Cons. const., 13 décembre 1985, *Loi modifiant la loi n° 82-652 du 29 juillet 1982 et portant diverses dispositions relatives à la communication audiovisuelle*, n° 85-198 DC, cons. 4 ; Cons. const., 24 avril 2025, *Loi relative au renforcement de la sûreté dans les transports*, n° 2025-878 DC, § 78). Le Conseil constitutionnel a récemment, par exemple, considéré qu'un amendement à un texte relatif à la sécurité dans les transports qui prolongeait une expérimentation de vidéosurveillance algorithmique était sans lien, même indirect, avec le texte initial, alors même que cette expérimentation aurait trouvé à s'appliquer, entre autres, dans les transports (*cf.* Cons. const., 24 avril 2025, *Loi relative au renforcement de la sûreté dans les transports*, préc., § 137).

En l'espèce, le II de l'article 1er de la loi déférée modifie l'article L. 822-3 du code de la sécurité intérieure qui, aujourd'hui, exige que les services de renseignement obtiennent une autorisation du Premier ministre après avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR) dans deux hypothèses :

— lorsque les transmissions de renseignements collectés poursuivent une finalité différente de celle qui en a justifié le recueil ;
— lors de la transmission de renseignements collectés, extraits ou transcrits qui sont issus de la mise en œuvre d'une technique de recueil de renseignements à laquelle le service destinataire n'aurait pu recourir au titre de la finalité motivant la transmission.

Ce système d'autorisation préalable au partage d'informations entre services de renseignement permet de s'assurer, d'une part, que le partage n'ait pas comme conséquence de contourner les limites prévues par la loi et, d'autre part, que ce partage soit proportionné et conforme aux règles du code de la sécurité intérieure. Pour permettre de contrôler les partages par les services

de renseignement, l'article L. 822-4 prévoit également, aujourd'hui, la tenue de relevés mis à la disposition de la CNCTR qui précisent la nature, la date et la finalité des transmissions de renseignements ainsi que le ou les services qui ont été destinataires des données transmises.

Dans son rapport pour l'année 2021, la CNCTR soulignait le fait que ce mécanisme de contrôle permet de garantir le bon respect de la loi et rappelait que l'encadrement de ces transmissions d'informations est nécessaire pour la bonne garantie des droits et libertés. En effet, si l'atteinte aux droits qu'implique la mise en œuvre de la technique de renseignement est déjà consommée, la transmission d'information pose de nouvelles problématiques [1] :

> « *Ce qui importe alors, c'est l'appréciation de la sensibilité des données concernées par cette transmission au regard de la deuxième composante de la protection, c'est-à-dire la protection des données personnelles, lesquelles sont susceptibles de révéler le "contenu" essentiel de la vie privée. Il appartiendra donc à la commission d'apprécier la proportionnalité de l'atteinte que la divulgation de telles données porte au droit au respect de la vie privée au regard de la menace que le service destinataire entend prévenir.* »

Or, le II de l'article 1er de la loi déférée prévoit de supprimer l'autorisation du Premier ministre lorsque la transmission d'information poursuit une finalité différente de celle qui a justifié la collecte ou que l'information a été collectée grâce à une technique normalement inaccessible au service destinataire. Cette modification concernerait toutes les finalités de renseignement et bénéficierait à tous les services, spécialisés ou du « second cercle ».

Premièrement, ces dispositions, issues d'un amendement introduit en première lecture [2], ne présentent pas de lien, même indirect, avec aucune autre des dispositions qui figuraient dans la proposition de loi no 735 déposée sur le bureau du Sénat. En particulier, ces dispositions ne présentent aucun lien, même indirect, avec l'Office anti-stupéfiants (Ofast), objet de l'article 1er dans sa version déposée devant le bureau du Sénat.

Deuxièmement, en supprimant une telle garantie pour les droits et libertés, le législateur a méconnu l'étendue de sa compétence que lui confie l'article 34 de la Constitution, au prix d'une atteinte manifestement disproportionnée au droit au respect de la vie privée protégé par l'article 2 de la Déclaration de 1789. En effet, les garanties procédurales prévues par la loi existent pour assurer le bon respect des règles démocratiques et limiter les potentiels abus des services de l'État, qui disposent de pouvoirs de surveillance importants.

Troisièmement, le législateur n'a, par ces dispositions, pas entendu poursuivre l'objectif de sauvegarde des intérêts fondamentaux de la Nation. En effet, il ressort de l'exposé des motifs de

1. CNCTR, Rapport d'activité pour l'année 2021, p. 81, URL : https://cms.cnctr.fr/uploads/RAPPORT_CNCTR_2021_interactif_30c40b93e6.pdf.

2. Amendement COM-17 rect. URL : https://www.senat.fr/amendements/commissions/2023-2024/735/Amdt_COM-17.html

l'amendement ayant introduit cette modification au Sénat[3] que la suppression de cette garantie serait justifiée par une procédure d'autorisation et de contrôle qui serait aujourd'hui « *particulièrement lourde* ». Autrement dit, la suppression de mesures permettant de garantir le respect du droit au respect de la vie privée est justifiée par une simplification administrative, qui ne poursuit aucunement un objectif à valeur constitutionnel ni un motif d'intérêt général : ces dispositions n'ont pas comme conséquence d'étendre les possibilités d'échanges de renseignement mais bien d'empêcher qu'un abus puisse être prévenu ou, s'il survient, être réparé.

De telles violations sont loin d'être théoriques. Ainsi, dans son rapport d'activités pour l'année 2021, la CNCTR mentionne un manquement qui a permis à un service du second cercle d'avoir accès à des informations collectées pour une finalité qui ne lui était normalement pas accessible. Dans l'exemple pris par l'autorité, un service du « second cercle » a pu accéder à des informations collectées suite à la mise en œuvre de techniques autorisées sur le fondement de la défense et la promotion des 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. Or, cette finalité n'est accessible à aucun des services du « second cercle ». Pour justifier sa demande de partage d'informations, le service destinataire avait précisé que le partage d'information avait été fait au titre de la prévention des violences collectives de nature à porter gravement atteinte à la paix publique. Mais, suite à un contrôle, la CNCTR a cependant estimé qu'aucune des informations qui y étaient consignées n'était susceptible de se rattacher à une telle finalité[4].

Il en résulte que, en supprimant une telle autorisation, donc en ôtant l'étape de contrôle du Premier ministre et de la CNCTR, le législateur a méconnu la procédure de l'article 45 de la Constitution, ainsi que porté une atteinte manifestement disproportionnée au droit au respect de la vie privée.

II. Sur le partage d'information entre l'autorité judiciaire et les services de renseignement (article 13)

Les dispositions de l'article 13 de la loi déférée sont contraires à l'article 66 de la Constitution en ce qu'elles élargissent le champ des informations qui peuvent être communiquées entre l'autorité judiciaire et les services de renseignement.

En droit, le Conseil constitutionnel distingue les finalités visant à prévenir des troubles à l'ordre public – qui peuvent être mises en œuvre par le pouvoir exécutif – et celles visant à rechercher les auteurs d'infractions – qui doivent impérativement être mise en œuvre par l'autorité judiciaire. Ainsi le Conseil constitutionnel a-t-il censuré, en raison de l'atteinte portée au principe de séparation des pouvoirs, des dispositions permettant à l'autorité administrative de mettre en œuvre des mesures de surveillance visant à « *réprimer* » des actes de terrorisme (*cf.* Cons.

3. *Ibid.*
4. *Ibid.*, p. 79

const., 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, n° 2005-532 DC, cons. 5 ; v. également Cons. const., 23 juillet 2015, *Loi relative au renseignement*, n° 2015-713 DC, cons. 9). Ce principe de séparation des pouvoirs dont découle une obligation de distinction des finalités de police administrative et celles de police judiciaire s'applique au-delà des activités de renseignement (*cf.* Cons. const., 21 mars 2019, *Loi de programmation 2018-2022 et de réforme pour la justice*, n° 2019-778 DC, pt. 80 ; Cons. const., 19 janvier 2023, *Loi d'orientation et de programmation du ministère de l'intérieur*, n° 2022-846 DC, pts. 70 et 80).

Par là, le Conseil rappelle qu'une administration – que sont les services de renseignement – ne peut se substituer à l'autorité judiciaire. Si cette dernière dispose d'informations relatives à une potentielle infraction, elle constitue la seule autorité constitutionnellement habilitée pour poursuivre la personne autrice d'une violation de la loi. Si l'autorité judiciaire ne dispose pas assez d'éléments, il lui incombe alors, au nom du principe de séparations des pouvoirs, de poursuivre sa mission de rassembler des preuves permettant d'ouvrir une enquête ou de clôturer l'affaire, plutôt que la confier à une administration qui, même dans le cas où elle bénéficie de pouvoirs de police administrative, ne dispose pas de pouvoirs répressifs ni de prérogatives de recherche d'auteurs d'infractions.

