[redacted]
La Quadrature du Net
[redacted]

Mesdames et Messieurs les députés de la
Commission des Lois
Assemblée nationale
126, rue de l'Université
75007 Paris

Paris, le 4 mars 2025.

Objet : Note sur la proposition de loi « visant à sortir la France du piège du narcotrafic »

Mesdames et Messieurs les députés,

Vous vous apprêtez à examiner la proposition de loi n° 907 « visant à sortir la France du piège du narcotrafic ». En tant qu'association spécialisée dans le domaine des libertés numériques, La Quadrature du Net est vivement opposée à l'adoption de ce texte.

D'une part, il introduit de nombreuses mesures de surveillance portant atteinte aux droits et libertés, ainsi qu'aux principes fondateurs de la procédure pénale et à la séparation des pouvoirs. D'autre part, ces mesures vont bien au-delà du seul trafic de stupéfiants, dès lors qu'elles s'appliquent à l'ensemble du régime de la délinquance et la criminalité organisée, aujourd'hui utilisé dans un nombre très large de situations et sur un nombre important de personnes, notamment des personnes ayant des activités militantes.

Cette note rassemble les éléments de compréhension, à la fois techniques et juridiques, nécessaires à un examen rigoureux du texte pour prendre la mesure des multiples atteintes aux libertés publiques qu'engendrerait l'adoption de ce texte. La note concerne les mesures que nous considérons comme les plus dangereuses. En l'état, si l'équilibre du texte n'était pas significativement renversé pour une meilleure protection des libertés publiques, La Quadrature du Net appelle à son rejet entier.

I. Étendue du régime de la criminalité organisée

Cette proposition de loi vient modifier lourdement le régime de la criminalité organisée, créé par la loi n° 2004-204 du 9 mars 2004, dite « Perben II », et dérogeant au droit commun pour certaines infractions. Ce régime autorise notamment le recours à des « techniques spéciales » d'enquête – similaires ou comparables à celles utilisés en renseignement – dès le stade de l'enquête préliminaire. Ces techniques spéciales sont davantage attentatoires aux libertés publiques. Le régime de la criminalité organisée permet notamment de déroger aux règles de droit commun applicables à la garde à vue et aux perquisitions.

La liste des infractions pour lesquelles les règles dérogatoires sont applicables est définie à l'article 706-73 du code de procédure pénale. Elle a été élargie à plusieurs reprises et vise aujourd'hui :

- un certain nombre de crimes et délits lorsqu'ils sont commis avec la circonstance aggravante de bande organisée (comme le meurtre, la torture, l'enlèvement et la séquestration la destruction, la dégradation et la détérioration d'un bien) ;
- les crimes et délits de trafic de stupéfiants ;
- le délit d'association de malfaiteurs lorsqu'il a pour objet la préparation de certaines infractions visées dans l'article 706-73 du code de procédure pénale, dont le vol en bande organisée, l'extorsion, la destruction, la dégradation et la détérioration d'un bien commis en bande organisée, le détournement d'un moyen de transport, les délits d'armes ou de produits explosifs ou encore les crimes et délits d'aide à l'entrée, à la circulation et au séjour irréguliers d'un étranger en France commis en bande organisée.

Le champ d'application de ce régime dérogatoire dépasse donc largement les seules infractions liées au trafic de stupéfiants.Ainsi, les infractions commises en bande organisée présentes dans la liste, de même que l'association de malfaiteurs pour les infractions visées à l'article 706-73 du code de procédure pénale, ont pu être utilisées dans de nombreuses affaires visant des actions ou groupes militants :

- Lors du mouvement des Gilets jaunes, en 2019 [1] :
  - Dans la Drôme, quatre personnes sont mise en examen pour « association de malfaiteurs en vue de commettre des destructions par substance incendiaire et explosive, tentative de destructions aggravées et vols aggravés ».
  - À Toulon, deux personnes soupçonnées d'avoir préparé des engins incendiaires sont déférés devant un juge d'instruction en vue d'une mise en examen pour « association de malfaiteurs » et « transport de substances incendiaires ».
  - À Toulouse, un homme est mis en examen et placé en détention provisoire pour « as-

1. Exemples tirés de l'article « L' association de malfaiteurs – De Napoléon aux Gilets jaunes, histoire et réflexion autour d'un outil juridique et policier » disponible à l'adresse suivante : `https://lundi.am/L-association-de-malfaiteurs`.

sociation de malfaiteurs en vue de commettre des dégradations ».