De plus, l'activité du renseignement, par nature secrète, n'est pas soumise aux mêmes règles de procédures ni de contrôle. La CNCTR évoque ainsi le risque d'« *allers-retours* » entre les régimes administratif et judiciaire. Ceux-ci « *interviennent, par exemple lorsqu'une enquête judiciaire est ouverte sur la base d'un renseignement administratif aux fins de mise en œuvre des techniques spéciales d'enquête prévues par le code de procédure pénale, puis clôturée aux fins d'ouverture d'une nouvelle phase administrative sur le fondement du code de la sécurité intérieure destinée à permettre in fine l'ouverture d'une enquête judiciaire. Ces configurations sont en effet porteuses d'un risque procédural majeur tant au regard du principe de légalité que du principe de loyauté dans le recueil de la preuve* »[5].

En l'espèce, d'une part, les dispositions de l'article 13 de la loi déférée étendent la possibilité de signalement à tous les procureurs, alors qu'une telle possibilité de signalement était auparavant limitée au seul procureur de Paris. D'autre part, le périmètre des infractions concernées par cette transmission d'informations est largement étendu. S'il vise les crimes et délits de trafic de stupéfiants, ce nouveau périmètre englobe également des infractions ayant un champ d'application beaucoup plus large comme le vol en bande organisée ou la destruction, dégradation et détérioration d'un bien commis en bande organisée qui peuvent fonder des procédures visant des actions politiques ou militantes.

Or, en étendant ainsi la possibilité de signalement de l'autorité judiciaire vers une autorité administrative que sont les services de renseignement, dans le but de pallier le manque de preuves que détient la première, le législateur a, de fait, confié aux services de renseignement un pouvoir

5. *Ibid.*, p. 107.

de recherche d'auteurs d'infractions, en violation de l'article 66 de la Constitution.

Il en résulte que les dispositions de l'article 13 de la loi déférée méconnaissent manifestement l'exigence de séparation des pouvoirs.

III. Sur la surveillance par algorithme, ou « boites noires » (article 15)

Les dispositions de l'article 15 de la loi déférée méconnaissent les articles 2, 4 et 11 de la Déclaration de 1789, et l'article 34 de la Constitution, en ce qu'elles étendent davantage le champ d'application de la technique de renseignement dite des « boites noires », ou de « l'algorithme ».

En droit, comme rappelé ci-avant, il ressort de l'article 2 de la Déclaration de 1789 un droit au respect de la vie privée. 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* » (*cf.* Cons. const., 22 mars 2012, *Loi relative à la protection de l'identité*, n° 2012-652 DC, cons. 8). Également, il a admis la valeur constitutionnelle du droit au secret des correspondances, rattaché aux articles 2 et 4 de la Déclaration de 1789 (*cf.* Cons. const., 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*, n° 2004-492 DC, cons. 4).

Le Conseil constitutionnel considère par ailleurs que l'article 11 de la Déclaration des droits de l'homme et du citoyen de 1789 implique la liberté d'accéder aux services de communication au public en ligne et de s'y exprimer (*cf.* Cons. const., 18 juin 2020, *Loi visant à lutter contre les contenus haineux sur internet*, n° 2020-801 DC, cons. 4). Or, la surveillance d'un grand nombre de personnes par la collecte de façon indifférenciée d'importants volumes de données est de nature à dissuader les personnes d'utiliser ces sites et porte donc atteinte à la liberté d'expression (*cf.* Cons. const., 27 décembre 2019, *Loi de finances pour 2020*, préc., pt. 82).

Le Conseil constitutionnel estime que les données de connexion peuvent porter « *sur l'identification des utilisateurs des services de communications électroniques, mais aussi sur la localisation de leurs équipements terminaux de communication, les caractéristiques techniques, la date, l'horaire et la durée des communications ainsi que les données d'identification de leurs destinataires* ». Il estime ainsi que, « *compte tenu de leur nature, de leur diversité et des traitements dont elles peuvent faire l'objet, ces données fournissent sur ces utilisateurs ainsi que, le cas échéant, sur des tiers, des informations nombreuses et précises, particulièrement attentatoires à leur vie privée* » (*cf.* Cons. Const., 25 février 2022, *M. Habib A. et autre [Conservation des données de connexion pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales]*, n° 2021-976/977 QPC, § 11 ; Cons. const., 20 mai 2022, *M. Lotfi H. [Réquisition de données informatiques dans le cadre d'une enquête de flagrance]*, n° 2022-993 QPC, § 10).

Dans sa décision n° 2021-976/977 QPC du 25 février 2022, le Conseil constitutionnel a notamment censuré les dispositions de l'article L. 34-1 du code des postes et des communications électroniques qui prévoyaient une conservation généralisée et indifférenciée des données de connexion. Le commentaire de cette décision indique que le Conseil constitutionnel s'est directement inspiré de la jurisprudence de la Cour de Justice de l'Union européenne (CJUE) en la matière, et notamment de son arrêt *La Quadrature du Net* (*cf.* CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e. a.*, aff. C-511/18, C-512/18 et C-520/18). Celle-ci y a notamment souligné 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* » (*cf.* CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e. a.*, préc., pt. 192).

De même, comme rappelé ci-avant, il ressort de l'article 34 de la Constitution que le législateur est tenu d'exercer pleinement sa compétence, notamment en fixant les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Le Conseil constitutionnel a ainsi relevé la méconnaissance de l'article 34 de la Constitution en raison 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 (*cf.* Cons. const., 23 juillet 2015, *Loi relative au renseignement*, préc., cons. 78).

Enfin, la conformité à la Constitution d'une loi déjà promulguée peut être appréciée à l'occasion de l'examen des dispositions législatives qui la modifient, la complètent ou affectent son domaine (*cf.* Cons. const., 25 janvier 1985, *Loi relative à l'état d'urgence en Nouvelle-Calédonie et dépendances*, n° 85-187 DC, cons. 10 ; Cons. const., 16 décembre 2021, *Loi de financement de la sécurité sociale pour 2022*, n° 2021-832 DC, § 10 ; Cons. const., 21 mars 2019, *Loi de programmation 2018-2022 et de réforme pour la justice*, préc., §§ 247 et 254).

En l'espèce, la technique de surveillance prévue par l'article L. 851-3 du code de la sécurité intérieure, visée par les dispositions de l'article 15 de la loi déférée, consiste à collecter l'intégralité des télécommunications d'un réseau donné dans le but d'analyser les métadonnées (qui contacte qui ? quand ? à quelle fréquence ? depuis quel(s) emplacement(s) ?). Or, la technique de l'algorithme est, par nature, une surveillance de masse puisqu'il s'agit de surveiller l'ensemble d'un réseau de télécommunications pour détecter automatiquement des « signaux faibles », c'est-à-dire des communications suspectes qu'un œil humain ne serait prétendument pas capable de détecter. Les personnes ainsi repérées peuvent ensuite être ciblées par d'autres techniques de renseignement. Cette technique de surveillance concerne tout autant les réseaux téléphoniques que le réseau internet, et peut être mise en œuvre sur des réseaux de toute taille (le réseau d'une résidence étudiante tout comme le cœur de réseau d'un fournisseur français d'accès internet peuvent être concernés).

Cette technique de renseignement agit donc à la manière d'un énorme « filet de pêche » jeté sur l'ensemble des personnes utilisant le réseau ainsi surveillé, la largeur de maille étant déter-

minée par le gouvernement lors de l'élaboration de ces algorithmes et la taille du filet librement déterminée par les services de renseignement.

Or, l'article 15 de loi la loi déférée étend les possibilités d'utilisation de cette technique de renseignement aux fins de « *prévention de la criminalité et de la délinquance organisées* » prévus par le 6° de l'article L. 811-3 du code de la sécurité intérieure.

Rappelons que les dispositions de l'article 15 de la loi déférée modifient l'article L. 851-3 du code de la sécurité intérieure en prévoyant que cette technique de renseignement puisse être mobilisée pour poursuivre une nouvelle finalité. Ce faisant, c'est l'ensemble de cette technique de renseignement qui peut être contrôlée par le Conseil constitutionnel dans le cadre de la présente saisine, notamment parce qu'elle n'a pas fait l'objet d'un précédent contrôle de constitutionnalité depuis les modifications apportées par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement.

Les dispositions de l'article L. 851-3 du code de la sécurité intérieure, que modifie l'article 15 de la loi déférée, autorisent une technique de surveillance qui porte une atteinte manifestement disproportionnée aux droits et libertés constitutionnellement protégés.

En effet, s'il est vrai que le Conseil constitutionnel a déjà considéré que cette technique pouvait être conforme au droit à la vie privée (*cf.* Cons. const., 23 juillet 2015, *Loi relative au renseignement*, préc., cons. 60), cette conformité à la Constitution était conditionnée à certaines garanties et notamment, d'une part, qu'elle ne pouvait être mise en œuvre qu'aux fins de prévention du terrorisme et, d'autre part, qu'elle ne portait que sur les informations ou documents mentionnés à l'article L. 851-1 du code de la sécurité intérieure, c'est-à-dire à l'exclusion du « *contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications* » (cons. 55). Or, depuis son précédent contrôle de constitutionnalité, le Conseil constitutionnel a non seulement adopté un contrôle plus étendu de ce type de surveillance en ligne, notamment au regard de la liberté d'expression et de communication protégée par l'article 11 de la Déclaration de 1789, mais les dispositions de l'article L. 851-3 du code de la sécurité intérieure ont été largement étendues, à de nouvelles finalités ainsi qu'au contenu des correspondances.

Premièrement, les dispositions de l'article L. 851-3 du code de la sécurité intérieure telles que modifiées par l'article 15 de la loi déférée ne sont pas limitées à l'existence d'une « *menace grave pour la sécurité nationale* » qui serait « *actuelle ou prévisible* » au sens de la jurisprudence de la CJUE.

Deuxièmement, le périmètre des infractions visées par cette extension est radicalement différent de la stricte lutte contre le risque terroriste, qui avait seule justifié la conformité du dispositif en 2015. Or, en permettant de mobiliser cette technique de surveillance pour des finalités différentes, le législateur autorise à ce qu'elle soit plus largement utilisée, pour des situations plus nombreuses et concernant un nombre de personne plus important, décuplant les atteintes aux droits

et libertés constitutionnellement protégés.

Troisièmement, si ce dispositif avait été jugé constitutionnel car instauré de façon expérimentale pour quelques années avec des obligations d'évaluation, force est de constater que les quelques évaluations ne démontrent pas la nécessité de prévoir une telle surveillance dans la loi. Dans son rapport pour l'année 2023, la CNCTR a indiqué que 5 boites noires avait été installées. Pour autant, aucune information sur le fonctionnement, l'utilisation ou l'utilité de ces techniques n'a été rendue publique. Après avoir étendu cette technique de surveillance à la prévention des ingérences étrangères par la loi n° 2024-850 du 25 juillet 2024, c'est donc un nouvel élargissement qui est proposé sans aucune clarté sur l'étendue de cette surveillance de masse.

La Commission nationale de l'informatique et des libertés (CNIL) a ainsi rappelé dans son avis de 2021 relatif à la pérennisation de cette surveillance 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* »[6], et souligné ne pas avoir pu analyser la proportionnalité de l'atteinte à la vie privée constituée par une première pérennisation[7].

Quatrièmement, les dispositions de l'article L. 851-3 du code de la sécurité intérieure telles que modifiées par l'article 15 de la loi déférée ne sont aucunement limitées aux seules données de connexion. Contrairement à ce que le Conseil constitutionnel avait érigé comme garantie permettant de considérer cette surveillance conforme à la Constitution, elle peuvent porter désormais également sur les « *adresses complètes de ressources utilisées sur internet* » (communément appelées « URL complètes »). Or, ces URL complètes sont de nature à révéler le contenu d'une communication ou les informations consultées. En effet, une adresse d'un site internet peut donner des indications sur les informations consultées : une URL complète peut révéler, lorsqu'elle contient une référence unique à un contenu, le contenu de la communication. Ce sera par exemple le cas d'un article de presse[8] ou d'une vidéo en ligne[9].

La CNIL rappelait ce problème intrinsèque à l'analyse des URL complètes dans son avis sur la réforme de 2021 du droit du renseignement[10] :

« *La Commission rappelle que ces données ont une nature particulière. Comme sou-*

6. CNIL, Délibération n° 2021-040 du 8 avril 2021, § 24. URL : `https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000043505603/`

7. *Ibid.*, § 31.

8. Il suffit de regarder l'URL `https://www.lemonde.fr/politique/article/2025/04/29/la-loi-sur-le-narcotrafic-adoptee-definitivement-au-parlement_6601733_823448.html` pour deviner le contenu de l'article.

9. Même si la seule lecture de l'URL `https://www.youtube.com/watch?v=VyLOy7l_jP4` ne donne aucune information sur la nature de la vidéo, il suffit de consulter l'URL pour prendre connaissance du contenu de la communication.

10. CNIL, Délibération n° 2021-040 du 8 avril 2021 portant avis sur un projet de loi relatif à la prévention d'actes de terrorisme et au renseignement. URL : `https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000043505603`.

ligné par le Comité européen de la protection des données (CEPD), les URL sont susceptibles de faire apparaître des informations relatives au contenu des éléments consultés ou aux correspondances échangées. La Commission rappelle que la protection particulière dont bénéficient les données de contenu ainsi que les correspondances représente une garantie essentielle pour assurer le respect de la vie privée et des autres libertés afférentes. »

Cinquièmement, les dispositions de l'article L. 851-3 du code de la sécurité intérieure telles que modifiées par l'article 15 de la loi déférée ne prévoient plus que « *peut être imposé aux opérateurs* [...] *la mise en œuvre sur leurs réseaux* » du dispositif de détection automatisée, mais que ce dispositif est directement mis en œuvre par les services de renseignement « *sur les données transitant par les réseaux des opérateurs* ». Cette modification, issue de la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, implique une architecture radicalement différente que la loi échoue entièrement à décrire et à encadrer. La CNIL a ainsi précisé 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* ». Pour la CNIL, il était « *indispensable que le texte soit précisé* » sur ce sujet, et le fonctionnement de l'architecture technique permettant la mise en œuvre de cette technique de renseignement aurait dû « *figurer dans la loi* »[11].

Les dispositions de l'article L. 851-3 du code de la sécurité intérieure ne précisent pourtant pas comment la technique de surveillance autorisée est concrètement mise en œuvre. Par ce silence, le législateur n'a pas prévu de garanties suffisantes permettant que cette technique de renseignement ne soit pas dévoyée à d'autres fins que celles définies par le texte, et ce d'autant plus que d'autres dispositions du code de la sécurité intérieure permettent de conserver les données analysées par cette technique de renseignement pour la recherche et développement pendant 5 ans. Le législateur a notamment échoué à empêcher que l'intégralité du trafic internet se retrouve dupliqué et mis de côté par les services de renseignement.

Ainsi, en ne précisant pas les modalités de mise en œuvre de la technique de recours aux algorithmes ni l'architecture précise du traitement automatisé permettant la mise en œuvre de cette technique, le législateur n'a 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, méconnaissant ainsi l'étendu de sa compétence au prix d'une atteinte manifestement disproportionnée au droit au respect de la vie privée, à la liberté d'expression et au secret des correspon-

11. CNIL, Délibération n°2021-040 du 8 avril 2021, § 16 et s.

dances.

Il en résulte que les dispositions de l'article 15 de la loi déférée, ainsi que les dispositions de l'article L. 851-3 du code de la sécurité intérieure telles que modifiées par cet article, sont manifestement contraires au droit à la vie privée, à la liberté d'expression et au secret des correspondances, et que le législateur a méconnu l'étendue de sa compétence.

IV. Sur l'extension du périmètre de la censure administrative (article 28)

L'article 28 de la loi déférée est contraire à l'article 11 de la Déclaration de 1789 en ce qu'elle crée de nouvelles possibilités de censure administrative de contenus en ligne.

En droit, comme rappelé précédemment, découle de l'article 11 de la Déclaration de 1789 la liberté d'accéder aux services de communication au public en ligne et de s'y exprimer (*cf.* Cons. const., 18 juin 2020, *Loi visant à lutter contre les contenus haineux sur internet*, préc., § 4).

Le Conseil constitutionnel estime que, s'il est loisible au législateur, en vertu de l'article 34 de la Constitution, « *d'instituer des dispositions destinées à faire cesser des abus de l'exercice de la liberté d'expression et de communication qui portent atteinte à l'ordre public et aux droits des tiers* », c'est à la stricte condition que les atteintes portées à l'exercice de cette liberté soient nécessaires, adaptées et proportionnées à l'objectif poursuivi (*cf.* Cons. const., 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet*, n° 2009-580 DC, cons. 15 ; Cons. const., 20 mai 2011, *Mme Térésa C. et autre [Exception de vérité des faits diffamatoires de plus de dix ans]*, n° 2011-131 QPC, cons. 3 ; Cons. const., 28 février 2012, *Loi visant à réprimer la contestation de l'existence des génocides reconnus par la loi*, n° 2012-647 DC, cons. 5 ; Cons. const., 17 mai 2024, *Loi visant à sécuriser et à réguler l'espace numérique*, n° 2024-866 DC, § 19 ; Cons. const., 27 décembre 2019, *Loi de finances pour 2020*, n° 2019-796 DC, pt. 82).

Appliqué au cas d'une censure administrative en ligne, le Conseil constitutionnel a déjà jugé qu'une loi prévoyant un mécanisme de retrait administratif des contenus à caractère terroriste ou pédopornographique en une heure portait une atteinte disproportionnée à la liberté d'expression et de communication protégée par l'article 11 de la Déclaration de 1789 dans la mesure où « *la détermination du caractère illicite des contenus en cause ne repose pas sur leur caractère manifeste* [et] *est soumise à la seule appréciation de l'administration* » (*cf.* Cons. const., 18 juin 2020, *Loi visant à lutter contre les contenus haineux sur internet*, préc., § 7).