— À Bure, des personnes luttant contre l'enfouissement des déchets nucléaires ont notamment été poursuivies pour « participation à une association de malfaiteurs des délits de dégradation en réunion et par des personnes dissimulant volontairement leur visage » et « détention en bande organisée de substance ou produit incendiaire ou explosif ou d'éléments composant un engin incendiaire ou explosif pour préparer une destruction, dégradation ou atteinte aux personnes ». Elles ont été relaxées de ces chefs d'inculpation. Néanmoins, une surveillance accrue a été permise en amont, grâce à la qualification d'infractions relevant du régime de la criminalité organisée [2].

— Lors d'une manifestation en novembre 2019, un manifestant a été placé en garde à vue pour « association de malfaiteurs en vue de commettre des dégradations sur des bâtiments publics » pour avoir construit un homard géant de papier mâché et polystyrène ainsi qu'une banderole, et possédé des ballons de baudruche en forme de homard. Le juge d'instruction n'a ensuite pas suivi cette qualification du procureur [3].

— À Briançon, des personnes militant pour l'aide aux personnes exilées ont été poursuivies des faits d'aide à l'entrée et à la circulation de personnes en situation irrégulière en bande organisée. Cette circonstance aggravante a ensuite été écartée par la justice [4].

— Deux actions militantes contre le cimentier Lafarge ont été qualifiées d'infractions relevant du régime de la délinquance et la criminalité organisée. À Bouc-Bel-Air, près de Marseille, la qualification retenue de « dégradation et destruction en bande organisée » et « association de malfaiteurs » [5] ont notamment permise la mise en place de moyens de surveillance très importants. À Évreux, des personnes s'étant introduit dans une usine ont été poursuivies pour association de malfaiteurs et « dégradations en réunion et sur un site destiné au stockage de marchandises », punies de sept ans d'emprisonnement et 100 000 euros d'amende.

Pour toutes ces situations, la qualification par le parquet d'infractions relevant du régime de la délinquance et criminalité organisée a permis d'avoir accès aux techniques spéciales d'enquêtes, autrement interdites, et de déroger aux règles de procédure pénale en matière de garde à vue et de perquisition.

---

2. Toutes les informations relatives à la procédure sont disponibles sur le site `https://noussommestousdesmalfaiteurs.noblogs.org/`.

3. Mediapart, « A Nantes, 48 heures de garde à vue pour un homard de carnaval », 17 septembre 2019 : `https://www.mediapart.fr/journal/france/170919/nantes-48-heures-de-garde-vue-pour-un-homard-de-carnaval`

4. Communiqué de la Ligue des droits de l'Homme : « Relaxe pour "les 7 de Briançon" », 10 septembre 2019, `https://www.ldh-france.org/relaxe-pour-les-7-de-briancon/`

5. Voir France 3 Régions, « Action écologiste contre la cimenterie Lafarge : "réprimés comme des terroristes", retour en quatre actes sur le sabotage des activistes »`https://france3-regions.francetvinfo.fr/provence-alpes-cote-d-azur/bouches-du-rhone/aix-en-provence/action-ecologiste-contre-la-cimenterie-lafarge-retour-en-quatre-actes-sur-le-sabotage-d-une-cimenterie-du-groupe-lafarge-par-des-activistes-2950727.html`

On constate donc que les exemples sont nombreux de dévoiement de ce régime d'exception, pour des finalités bien différentes que la recherche de réseaux mafieux. La présente proposition de loi s'inscrit dans le prolongement de ce phénomène. Contrairement à ce que l'intitulé du texte le laisse entendre, les importantes modifications du régime de la criminalité organisée contenues dans la proposition de loi auront donc une application bien plus large que le trafic de stupéfiants. L'article 9 du texte tend d'ailleurs à étendre encore plus ce périmètre.

II. Principales mesures attentatoires aux libertés

Article 1er – Échange d'informations entre les services de renseignement

Le III de l'article 1er de la proposition de loi propose de supprimer une limite essentielle à la transmission des informations entre services de renseignement.

Avant la réforme de la loi no 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, l'article L. 863-2 du code de la sécurité intérieure était très souple, autorisant les services de renseignement à « *échanger toutes les informations utiles à l'accomplissement de leurs missions* ».