En l'espèce, aujourd'hui, les agents de la plateforme Pharos peuvent exiger le retrait de tout contenu qu'ils jugeraient illégal parce qu'il ferait l'apologie du terrorisme, serait à caractère pédocriminel ou, depuis la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, serait relatif à des actes de torture barbarie. L'article 28 de la loi déférée étend ces capacités de censure administrative en ajoutant à la liste des contenus pouvant faire l'objet d'une

injonction de retrait tout contenu qui contreviennent à l'article 222-39 du code pénal, c'est-à-dire qui serait relatif à la cession ou l'offre illicites de stupéfiants à une personne en vue de sa consommation personnelle.

Le large périmètre de cette infraction risque de concerner de nombreuses situations qui n'ont aucun lien avec le cession ou la consommation de drogues à proprement parler.

De plus, ce mécanisme de censure administrative pose, depuis sa création, de nombreux risques pour la liberté d'expression en ligne. De par son caractère extra-judiciaire, cette procédure donne à l'administration un pouvoir de fait discrétionnaire d'appréciation de l'illégalité des contenus. Ce n'est qu'en cas de contestation que le juge administratif peut être saisi et pourra apprécier la légalité de la demande de retrait. Des exemples concrets ont démontré ces dernières années les abus auxquels pouvait mener une interprétation large du « terrorisme » par la police française. Le régime existant de censure administrative a ainsi pu conduire à bloquer un site militant (décisions annulées par la justice administrative un an et demi après, *cf.* TA Cergy-Pontoise, 4 février 2019, *Alexandre Linden*, n^{os} 1801344, 1801346, 1801348, 1801352) ou à demander le retrait d'une caricature d'Emmanuel Macron sans que l'on ne sache sur quel fondement cette demande avait été faite.

Ainsi, cette modification élargit de façon disproportionnée une capacité de censure administrative déjà très importante et non soumis au contrôle effectif d'un juge.

Il en résulte que les dispositions de l'article 28 de la loi déférée porte une atteinte manifestement disproportionnée à la liberté d'expression.

V. Sur la collecte des données d'identification par les opérateurs de communications électroniques (article 29)

Les dispositions de l'article 29 de la loi déférée, qui exigent des opérateurs de communication électronique de collecter l'identité des utilisateurs d'un « *service de communications interpersonnelles avec prépaiement* », sont contraires aux articles 2, 4, 5, 6, 11 et 16 de la Déclaration de 1789 en ce qu'elles portent une atteinte manifestement disproportionnée au droit au respect de la vie privée et à la liberté d'expression, et qu'elles méconnaissent le principe de clarté et d'intelligibilité de la loi, ainsi qu'à l'article 45 de la Constitution.

En droit, comme rappelé précédemment, il découle de l'article 2 de la Déclaration de 1789 le droit au respect de la vie privée, et de l'article 11 la liberté d'expression, laquelle implique le droit d'accéder aux services en ligne.

Le Conseil constitutionnel pourra ainsi utilement s'inspirer de la Cour européenne des droits de l'homme (ci-après « CEDH ») qui reconnaît, au visa de l'article 10 de la CESDH qui protège le droit à la liberté d'expression, un principe de droit à l'anonymat sur Internet (*cf.* CEDH, gr. ch.,

16 juin 2015, *Delfi AS c. Estonie*, n° 64569/09, § 147 ; v. également, au visa de l'article 8 de la Convention, CEDH, 24 avril 2018, *Benedik c. Slovénie*, n° 62357/14, §§ 100–119), principe qui ne souffre aucune difficulté d'application, *mutatis mutandis*, au cas d'une communication interpersonnelle, que celle-ci transite par le réseau internet ou par le réseau téléphonique. Il pourra également s'inspirer de la jurisprudence de la CJUE, laquelle retient elle aussi un droit à l'anonymat en ligne, fondé sur le droit à la vie privée, le droit à la protection des données personnelles, et la liberté d'expression (*cf.* CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e.a.*, préc., pt. 109).

La CJUE a récemment précisé sa jurisprudence sur la collecte de l'identité civile : la conformité au droit de l'UE d'une disposition nationale exigeant la conservation de données relatives au trafic est subordonnée à la circonstance que les données ainsi conservées ne puissent permettre de tirer des conclusions précises sur la vie privée des personnes concernées (*cf.* CJUE, ass. plen., 30 avril 2024, *La Quadrature du Net e. a.*, aff. C-470/21). La CJUE considère que la seule conservation de l'identité civile associée à une adresse IP ne permet pas de tirer de telles conclusions (§ 82), mais rappelle qu'une législation nationale qui impose la conservation « *d'un ensemble de données nécessaires pour déterminer la date, l'heure, la durée et le type de la communication, identifier le matériel de communication utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figuraient, notamment, le nom et l'adresse de l'utilisateur, les numéros de téléphone de l'appelant et de l'appelé ainsi que l'adresse IP pour les services Internet* » porterait une atteinte disproportionnée au droit à la vie privée, au droit à la protection des données personnelles, ainsi qu'à la liberté d'expression (§ 80). Pour établir si une conservation de l'adresse IP associée à l'identité civile constitue une ingérence grave, la Cour exige de prendre en compte les possibilités de recoupement des « *adresses IP avec un ensemble de données de trafic ou de localisation qui auraient également été conservées par ces fournisseurs* » (§ 82, *in fine*).

Par ailleurs, des articles 4, 5, 6 et 16 de la Déclaration découle un principe de clarté et d'intelligibilité de la loi (*cf.* Cons. const., 9 juillet 2004, *Loi organique relative à l'autonomie financière des collectivités territoriales*, n° 2004-500 DC, cons. 13).

Enfin, comme rappelé précédemment, il ressort de l'article 45 de la Constitution que, pour être recevable, un amendement en première lecture doit avoir un lien, même indirect, avec le texte en discussion.

En l'espèce, les dispositions de l'article 29 de la loi déférée modifient le 1° du II *bis* de l'article L. 34-1 du code des postes et des communications électroniques, pour désormais exiger des « *opérateurs de communications électroniques* » qu'ils conservent « *les informations relatives à l'identité civile de l'utilisateur* » de « *son service de communications interpersonnelles avec prépaiement* ».

Premièrement, la rédaction des dispositions de cet article ne permet pas de déterminer avec

certitude l'étendue des obligations nouvellement créées. En effet, l'exposé des motifs de l'amendement n° 194 [12] du Sénat introduisant ces dispositions visait les fournisseurs de cartes SIM prépayées alors que la rédaction initiale ne se limitait aucunement à ces derniers. Or, la rédaction actuelle – qui déporte l'obligation de collecter l'identité civile de certains utilisateurs à l'article L. 34-1 du code des postes et des communications électroniques au lieu de créer un nouvel article à ce même code comme l'envisageait l'amendement du Sénat – loin de clarifier la lettre de la loi, vient, au contraire, rajouter de l'approximation.

D'une part, si l'on adopte une lecture littérale des dispositions de l'article 29, alors les « *opérateurs de communications électroniques* » sont tenus de conserver les données d'identité civile de « *l'utilisateur* » jusqu'à cinq ans après la fin de « *validité* » du « *service de communications interpersonnelles avec prépaiement* » de l'« *utilisateur* ». En effet, l'usage du déterminant possessif « *son* » fait nécessairement référence à « *l'utilisateur* ». Mais, dans ce cas, on comprend mal la volonté du législateur puisque la notion de fin de validité d'un « *service de communications interpersonnelles avec prépaiement* » n'a strictement aucun sens.

Si l'exposé des motifs de l'amendement ayant introduit ces dispositions fait référence aux opérateurs fournissant des cartes SIM prépayées, force est de constater que la notion de « *service de communications interpersonnelles avec prépaiement* » va bien au-delà des seules cartes SIM prépayées. La directive n° 2018/1972 du 11 décembre 2018 établissant le code des communications électroniques européen, applicable en l'espèce, définit la notion de « *service de communications interpersonnelles* » au 5 de son article 2 :

> « *un service normalement fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service* »

Par ailleurs, cette même directive classe les services de communications interpersonnelles entre ceux qui sont « *fondés sur la numérotation* » et ceux « *non fondé sur la numérotation* ». En l'absence de précision, les dispositions de l'article 29 de la loi déférée ne peuvent être lues que dans un sens qui inclut ces deux sous-catégories, qui vont donc bien au-delà des seules cartes SIM : elles concerneraient donc toute messagerie interpersonnelle, utilisant le réseau téléphonique ou passant par Internet, à partir du moment où le service est prépayé, c'est-à-dire lorsque l'utilisateur effectue un paiement avant de pouvoir utiliser le service. Des messageries dont certaines fonctionnalités sont réservées aux utilisateurs payant un forfait chaque mois, telles que Olvid, seraient donc concernées par ces nouvelles dispositions.

12. Disponible à l'adresse suivante : `https://www.senat.fr/amendements/2024-2025/254/Amdt_194.html`

L'exposé des motifs est donc insusceptible de guider l'interprétation des dispositions de l'article 29 de la loi déférée.