Désormais, l'article L. 822-3 du code de la sécurité intérieure encadre plus précisément les échanges d'informations entre services, en exigeant que les services 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 notamment de s'assurer que le partage n'ait pas comme conséquence de contourner les limites prévues par la loi. Le Premier ministre et la CNCTR s'assurent également que le partage de renseignement soit proportionné et conforme aux règles du code de la sécurité intérieure. Pour permettre le contrôle des partages par les services de renseignement, l'article L. 822-4 prévoit la mise en œuvre de relevés tenus 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 rappelle que l'encadrement de ces transmissions d'informations était nécessaire pour la bonne garantie des 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 [6] :

> « *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, l'article 1er de la proposition de la loi 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. Selon l'exposé des motifs de l'amendement ayant introduit cette modification au Sénat, ce mécanisme d'autorisation constituerait une « lourdeur » procédurale. Un tel argument ne peut être entendable en matière d'atteinte au droit à la vie privée et de mesures de surveillance secrètes. Si ces garanties procédurales existent, c'est 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. De plus, le sénateur Perrin justifie cet amendement par le besoin d'échanges d'informations en matière de criminalité organisée, mais cette modification concernerait toutes les finalités de renseignement et bénéficierait à tous les services, spécialisés ou du « second cercle ».

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 [7].

Dès lors, en supprimant une telle autorisation, donc en ôtant l'étape de contrôle du Premier ministre et de la CNCTR, les risques d'abus et de violation des droits des personnes en seraient potentiellement démultipliées.

---

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

7. *Ibid.*, p. 79

Si la CNCTR a effectivement pointé des difficultés d'application du mécanisme introduit en 2021[8], la commission insiste sur le travail d'accompagnement des services qu'elle a essayé d'engager. De façon générale, si la procédure ne permet pas de satisfaire les objectifs de transparence et de contrôle des transmissions d'informations, il convient de les améliorer et non de simplement les supprimer. En l'état, le III de l'article 1er poursuit une démarche de diminution des droits en faisant disparaître des garanties offertes aux citoyens, sans les remplacer.

Nous appelons donc à la suppression de cette disposition et à entamer plutôt une discussion sérieuse pour améliorer les processus de limitation des pouvoirs d'échanges de renseignements entre services.

Article 6 – Partage d'information entre l'autorité judiciaire et les services de renseignement

L'article 6 élargit le champ des informations qui peuvent être communiquées entre l'autorité judiciaire et les services de renseignement. D'une part, cette disposition étend cette possibilité de signalement à tous les procureurs, alors qu'elle 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, comme cela a été rappelé précédemment, peuvent fonder des procédures visant des actions politiques ou militantes.

Au-delà de cet élargissement, c'est l'existence même de cette prérogative qui est contestable. La possibilité pour les procureurs de signaler des faits à des services de renseignement va frontalement 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. En effet, 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 (Cons. const., 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, no 2005-532 DC, cons. 5 ; v. également Cons. const., 23 juillet 2015, *Loi relative au renseignement*, no 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 (Cons. const., 21 mars 2019, *Loi de*

8. CNCTR, Rapport d'activité pour l'année 2023, pp. 119 et s., URL : `https://cms.cnctr.fr/uploads/CNCTR_Rapport_2023_VERSION_NUMERIQUE_b1cd8eda21.pdf`

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 celle-ci dispose d'informations relatives à une potentielle infraction, elle constitue la seule autorité légitime pour éventuellement 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 plutôt que les confier à la police administrative, qui elle ne dispose pas de pouvoirs répressifs ni de prérogatives de recherche d'infraction.

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* »[9].

Pourtant, la solution n'est pas de favoriser la transmission d'informations entre deux institutions aux missions divergentes, qui aura pour effet de renforcer les capacités de surveillance d'État. Elle est plutôt de mieux circonscrire et limiter les activités de renseignement, en passant par des interprétations restrictives dès lors qu'il s'agit de la finalité de « prévention de la criminalité et de la délinquance organisées » (6° de l'article L. 811-3 du code de la sécurité intérieure, mobilisée par les services de renseignement pour surveiller des militants) pour laisser toute sa place et sa légitimité aux missions de l'institution judiciaire.

La Quadrature du Net vous invite donc à supprimer l'article 6 de cette proposition de loi.

Article 8 – Boites noires

L'article 8 de la proposition de loi vise à étendre davantage le champ d'application de la technique de renseignement dite des « boites noires », ou de « l'algorithme », qui 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) ?). L'article 8 de la proposition de loi étendrait les possibilités d'utilisation de cette technique de renseignement aux fins de prévention de la criminalité et de la délinquance organisées.