D'autre part, la rédaction des dispositions de l'article 29 ne permet pas de savoir ce qui est nouvellement attendu des « *opérateurs de communications électroniques* » à qui le II *bis* de l'article L. 34-1 du code des postes et des communications électroniques s'applique. En effet, les « *opérateurs de communications électroniques* » et les fournisseurs d'un « *service de communications interpersonnelles avec prépaiement* » ne sont pas nécessairement la même entité juridique. Ces dispositions pourraient donc se comprendre comme imposant aux « *opérateurs de communications électroniques* » de collecter l'identité civile de leurs utilisateurs si ces derniers utilisent un « *service de communications interpersonnelles avec prépaiement* » à l'aide du réseau fourni par leur opérateur. Ce qui n'aurait pas beaucoup de sens.

En somme, on peut penser que le législateur ait voulu imposer aux seules opérateurs de téléphonie mobile qui proposent des cartes SIM prépayées de collecter l'identité de leurs clients. Mais ce n'est pas ce qui ressort de la lettre de la loi. Les notions utilisées et le fait que les dispositions de l'article 29 de la loi déférées concernent l'article L. 34-1 du code des postes et des communications électroniques ne permettent pas de remplir l'exigence constitutionnelle de clarté et d'intelligibilité de la loi.

Deuxièmement, ces dispositions de l'article 29 de la loi déférée ne présentent pas de lien, même indirect, avec aucune autre des dispositions qui figuraient dans la proposition de loi n° 735 déposée sur le bureau du Sénat. L'article 29, créé par l'amendement n° 194 du Sénat introduisant ces dispositions dans un article 12 *bis* à la proposition de loi, s'insère dans une section relative à la répression pénale du trafic de stupéfiant. Or, si la collecte de l'identité civile de toute personne va nécessairement pouvoir être utilisée dans les affaires de lutte contre le trafic de stupéfiants, tel n'est pas l'objet, même indirect, de cet amendement.

Troisièmement, l'ingérence ainsi créée dans le droit au respect de la vie privée et la liberté d'expression serait manifestement disproportionnée.

En effet, la conservation de l'identité civile envisagée par les dispositions contestées implique non seulement de conserver l'identité civile, mais surtout de l'associer à un identifiant unique dans le service de messagerie (numéro de téléphone, pseudo, identifiant technique interne, etc.). Contrairement au cas d'une identité civile associée à une adresse IP qui, en soi, ne permet pas de retracer l'historique de navigation selon la CJUE [13], il en va différemment d'une identité civile associée à un numéro de téléphone ou à un identifiant d'une messagerie interpersonnelle : dans ce cas, il est possible de déterminer le graphe social de la personne (avec qui et à quelle fréquence la personne concernée communique), dont l'anonymat est levé. Même à supposer que ces dispositions ne s'appliquent qu'au cas d'un opérateur de téléphonie mobile fournissant des cartes

13. Notons toutefois que, même s'il s'agit d'une hypothèse permettant à la CJUE de fonder ensuite son raisonnement, cette affirmation peut se révéler fausse dans un certain nombre de cas.

SIM prépayées, il serait quand même dans la situation de pouvoir techniquement rapprocher les numéros de téléphones appelés et appelant avec l'identité civile.

Il en résulte que les dispositions de l'article 29 de la loi déférée méconnaissent le principe de clarté et d'intelligibilité de la loi, n'ont pas leur place dans la loi déférée, et portent une atteinte manifestement disproportionnée au droit au respect de la vie privée et à la liberté d'expression.

VI. Sur l'activation à distance des objets connectés (articles 38 et 39)

Les dispositions des articles 38 et 39 de loi déférée sont contraires aux articles 2 et 11 de la Déclaration de 1789 en ce qu'elles autorisent des techniques permettant d'activer, à distance, les appareils électroniques d'une personne à son insu pour capter des images et des sons.

En droit, comme rappelé précédemment, il ressort des articles 2 et 11 de la Déclaration de 1789 un droit au respect de la vie privée et à la liberté d'expression. Surtout, le Conseil constitutionnel a déjà censuré de précédentes dispositions qui autorisaient l'activation à distance d'appareils électroniques afin de capter des sons et des images, relevant qu'une telle surveillance « *est de nature à porter une atteinte particulièrement importante au droit au respect de la vie privée dans la mesure où elle permet l'enregistrement, dans tout lieu où l'appareil connecté détenu par une personne privée peut se trouver, y compris des lieux d'habitation, de paroles et d'images concernant aussi bien les personnes visées par les investigations que des tiers* » (*cf.* Cons. const., 16 novembre 2023, *Loi d'orientation et de programmation du ministère de la justice 2023-2027*, n° 2023-855 DC, § 68).

En l'espèce, les dispositions des articles 28 et 29 de la loi déférée autorisent l'autorité judiciaire à recourir à une technique de surveillance reposant sur la compromission d'appareils électroniques par un « logiciel espion », ou « *spyware* », qui va exploiter les failles de sécurité de ces appareils (notamment, s'ils ne sont pas mis à jour) en y accédant physiquement ou en les piratant à distance, afin de contourner les barrières techniques pour accéder aux données stockées, activer des fonctionnalités (micro, caméra) et exfiltrer les données captées.

Ces dispositions concernent les téléphones et ordinateurs, mais plus largement tout « *appareil électronique* », c'est-à-dire tout objet numérique connecté disposant d'un micro ou d'une caméra. Cette mesure d'enquête pourrait ainsi permettre de « sonoriser » – c'est-à-dire d'écouter – des espaces à partir d'une télévision connectée, d'un babyphone, d'un assistant vocal (Google Home, Alexa, etc.), ou encore d'un robot cuiseur ou d'une voiture qui disposeraient d'un micro. Ces dispositions pourraient également permettre à la police de retransmettre des images et des vidéos à partir de la caméra d'un ordinateur portable, d'un smartphone ou d'une caméra de sécurité.

Le Conseil constitutionnel a déjà relevé qu'une telle surveillance « *est de nature à porter une atteinte particulièrement importante au droit au respect de la vie privée* » (*cf.* Cons. const., 16 no-

vembre 2023, *Loi d'orientation et de programmation du ministère de la justice 2023-2027*, préc., § 68). Cette constatation n'est pas isolée : les révélations concernant l'espionnage de téléphones de journalistes et opposants politiques par les polices de certains États européens à l'aide d'un *spyware*, Pegasus, conçu par l'entreprise NSO, ont fait réagir la sphère politique et institutionnelle dans le sens d'une demande de restriction, voire d'interdiction, de ce type de pratiques, en raison de l'atteinte disproportionnée aux droits fondamentaux.

Ainsi, le Haut-Commissariat des Nations Unies aux droits de l'homme a condamné les possibilités offertes par les logiciels espions [14]. En juin 2023, le Parlement européen a adopté des recommandations pour lutter contre l'utilisation abusive des logiciels espions [15]. De nouveaux scandales concernant les « Predator Files » et le logiciel « Paragon » ont, depuis, confirmé l'ampleur des dangers pour les équilibres démocratiques et les libertés individuelles que présente ce type de surveillance. La société civile demande elle aussi l'interdiction de ces outils, comme Amnesty International qui, suite à son enquête sur le logiciel Pegasus, s'est prononcée en faveur d'« *un moratoire mondial sur la vente, le transfert et l'utilisation des logiciels espions* » [16], ou encore du European Digital Rights qui demande « *une interdiction* [des techniques de] *hacking développées par les États* » [17].

Il en résulte que, en autorisant ce type de surveillance par compromission des appareils, le législateur a porté une atteinte manifestement disproportionnée au droit à la vie privée et à la liberté d'expression.

VII. Sur la création d'un procès verbal distinct (article 40)

Les dispositions de l'article 40 de la loi déférée sont contraires aux articles 2, 6, 11 et 16 de la Déclaration de 1789 en ce qu'elles introduisent une procédure inédite dénommée « dossier-coffre », ou « procès-verbal distinct », consistant à ne pas verser au contradictoire certains actes de procédure, notamment des actes relatifs à des mesures de surveillance.

<u>En droit</u>, comme rappelé précédemment, des articles 2 et 11 de la Déclaration de 1789 sont protégés respectivement le droit à la vie privée et la liberté d'expression.