9. *Ibid.*, p. 107.

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

En raison de son caractère hautement liberticide, cette mesure avait été limitée à la stricte lutte contre le risque terroriste et instaurée de façon expérimentale pour quelques années avec des obligations d'évaluation. Malgré des résultats qui semblent peu convaincants et des rapports d'évaluation manquants, cette technique a, depuis, été pérennisée et explicitement élargie à l'analyse des adresses web des sites Internet par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement. Depuis 2021, les adresses URL dites « complètes » peuvent être automatiquement analysées. Cela implique donc que des données très précises sur le « contenu » des communications peut être recherchées par les algorithmes ainsi mis en œuvre. 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 [10] ou d'une vidéo [11].

La Commission nationale de l'informatique et des libertés (CNIL) rappelait ce problème intrinsèque à l'analyse des URL complètes dans son avis sur la réforme de 2021 du droit du renseignement [12] :

> « *La Commission rappelle que ces données ont une nature particulière. Comme souligné 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 pro-*

10. Il suffit de regarder l'URL `https://www.laquadrature.net/2025/02/24/la-loi-narcotrafic-est-une-loi-de-surveillance-mobilisons-nous/` pour deviner le contenu de l'article.

11. Même si la seule lecture de l'URL `https://www.youtube.com/watch?v=dQw4w9WgXcQ` ne donne aucune information sur la nature de la vidéo, il suffit de consulter l'URL pour prendre connaissance du contenu de la communication.

12. 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`.

tection 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.

Le Conseil constitutionnel a, dans sa décision n°2015-713 DC du 23 juillet 2015 concernant la loi relative au renseignement, relevé (pt 55), au titre des garanties appliquées aux méthodes de recueil ou de traitement en cause, l'impossibilité de recueil de données portant sur "le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications". C'est notamment au regard de cette garantie et, conformément à l'analyse du Gouvernement, qui avait alors précisé que le dispositif des algorithmes ne porterait que sur des données de connexion (ou méta données) et non sur le contenu des communications, qu'il a déclaré conformes les techniques de renseignement précitées. »

Dans son dernier 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 à la prévention des ingérences étrangères, c'est donc un nouvel élargissement qui est proposé sans aucune clarté sur l'étendue de cette surveillance de masse.

La Quadrature du Net appelle donc à la suppression de cet article 8.

Article 8 *ter* – Obligation de mise en place d'une porte dérobée

L'article 8 *ter* modifie profondément l'article L. 871-1 du code de la sécurité intérieure en imposant aux intermédiaires techniques, dont les services de messageries chiffrées, y compris les messageries chiffrées de bout-en-bout (c'est-à-dire des services où l'intermédiaire technique par lequel transitent les conversations n'a pas, lui non plus, accès au contenu des messages), la mise en place de portes dérobées, ou *backdoors*, pour donner un accès aux contenus des correspondances aux services de renseignement.

Aujourd'hui, cet article impose déjà aux « *personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité* » (qui inclut, notamment, les messageries chiffrées, mais concerne possiblement tout intermédiaire technique tel qu'un hébergeur qui propose des fonctionnalités de chiffrement à ses utilisateurs) de collaborer avec les services de renseignement afin de permettre à ces derniers de déchiffrer le contenu de correspondances. Le fait de ne pas de conformer à une telle injonction est puni jusqu'à deux ans de prison et 150 000 euros d'amende par l'article L. 881-2 du même code. Toutefois, cet article, lu de manière restreinte, n'impose pas aux personnes concernées de compromettre leur sécurité lorsque le service qu'elles offrent ne leur permet pas de connaître le contenu des messages échangés.

Alors que le respect de cet article L. 871-1 du code de la sécurité aux droits fondamentaux

interroge, l'article 8 *ter* de la proposition de loi, loin de le questionner, l'étend considérablement. Ainsi, la réécriture de l'article L. 871-1 du code de la sécurité opérée obligerait désormais les personnes concernées à « *prendre dans un délai n'excédant pas soixante-douze heures les mesures techniques nécessaires afin de permettre aux agents autorisés d'accéder au contenu intelligible des seules informations, documents, données ou renseignements* » dont la collecte a fait l'objet d'une autorisation préalable. Les données en question peuvent être issues d'un accès aux données de connexion en différé ou en temps réel, de la mise en d'une « boites noires », d'une la géolocalisation en temps réel, d'un IMSI-catcher, ou encore d'interceptions de communication.