---

14. Haut-Commissariat aux droits de l'homme, « Logiciels espions et surveillance : un rapport de l'ONU met en garde contre les menaces croissantes pour la vie privée et les droits de l'homme », 16 septembre 2022, URL : https://www.ohchr.org/fr/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

15. « Logiciels espions : les députés demandent des enquêtes complètes et des garanties pour prévenir les abus », 15 juin 2023, URL :https://www.europarl.europa.eu/news/fr/press-room/20230609IPR96217/logiciels-espions-le-pe-souhaite-des-enquetes-completes-et-des-garanties

16. https://www.amnesty.fr/militants-surveillance-numerique-ciblee

17. https://edri.org/wp-content/uploads/2022/10/Position-Paper-State-access-to-encrypted-data.pdf, p. 22

Par ailleurs, le Conseil constitutionnel dégage des articles 6 et 16 de la Déclaration un droit au procès équitable (*cf.* Cons. const., 1er avril 2011, *Mme Marielle D. [Frais irrépétibles devant la Cour de cassation]*, no 2011-112 QPC, cons. 3) duquel découle un droit au recours effectif (*cf.* Cons. const., 17 décembre 2010, *M. Boubakar B. [Détention provisoire : réserve de compétence de la chambre de l'instruction]*, no 2010-81 QPC, cons. 4 ; Cons. const., 13 juillet 2011, *M. Samir A. [Appel des ordonnances du juge d'instruction et du juge des libertés et de la détention]*, no 2011-153 QPC, cons. 3 ; Cons. const., 23 juillet 2010, *Région Languedoc-Roussillon et autres [Article 575 du code de procédure pénale]*, no 2010-15/23 QPC, cons. 4). Il exige alors qu'une différence de traitement soit justifiée, par exemple par « *la protection du respect de la vie privée, la sauvegarde de l'ordre public ou l'objectif de recherche des auteurs d'infraction, auxquels concourt le secret de l'information* » (*cf.* Cons. const., 16 septembre 2016, *Mme Marie-Lou B. et autre [Communication des réquisitions du ministère public devant la chambre de l'instruction]*, no 2016-566 QPC, § 9), et qu'elle soit également accompagnée de garanties équivalentes (*cf.* Cons. const., 25 janvier 2024, *Loi pour contrôler l'immigration, améliorer l'intégration*, no 2023-863 DC, § 241).

Ce principe d'égalité des armes est également reconnu par la CEDH (*cf.* CEDH, 18 mars 1997, *Foucher c. France*, no 22209/93, § 26–37) et par la CJUE, dont le Conseil constitutionnel pourra utilement s'inspirer. La CJUE considère que, en principe, « *ce serait violer le droit fondamental à un recours juridictionnel effectif que de fonder une décision juridictionnelle sur des faits et des documents dont les parties elles-mêmes, ou l'une d'entre elles, n'ont pas pu prendre connaissance et sur lesquels elles n'ont donc pas été en mesure de prendre position* » (*cf.* CJUE, 4 juin 2013, *ZZ contre Secretary of State for the Home Department*, aff. C-300/11, pt. 56).

Ce n'est que par exception que la CJUE estime que, si une décision a été prise sur la base d'informations potentiellement secrètes, « *le juge compétent de l'État membre concerné doit avoir à sa disposition et mettre en œuvre des techniques et des règles de droit de procédure permettant de concilier, d'une part, les considérations légitimes de la sûreté de l'État quant à la nature et aux sources des renseignements ayant été pris en considération pour l'adoption d'une telle décision et, d'autre part, la nécessité de garantir à suffisance au justiciable le respect de ses droits procéduraux, tels que le droit d'être entendu ainsi que le principe du contradictoire* » (pt. 57). Pour cela, l'État doit prévoir « *un contrôle juridictionnel effectif* [. . .] *de l'existence et du bien-fondé des raisons invoquées par l'autorité* [qui] *s'opposent à la communication des motifs précis et complets sur lesquels est fondée la décision en cause ainsi que des éléments de preuve y afférents* », et ce alors qu'« *il n'existe pas de présomption en faveur de l'existence et du bien-fondé de* [ce]*s raisons* » (pts. 58, 60 et 62).

La CJUE exige également que les personnes concernées soient informées par les autorités nationales des mesures de surveillance « *pour autant que et dès le moment où cette communication n'est pas susceptible de compromettre les missions qui incombent à ces autorités* ». Elle précise que « *cette information est, de fait, nécessaire pour permettre à ces personnes d'exercer leurs droits, découlant des articles 7 et 8 de la Charte, de demander l'accès à leurs données à caractère*

personnel faisant l'objet de ces mesures et, le cas échéant, la rectification ou la suppression de celles-ci, ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la Charte, un recours effectif devant un tribunal » (*cf.* CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e.a.*, préc., pt. 190 ; CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige et Watson e.a*, aff. C-203/15 et C-698/15, pt. 121). De même, la CEDH rappelle que l'existence d'un recours effectif est nécessaire à la mise en œuvre d'une surveillance secrète (*cf.* CEDH, gr. ch., 4 décembre 2015, *Roman Zakharov c. Russie*, n° 47143/06).

En l'espèce, le mécanisme prévu par l'article 40 de la loi déférée prévoit que certains actes de procédure ou certaines informations ne soient pas versés au contradictoire. Aux termes du 1° du nouvel article 706-104 du code de procédure pénale créé par l'article 40 de la loi déférée, ces éléments peuvent recouvrir « *la date* », « *l'heure* » et le « *lieu de la mise en place des dispositifs techniques d'enquête* ». C'est donc l'existence même d'une mesure de surveillance qui peut ainsi être cachée aux personnes mises en cause.

Premièrement, en empêchant ainsi aux personnes mises en cause de pouvoir connaître de l'existence d'une technique spéciale d'enquête, le législateur ne permet pas à la personne concernée par la mesure de surveillance ni d'être informée de cette technique, ni de pouvoir la contester. Il s'agit donc d'une atteinte grave au droit au recours effectif.

Or, **d'une part**, si le législateur a prévu que cette atteinte au principe du contradictoire ne peut être décidée que si le fait de révéler la mesure de surveillance « *est de nature à mettre gravement en danger la vie ou l'intégrité physique d'une personne, des membres de sa famille ou de ses proches* », le fait de dissimuler l'intégralité d'un acte n'est pas manifestement nécessaire pour atteindre cet objectif. En particulier, lors des premières phases de l'enquête, avant toute mise en examen et possibilité d'accès au dossier pénal par les personnes mises en cause, ce secret est déjà assuré. L'atteinte au droit au procès équitable n'est donc pas justifié.

D'autre part, cette atteinte n'est pas non plus accompagnée de garanties équivalentes. En effet, faute de pouvoir prendre connaissance de l'existence d'une mesure de surveillance, les personnes concernées ne pourront contester leur légalité. Cette absence de recours effectif est d'autant plus préjudiciable qu'il s'agit de techniques spéciales d'enquêtes, aux conditions légales strictes en raison de l'atteinte grave aux droits constitutionnellement protégés. Pire, le législateur n'a pas empêché qu'un acte d'enquête pris sur le fondement d'une mesure de surveillance dont le procès-verbal n'est pas versé au contradictoire puisse malgré tout orienter de nouvelles investigations dont les résultats permettront d'incriminer des personnes.

Deuxièmement, en ne permettant pas aux personnes concernées de contester les actes d'enquêtes non versés au contradictoire faute d'en avoir connaissance, la proportionnalité et le respect des règles procédurales de la technique de surveillance ne pourront pas être contestées. Ces dispositions empêchent donc un acte portant une atteinte disproportionnée au droit au respect de la vie privée ou à la liberté d'expression d'être contesté.

Il en résulte que les dispositions de l'article 40 de la loi déférée portent une atteinte manifestement disproportionnée au droit au procès équitable, au droit au respect de la vie privée et à la liberté d'expression.

VIII. Sur l'élargissement des personnes concernées par les enquêtes administratives (I de l'article 54)

Le I de l'article 54 de la loi déférée est contraire à l'article 1er de la Constitution et 6 de la Déclaration de 1789 en ce qu'il élargit le champ des enquêtes administratives prévues par l'article L. 114-1 aux « *emplois publics et privés exposant leurs titulaires à des risques de corruption ou de menaces liées à la criminalité organisée* ».

En droit, l'article 1er de la Constitution de 1958 dispose que la France « *assure l'égalité devant la loi de tous les citoyens sans distinction d'origine, de race ou de religion* ». De plus, l'alinéa 5 du Préambule de la Constitution de 1946 prévoit que « *nul ne peut être lésé, dans son travail ou son emploi, en raison de ses origines, de ses opinions ou de ses croyances* ». Le Conseil constitutionnel tire de ces dispositions, ainsi que de l'article 6 de la Déclaration de 1789, un principe d'égalité, qui se traduit par l'interdiction de certaines discriminations (*cf.* Cons. const., 15 novembre 2007, *Loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile*, no 2007-557 DC, cons. 29 ; Cons. const., 14 août 2003, *Loi portant réforme des retraites*, no 2003-483 DC, cons. 25 ; Cons. const., 29 mars 2018, *M. Rouchdi B. et autre*, no 2017-695 QPC, § 28–29)

En l'espèce, les enquêtes administratives visées l'article L. 114-1 du code de la sécurité intérieure qui est élargi par les dispositions de l'article 54 de la loi déférée peuvent être mises en œuvre pour « *vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées* ». Elles peuvent alors conditionner les « *décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation* » liées à ces emplois.

D'une part, le périmètre des fichiers consultés pour réaliser ces enquêtes est devenu extrêmement large. Comme l'explique la CNIL sur son site internet[18] :

> « *Lorsqu'ils sont chargés d'une enquête administrative de sécurité, les services compétents peuvent consulter un certain nombre de fichiers. Il s'agit principalement :*
>
> — *du "traitement d'antécédents judiciaires" (TAJ) ;*
> — *du "fichier des personnes recherchées" (FPR) ;*
> — *du fichier des "enquêtes administratives liées à la sécurité publique" (EASP) ;*
> — *des fichiers de "prévention des atteintes à la sécurité publique" (PASP) et de*

18. CNIL, « Les enquêtes administratives de sécurité », 4 avril 2023, URL : `https://www.cnil.fr/fr/les-enquetes-administratives-de-securite`

"gestion de l'information et prévention des atteintes à la sécurité publique" (GIPASP) ;

— *du fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) ;*
— *du système d'information Schengen (SIS) ;*
— *du fichier des objets et véhicules signalés (FOVeS).*

Le système ACCReD (automatisation de la consultation centralisée de renseignements et de données), créé en 2017, permet de consulter automatiquement et simultanément, via une interconnexion, tous les fichiers précédents. Il est utilisé par le service national des enquêtes administratives de sécurité (SNEAS).

En outre, selon les motifs de l'enquête administrative et les services en charge de l'enquête, d'autres fichiers, en particulier de services de renseignements, peuvent être consultés : par exemple, CRISTINA, géré par la direction générale de la sécurité intérieure (DGSI) du ministère de l'Intérieur, ou GESTEREXT, mis en œuvre par la direction du renseignement de la préfecture de police de Paris (DRPP). »

La CNIL exigeait ainsi en 2019 que soit précisé le périmètre de ces enquêtes, d'autant qu'elles « *conditionnent l'adoption de décisions administratives nombreuses, très diverses et ne présentant pas toutes le même degré de sensibilité* »[19].

D'autre part, certains de ces fichiers consultés permettent de donner des informations sensibles sur les personnes, et notamment sur les opinions politiques.

Premièrement, le fichier dit « traitement d'antécédents judiciaires (TAJ) » rassemble les informations de toute personne ayant eu affaire à l'autorité judiciaire, même si la personne n'a pas fait l'objet de poursuite ou a été ensuite relaxée. Or, le fichier TAJ comprend de nombreuses données incorrectes, ce qui a conduit récemment à une décision par la CNIL de rappel à l'ordre et d'injonction de se mettre en conformité à l'encontre du ministère de la justice et de celui de l'intérieur[20]. Un rapport parlementaire de 2018 dénonçaient le dévoiement de sa finalité première « *pour se rapprocher du rôle du casier judiciaire* ». Les auteurs précisaient que « *le fait que le TAJ contienne de nombreuses informations inexactes (erreurs diverses, absence de prise en compte de suites judiciaires favorables par l'effacement des données ou l'ajout d'une mention) peut en effet avoir des conséquences extrêmement lourdes pour les personnes concernées par une*

19. CNIL, Délibération n° 2019-096 du 11 juillet 2019 portant avis sur un projet de décret modifiant le décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD), URL : `https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000039258453`

20. CNIL, Délibération de la formation restreinte n° SAN-2024-017 du 17 octobre 2024 concernant le ministère de l'intérieur et des Outre-Mer et le ministère de la justice. URL : `https://www.cnil.fr/fr/traitement-dantecedents-judiciaires-la-cnil-rappelle-lordre-deux-ministeres`

enquête administrative »[21].

Deuxièmement, sont consultés, pour mener les enquêtes administratives prévues par l'article L. 114-1 du code de la sécurité intérieure, des fichiers de renseignement politique comme le PASP et le GIPASP, au champ extrêmement large : opinions politiques, état de santé, activités sur les réseaux sociaux ou encore convictions religieuses. Police nationale et gendarmerie nationale sont autorisées à collecter avec ces fichiers de nombreuses informations sur les personnes « *dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique ou à la sûreté de l'État* ». Cette définition large et floue permet en pratique de cibler de nombreuses personnes, et notamment des personnes ayant des activités militantes.

Troisièmement, d'autres fichiers interrogés sont classés secret-défense ou font l'objet de décrets non publiés. Il est donc impossible de savoir précisément ce que contiennent ces fichiers et qui y a accès. Il en est ainsi du fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) et du fichier CRISTINA (« Centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux »), mis en œuvre par la direction générale de la sécurité intérieure (DGSI), ou du fichier GESTEREXT (« Gestion du terrorisme et des extrémistes à potentialité violente ») géré par la direction du renseignement de la préfecture de police de Paris (DRPP).

Une enquête administrative permet donc d'accéder à de nombreuses informations sur la vie privée et les opinions d'individus ayant fait le choix de postuler aux emplois concernés. De plus, il n'existe aucun critère dans la loi définissant la notion de « *comportement des personnes physiques ou morales* [...] *incompatible avec l'exercice des fonctions ou des missions envisagées* » avec l'exercice des fonctions concernées. Ainsi, à l'été 2024, plus d'un millions d'enquêtes administratives ont été conduites sur les personnes devant travailler dans le cadre des Jeux Olympiques, ceux-ci ayant été qualifiées de « grand évènement ». Or, de nombreux témoignages récoltés par La Quadrature du Net ont révélé que certaines personnes n'ont pas pu obtenir leur accréditation du fait de la présence dans ces fichiers d'informations liées à des activités militantes[22]. Loin d'être des cas isolés, les situations de discrimination documentées sont le résultat direct des largesses actuelles de l'article L. 114-1 du code de la sécurité intérieure, que les dispositions de l'article 54 de la loi déférée veulent pourtant étendre.

En étendant le champ de ces enquêtes administratives, au périmètre large et dont les modalités ne sont pas définies par la loi, à une catégorie aussi vaste et floue que « *les emplois publics et privés exposant leurs titulaires à des risques de corruption ou de menaces liées à la criminalité organisée* », catégorie qui peut potentiellement concerner des millions d'emplois, les dispositions de l'article 54 de la loi déférée créent de ce fait une potentialité de décisions discriminatoires,

21. Didier Paris, Pierre Morel-À-L'Huissier, *op. cit.*, p. 58.

22. « Jeux Olympiques : fichage de masse et discrimination politique », 30 juillet 2024, URL : `https://www.laquadrature.net/2024/07/30/jeux-olympiques-fichage-de-masse-et-discrimination-politique/`

fondées uniquement sur des informations présentes dans des fichiers aux critères arbitraires et opaques.

Il en résulte que cet article porte une atteinte manifestement disproportionnée au principe d'égalité. Le Conseil constitutionnel pourra ici opportunément adopter un contrôle *in concreto* pour relever l'inconstitutionnalité de ces dispositions.

IX. Sur l'autorisation des drones par l'administration pénitentiaire (III de l'article 56)

Les dispositions du III de l'article 56 de la loi déférée autorisent, en violation des articles 2 et 11 de la Déclaration de 1789 et des articles 34 et 66 de la Constitution, l'administration pénitentiaire à utiliser des caméras installées sur des aéronefs pour effectuer des missions de surveillance des lieux de détention.

En droit, comme rappelé précédemment, il est de jurisprudence constante que la liberté proclamée par l'article 2 de la Déclaration de 1789 implique le droit au respect de la vie privée. Le Conseil constitutionnel admet ainsi que la surveillance par caméras consiste en une atteinte au droit au respect de la vie privée, que les caméras soient fixes (*cf.* Cons. const., 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, n° 94-352 DC, cons. 3 et 4 ; Cons. const., 20 mai 2021, *Loi pour une sécurité globale préservant les libertés*, préc., § 88 et 96) ou mobiles (*cf.* Cons. const., 20 mai 2021, *Loi pour une sécurité globale préservant les libertés*, préc., § 114, 126 et 135), et exige ainsi que le législateur prévoie des garanties particulières de nature à sauvegarder ce droit.

Appliqué au cas de drones de surveillance, si le Conseil constitutionnel a laissé aux juridictions administratives le soin d'apprécier au cas par cas la proportionnalité d'autorisations de drones par la police nationale ou la gendarmerie nationale en application des dispositions du code de la sécurité intérieure, c'est en précisant que de telles mesures de surveillance ne puissent être autorisées qu'en l'absence d'autre moyen moins intrusif en ce qui concerne les droits et libertés constitutionnellement protégés (*cf.* Cons. const., 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure*, n° 2021-834 DC, pt. 27).

De plus, la surveillance de l'espace public peut avoir un effet dissuasif sur la liberté d'expression protégée par l'article 11 de la Déclaration de 1789. Le Conseil constitutionnel a par exemple reconnu que la surveillance d'un grand nombre de personnes par la collecte de façon indifférenciée d'importants volumes de données est de nature à dissuader les personnes d'utiliser ces sites et porte donc atteinte à la liberté d'expression (*cf.* Cons. const., 27 décembre 2019, *Loi de finances pour 2020*, préc., pt. 82). Ce principe trouve parfaitement à s'appliquer au cas d'une surveillance de l'espace public, dans le prolongement notamment de la Cour européenne des droits de l'homme concernant la surveillance physique de journalistes, qui estime que les questions de surveillance physique ne peuvent pas être appréhendées du seul point de vue du droit à la vie pri-

vée (*cf.* CEDH, 22 novembre 2012, *Telegraaf Media Nederland Landelijke Media B.V. et autres c. Pays-Bas*, n° 39315/06, pts. 84–88).