Surtout, le nouvel article L. 871-1 du code de la sécurité précise que les services concernés « *ne peuvent exciper d'arguments contractuels ou techniques qui y feraient obstacle* ». Dès lors, entreraient dans le giron de cette obligation de compromission de la confidentialité des communication une messagerie chiffrée de bout-en-bout.

Autrement dit, une telle obligation signifierait que tout fournisseur de moyen de chiffrement d'une communication serait tenu de mettre en place des mesures pour mettre à disposition le contenu des communications en cas de demande par un service de renseignement. Appliqué au cas d'une messagerie chiffrée de bout-en-bout, dont le service ne peut pas, par définition, avoir connaissance du contenu des messages échangés par le service fourni, cela signifie une obligation de mettre en place des portes dérobées, ou *backdoors*.

Techniquement, une porte dérobée peut prendre différentes formes. Dans tous les cas, il s'agit de donner à une personne tierce accès à une conversation dont elle n'est ni destinataire, ni expéditrice, et donc d'en avoir connaissance. Une obligation de mettre place une porte dérobée est incompatible avec le principe même d'une messagerie chiffrée de bout-en-bout. En effet, avec le chiffrement de bout-en-bout, seuls le destinataire et l'expéditeur ont connaissance du contenu des conversations, grâce à un échange de clés cryptographiques entre eux. Par nature, cela empêche l'intermédiaire technique par lequel transitent les messages d'avoir connaissance du contenu de ces conversations. Une porte dérobée aurait comme conséquence d'imposer l'existence d'une troisième clé cryptographique, en plus de celles du destinataire et de l'expéditeur, ou bien d'une copie de celles existantes. Métaphoriquement, cela reviendrait à avoir une troisième personne, inconnue, dans une conversation individuelle.

Par ailleurs, l'article 8 *ter* modifie d'autres dispositions du code de la sécurité intérieure afin de renforcer les obligations de collaboration, pour un champ plus large de services et opérateurs de communication qu'auparavant. Ces derniers seraient ainsi tenus d'autoriser, à des fins de contrôle, les membres et les agents de la CNCTR à entrer dans les locaux (modification de l'article L. 871-4 du code de la sécurité intérieure) et devraient procéder à la mise en place des techniques de renseignement tout en fournissant, sur ordre du Premier ministre, les informations, documents, données ou renseignements requis (modification de l'article L. 871-6 du code de la sécurité intérieure).

Les sanctions sont alourdies en cas de non respect de ces obligations renforcées. Lorsque

ces infractions sont commises à titre habituel, elles seraient désormais punies d'une amende de 1 500 000 euros. Pour les personnes morales, cette amende pourrait être portée à 2 % du chiffre d'affaires mondial moyen annuel hors taxes.

De plus, l'article 8 *ter* ajoute plusieurs dispositions au code des postes et communications électroniques pour forcer les intermédiaires techniques à mettre en place des mesures de surveillance. Ainsi, le I du nouvel article L. 34-18 du code des postes et des communications électroniques oblige les « hébergeurs » (au sens du Digital Services Act) à mettre en place ou à assurer « la mise en œuvre des moyens nécessaires pour exécuter » les techniques d'enquêtes numériques judiciaires suivantes :

— les saisies informatiques et interceptions lors d'instructions judiciaire ;
— les interceptions en matière de criminalité organisée ;
— les techniques spéciales d'enquête en matière de criminalité organisée : IMSI-catcher, pose de micro et de caméra, captation de données informatiques (qui englobe les spywares).

À nouveau, de telles obligations, notamment lorsqu'elles concernent l'interception de correspondances, impliquent l'accès au contenu des messages et communications chiffrées, dont la conséquence est, de fait, l'obligation pour les intermédiaires techniques de prévoir des portes dérobées dans leurs services.

De plus, la notion « d'enquête numérique judiciaire » n'étant pas un concept juridique existant en droit français, il est difficile de délimiter le champ d'application de cette disposition. Les dangers liés à ce flou juridiques sont décuplés par les sanctions pouvant aller jusqu'à une astreinte de 50 000 euros par jour en cas de refus, voire une suspension partielle ou totale du service en France.