Par ailleurs, du principe de séparation des pouvoirs tiré de l'article 66 de la Constitution découle une impossibilité pour le législateur de confier au pouvoir exécutif des missions de police judiciaire, et notamment d'autoriser l'autorité administrative de mettre en œuvre des mesures de surveillance visant à « *réprimer* » des actes.

Enfin, comme rappelé précédemment, il ressort des articles 6 et 16 de la Déclaration de 1789 un droit droit au recours effectif, composante du droit à un procès équitable, et de l'article l'article 34 de la Constitution l'obligation, pour le législateur, d'exercer pleinement sa compétence.

En l'espèce, les dispositions de l'article 56 de la loi déférée autorisent l'administration pénitentiaire à utiliser des caméras sur aéronefs, aussi appelés « drones ». Pour ce faire, cet article crée une section intitulée « *Caméras installées sur des aéronefs* » au code pénitentiaire, fortement inspirée des articles L. 242-1 à L. 242-8 du code de la sécurité intérieure qui autorisent déjà aujourd'hui l'usage de drones à des fins de missions de police administrative par la gendarmerie nationale et la police nationale. Une telle extension irait à l'encontre de plusieurs principes constitutionnels.

Premièrement, la rédaction de cette nouvelle section du code pénitentiaire va à l'encontre du principe de séparation des pouvoirs de l'article 66 de la Constitution, dont découle l'impossibilité de confier au pouvoir exécutif des missions de police judiciaire. Le 4° du I. de l'article L. 223-21 du code pénitentiaire créé par l'article 56 de la loi déférée permettrait à l'administration pénitentiaire de mobiliser des drones pour « *Le constat des infractions et la poursuite de leurs auteurs par une collecte de preuves* ». Pourtant, les mesures de surveillance mises en œuvre par l'administration pénitentiaire se rattachent à des missions de police administrative et relèvent de la compétence de l'ordre administratif (*cf.* CE, 28 décembre 2009, n° 328768, Rec. T. p. 823 ; CE, 30 décembre 2015, n° 383294). Il en va de même pour le renseignement pénitentiaire, qui relève de missions de police administrative (*cf.* art. L. 855-1 du code de la sécurité intérieure ; Cons. const., 21 mars 2019, *Loi de programmation 2018-2022 et de réforme pour la justice*, préc., pt. 342).

Ainsi, les dispositions du III de l'article 56 de la loi déférée, en prévoyant que les drones que peut déployer l'administration pénitentiaire puissent poursuivre une finalité de constatation d'infractions – finalité qui, au demeurant, ne figure pas à l'article L. 242-4 du code de la sécurité intérieure dont il s'inspire –, vont frontalement à l'encontre du principe de séparation des pouvoirs prévu à l'article 66 de la Constitution.

Deuxièmement, ces nouveaux pouvoirs accordés à l'administration pénitentiaire sont manifestement disproportionnés en ce qu'ils ne sont pas nécessaires. En effet, les juridictions administratives ont déjà établi que l'usage de drones pour surveiller des centres de rétention administrative (CRA) n'est pas nécessaire. Ainsi, le juge des référés du tribunal administratif de Marseille, saisi de la légalité d'un arrêté préfectoral autorisant la surveillance par drones du CRA du Canet, a

suspendu, sur le fondement de l'article L. 521-2 du code de justice administrative, cette décision, en relevant que le préfet des Bouches-du-Rhône n'apportait pas la preuve qu'il n'était pas possible de poursuivre les finalités de maintien de l'ordre invoquées sans procéder à une surveillance par drone du CRA, et alors même que le juge des référés ne remettait pas en cause l'existence de troubles importants à l'ordre public (*cf.* TA Marseille, ord., 14 décembre 2024, *Ordre des avocats au barreau de Marseille et La Cimade*, n° 2412733, pt. 9).

Appliqué au cas de la surveillance de lieux de détentions, l'usage de drones paraît donc radicalement disproportionné. Le législateur a, notamment, déjà octroyé à l'administration pénitentiaire de larges pouvoirs pour surveiller tant l'intérieur (art. L. 223-1 à 223-16 du code pénitentiaire) que les abords (art. L. 223-17 à L. 223-19 du code pénitentiaire) des établissements pénitentiaires, en sorte que les constations de l'absence de nécessité à surveiller par drones des CRA s'appliquent parfaitement au cas de la surveillance par drones d'un établissement pénitentiaire.

Troisièmement, les dipositions du III de l'article 56 de la loi déférée ne prévoient aucune forme de publicité des décisions autorisant l'administration pénitentiaire à recourir à des drones, niant ainsi le droit d'information des personnes et rendant impossible de fait le droit au recours effectif. Pourtant, le Conseil constitutionnel considère que la publication de telles décisions participe à la conformité à la Constitution de ce type de surveillance, l'usage de drones étant souvent imperceptible par les personnes concernées (*cf.* Cons. const., 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure*, préc., pt. 23). Au-delà de la question de l'information des personnes concernées par cette surveillance, qui est également une exigence européenne de laquelle le Conseil constitutionnel pourra utilement s'inspirer (*cf.* CJUE, gr. ch., 26 juillet 2017, *Accord PNR UE-Canada*, avis 1/15, pt. 219 ; CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige et Watson e.a*, préc., pt. 121 ; CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e.a.*, préc., pt. 190), la publicité des mesures de surveillance est une condition *sine qua non* pour pouvoir les contester utilement en justice. Pourtant, en ce qui concerne les usages actuellement autorisés de drones, l'obligation de publier les autorisations préfectorales au recueil des actes administratifs se heurte déjà à des pratiques abusives de l'administration. En effet, certaines préfectures ne publient que quelques jours – voire quelques heures – seulement avant le début de la mise en œuvre de la surveillance, rendant impossible en pratique la saisie en référé du juge administratif (lequel dispose théoriquement, en référé-liberté, de 48 heures pour rendre son ordonnance, délai très souvent dépassé en raison de la surcharge des tribunaux administratifs et de la complexité des affaires).

Le cas de la surveillance du CRA du Canet à Marseille est, à ce titre, un parfait exemple des limites actuelles de la loi. En effet, alors que le préfet des Bouches-du-Rhône a vu un premier arrêté autorisant la surveillance du CRA du Canet à Marseille suspendu par la justice administrative (*cf.* TA Marseille, ord., 14 décembre 2024, *Ordre des avocats au barreau de Marseille et La Cimade*, préc.), il a, au lieu de se conformer à l'esprit de l'ordonnance de référé et de mener ses missions de maintien de l'ordre sans surveillance par drones, adopté une stratégie de publication *in extremis* d'autorisations préfectorales de drones, aux motifs tous identiques, quelques heures

seulement avant le début de l'autorisation. Ce faisant, cette pratique du préfet des Bouches-du-Rhône rend impossible toute saisine utile du juge administratif, y compris en référé, un recours en excès de pouvoir n'intervenant au mieux que plusieurs mois avant l'introduction de la requête et étant donc insusceptible de prévenir un tel abus. Cette pratique de contournement de la justice a perduré de long mois, le préfet des Bouches-du-Rhône ayant adopté 20 arrêtés, publiés la veille ou quelques heures avant le début de la surveillance, le dernier datant du 31 mars dernier[23].

Le régime actuel de publication des arrêtés préfectoraux des articles L. 242-1 et suivants du code de la sécurité intérieure est donc déjà largement inefficace et ne permettre aucunement l'exercice du droit au recours effectif. Au lieu de s'inspirer de ces articles, le législateur aurait donc non seulement dû prévoir une publicité des autorisations ainsi délivrées, mais également un délai minimal de publication, afin de garantir le droit au recours effectif. En l'absence de telles garanties, le législateur a méconnu l'étendu de sa compétence au prix d'une atteinte manifestement disproportionnée au droit au respect de la vie privée et au droit au recours effectif.

Il en résulte que le III de l'article 56 de la loi déférée méconnaît gravement et manifestement les exigences constitutionnelles.

* *

*

Par ces motifs, La Quadrature du Net vous invite à déclarer contraires à la Constitution les dispositions du II de l'article 1er, celles de l'article 13, 15, 28, 29, 38, 39, 40 et celles du I de l'article 54 et III de l'article 56.

Je vous prie de croire, Monsieur le président, Mesdames et Mesieurs les membres du Conseil contsitutionnel, en l'assurance de ma plus respectueuse considération.

Pour La Quadrature du Net,
Noémie Levain

23. Liste des arrêtés du préfet des Bouches-du-Rhône autorisant des drones pour surveiller le CRA du Canet suite à l'ordonnance du juge des référés du TA de Marseille de décembre 2024 : https://attrap.fr/search?s=Canet+AND+%22centre+de+r%C3%A9tention%22+AND+a%C3%A9ronefs&administration=pref13&start_date=2024-12-22&sort=desc