Comme le répètent de nombreuses institutions, dont l'ANSSI et le Comité européen de la protection des données, une telle mesure affaiblirait le niveau de protection de l'ensemble des communications et menacerait la confidentialité des échanges de l'ensemble des utilisateurs des services chiffrés. Il n'existe pas de technique d'affaiblissement du chiffrement qui ne permettrait de viser que les activités criminelles : l'ensemble des citoyens seraient alors aussi potentiellement visé. Il n'existe pas non plus de technique d'affaiblissement du chiffrement qui ne profiterait qu'à des acteurs « bien intentionnés ». Si une faille est créée pour un État (police, justice, service de renseignements, …), elle sera alors disponible pour tous les autres acteurs (autres États, organisations criminelles, hackers, …) moins bien intentionnés [13].

La Quadrature du Net appelle donc à la suppression de cet article 8 *ter*.

13. Pour des explications techniques et juridiques approfondies, voir la position de l'Observatoire des libertés et du Numérique – dont La Quadrature du Net fait partie – relative au chiffrement et publiée en 2017. URL : `https://www.laquadrature.net/files/201701_Oln_chiffrementsecuritelibertes.pdf`

Article 12 – Extension de la censure administrative d'internet

L'article 12 de la loi modifie l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, relative à la censure administrative en ligne d'Internet.

Aujourd'hui, les agents de la plateforme Pharos peuvent exiger le retrait de tout contenu qu'ils jugeraient illégal parce qu'ils feraient l'apologie du terrorisme, seraient à caractère pédo-criminel ou, depuis la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, seraient relatifs à des actes de barbarie. L'article 12 de la proposition de loi vise à étendre très largement ces capacités de censure administrative en ajoutant à la liste des contenus pouvant faire l'objet d'une injonction de retrait tout contenu relatif au trafic de stupéfiants, incluant également des contenus liées à l'usage de drogues.

En effet, l'article 12 de la proposition de loi vise tous les contenus qui contreviennent aux articles 222-34 à 222-39, à l'exception de l'article 222-38, du code pénal, et à l'article L. 3421-4 du code de la santé publique. Cela inclut donc :

— le fait de diriger ou d'organiser un groupement ayant pour objet la production, la fabrication, l'importation, l'exportation, le transport, la détention, l'offre, la cession, l'acquisition ou l'emploi illicites de stupéfiants ;
— la production ou la fabrication illicites de stupéfiants ;
— l'importation ou l'exportation illicites de stupéfiants ;
— le transport, la détention, l'offre, la cession, l'acquisition ou l'emploi illicites de stupéfiants ;
— la cession ou l'offre illicites de stupéfiants à une personne en vue de sa consommation personnelle ;
— la provocation à ces infractions alors même que cette provocation n'a pas été suivie d'effet, ou le fait de présenter ces infractions sous un jour favorable ;
— la provocation même non suivie d'effet, à l'usage de substances présentées comme ayant les effets de substances ou plantes classées comme stupéfiants.

Ce spectre très large d'infractions risque de concerner de nombreuses situations qui n'ont aucun lien avec le trafic de drogues à proprement parler. Ainsi, des extraits de films ou de clips musicaux mettant en scène des réseaux de drogues ou des consommateurs sous un jour favorable pourraient ainsi rentrer dans le champ de cette censure. Breaking Bad, Transpotting, des clips de musique faisant référence à la légalisation du cannabis, ou encore plus trivialement des blagues ou mèmes sur internet rentreraient donc directement dans le champ de cette nouvelle disposition et pourraient faire l'objet d'une injonction de retrait. De la même manière, de nombreux sites internet de prévention, diffusant notamment de l'information sur les manières de consommer de la drogue de façon à réduire les risques pour la santé, pourraient également être qualifiés de « provocation à l'usage de stupéfiants ».

Ce mécanisme de censure administrative pose pourtant, 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 [14]) 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.

Par ailleurs, alors que le Conseil constitutionnel a déjà censuré des dispositions imposant des retraits sous 24 heures pour des contenus haineux ou une heure pour des contenus relatifs au terrorisme, délais à partir desquels de lourdes amendes pouvaient être imposées aux plateformes et intermédiaires techniques (Cons. const., 18 juin 2020, *Loi visant à lutter contre les contenus haineux sur internet*, n° 2020-801 DC), la conformité au droit de l'Union de telles possibilités de censures extra-judiciaires est actuellement questionnée [15].

Ainsi, cette modification de l'article 6-1 de la LCEN élargit de façon disproportionnée une capacité de censure administrative déjà très importante et non soumis au contrôle effectif d'un juge. Cette volonté de verrouiller les contenus diffusés sur internet ne peut que mener à des abus au regard du volume de contenus concerné, du caractère extra-judiciaire de ces censures, et de la largesse des qualifications qui pourraient être retenues.

Au regard des atteintes disproportionnées à la liberté d'expression et de création sur internet que cette mesure engendrerait, La Quadrature du Net appelle à la suppression de l'article 12 de la proposition de loi.

Article 12 *bis* – Collecte disproportionnée des données d'identification

L'article 12 *bis* de la proposition de loi crée un nouvel article L. 34-1-1 au code des postes et des communications électronique qui vise à imposer à tout « *service de communications interpersonnelles à prépaiement* » de collecter puis de conserver pendant 5 ans la preuve d'identité de l'acheteur.

Présentées, dans l'exposé des motifs de l'amendement ayant créé cet article 12 *bis*, comme visant les opérateurs fournissant des cartes SIM prépayées, ces dispositions sont en réalité beaucoup

14. TA Cergy-Pontoise, 4 février 2019, *Alexandre Linden*, nos 1801344, 1801346, 1801348, 1801352.

15. « Une coalition de 6 organisations attaque en justice le dangereux règlement de l'UE sur les contenus terroristes », 9 novembre 2023, URL : `https://www.laquadrature.net/2023/11/09/une-coalition-de-6-organisations-attaque-en-justice-le-dangereux-reglement-de-lue-sur-les-contenus-terroristes/`

plus larges. Elles concerneront 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, seront donc concernées par ce nouvel article L. 34-1-1, notamment parce que la section dans laquelle est inséré cet article n'est aucunement limitée aux cartes SIM prépayées.

Par ailleurs, en imposant aux personnes fournissant une messagerie interpersonnelle prépayée de collecter l'identité civile de leurs utilisateurs, cet article 12 *bis* de la proposition de loi crée une ingérence beaucoup plus grave au droit à la vie privée et à la liberté d'expression que s'il ne faisait que leur permettre – sans les obliger – de collecter cette identité civile. La Cour européenne des droits de l'homme (ci-après « CEDH ») reconnaît pourtant, 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 (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. La Cour de Justice de l'Union européenne (CJUE) 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 (CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e.a.*, aff. C-511/18, C-512/18 et C-520/18, pt. 109).

La conformité au droit de l'UE d'une disposition nationale exigeant la conservation de données relatives au trafic est ainsi subordonnée à la circonstance que les données ainsi conservées ne puissent permettre de tirer des conclusions précises sur la vie privée des personnes concernées (CJUE, ass. plen., 30 avril 2024, *La Quadrature du Net e. a.*, aff. C-470/21). La CJUE considère ainsi 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*).

Or, la conservation de l'identité civile envisagée par l'article 12 *bis* de la proposition de loi 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.). Cela signifie que le service de messagerie interpersonnelle conservant ces informations relatives à l'identité civile pourra tirer des conclusions sur les personnes avec qui chaque utilisateur du service communique. 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 [16], 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.

Ainsi, une telle obligation de collecter l'identité civile irait à l'encontre du droit à la vie privée et à la liberté d'expression. La Quadrature du Net vous invite dès lors à rejeter cet article 12 *bis*.

Article 15 – Présomption d'habilitation pour les fichiers d'antécédents

Le I de l'article 15 de la proposition de loi permet de déroger aux règles de consultation des fichiers d'antécédents judiciaires prévus par l'article 230-10 du code de procédure pénale. Cette disposition liste l'ensemble des personnes habilitées à accéder aux informations figurant dans les traitements de données à caractère personnel relatives à ces fichiers, plus connus sous le nom de fichier « traitement d'antécédents judiciaires (TAJ) ».

L'article R. 40-28 du code de procédure pénale précise qu'ont accès au TAJ « *pour les besoins des enquêtes judiciaires* » une liste exhaustive d'agents de service de la police nationale et des militaires des unités de la gendarmerie nationale, individuellement désignés et spécialement habilités.

Le fichier TAJ constitue un des fichiers les plus volumineux mis en œuvre par le ministre de la justice et le ministre de l'intérieur. Dans un rapport d'information de 2018 sur les fichiers mis à la disposition des forces de sécurité [17], il est ainsi indiqué qu'il « *existe 18,9 millions de fiches de personnes mises en cause* » par la police pour des crimes, des délits ou certaines contraventions (telles que des dégradations légères). Ce même rapport constate que le « *le TAJ comprend entre 7 et 8 millions de photos de face* » de personnes mises en cause.

Ce fichier est régulièrement critiqué pour l'absence de contrôle de l'exactitude des données ainsi que pour les retards dans la mise à jour et la suppression des informations contenues dans les fiches. Ainsi la CNIL a-t-elle récemment relevé l'existence de plusieurs manquements en lien avec les conditions dans lesquelles sont traitées les données personnelles figurant dans le fichier TAJ, prononçant un rappel à l'ordre à l'encontre des deux ministères pour leur enjoindre de prendre les

16. 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.

17. Didier Paris, Pierre Morel-À-L'Huissier, *Rapport d'information sur les fichiers mis à la disposition des forces de sécurité*, 17 octobre 2018, URL : `https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b1335_rapport-information.pdf`

mesures nécessaires au respect de la réglementation [18]

Surtout, le fichier TAJ est une des principales sources de dévoiement de fichiers par des agents de police qui utilisent ou revendent les informations contenus dans les traitements de données auxquels ils ont accès [19]. Dans son rapport pour l'année 2022, l'IGPN s'inquiétait ainsi de ce phénomène de détournement. Elle l'expliquait à la fois par « *la multiplication du nombre de fichiers de police (en particulier ceux dédiés aux antécédents judiciaires, TAJ, à la gestion des titres de séjour…) et une meilleure accessibilité* » [20]. Dans son rapport de l'année suivante, elle notait une nette augmentation du nombre de saisines pour détournements de fichiers, celles-ci s'élevant à 93 pour l'année 2023, contre 56 en 2022 et 38 en 2021 [21].

Face à ces éléments, et afin de limiter les risques d'abus et de détournement, une réforme législative du TAJ devrait donc conduire à restreindre les accès à ce fichier et à réduire les situations dans lesquelles les agents de police nationale et de gendarmerie nationale peuvent collecter et consulter des informations dans ce fichier.

C'est pourtant le choix inverse qui est fait dans l'article 15 de la proposition de loi. Il allonge, ignorant les alertes et sanctions relatives aux abus du fichier TAJ, la liste déjà vaste des personnes autorisées à consulter ce fichier en y ajoutant une large catégorie d'agents « *affectés dans les services spécialement chargés des enquêtes en matière de délinquance et de criminalité organisées* » qui ne seraient ni individuellement désignés, ni spécialement habilités.

Une telle présomption d'habilitation apparaît contraire au droit à la vie privée et à la législation relative aux données personnelles. Le 1 de l'article 4 de la directive UE n° 2016/680 du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données (ci-après directive « police-justice ») [22] prévoit pourtant que les données personnelles doivent non seulement être « *collectées pour des finalités déterminées,*

18. 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.legifrance.gouv.fr/cnil/id/CNILTEXT000050449791`

19. Voir, par exemple, le recensement par Mediapart des détournements entre 2013 et 2023 : Clément Le Foll, Camille Polloni, Clément Pouré, « Fichiers de police et de gendarmerie : dix ans de détournements », Mediapart, 11 février 2023, URL :`https://www.mediapart.fr/journal/france/110223/fichiers-de-police-et-de-gendarmerie-dix-ans-de-detournements`

20. IGPN, Rapport annuel pour l'année 2022, p. 59, URL : `https://www.police-nationale.interieur.gouv.fr/sites/policenationale/files/2023-09/Rapport%20annuel%20de%20l%27IGPN%20-%202022_0.pdf`

21. IGPN, Rapport annuel pour l'année 2023, p. 56, URL : `https://www.police-nationale.interieur.gouv.fr/sites/policenationale/files/2024-11/IGPN%20RA%202023.pdf`

22. La directive « police-justice » est l'équivalent du règlement UE n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « RGPD ») pour les traitements visant des finalités de police judiciaire ou de police administrative.

explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités », mais également être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées* ». Ce principe doit être interprété à la lumière de la jurisprudence précitée de la CEDH et de la CJUE. Dès lors, l'accès aux données doit également être mis en œuvre de façon restrictive, en application de ces principe de proportionnalité et de stricte nécessité.

Ainsi, pour la CJUE, « *s'agissant de l'accès d'une autorité à des données à caractère personnel, une réglementation ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette réglementation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation*» (CJUE, 6 octobre 2020, *Privacy International*, aff. C-623/17, pt. 77).

En outre, « *dès lors qu'un accès général à toutes les données conservées, en l'absence de tout lien, même indirect, avec le but poursuivi, ne peut être considéré comme étant limité au strict nécessaire, une réglementation nationale régissant l'accès aux données relatives au trafic et aux données de localisation doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause* » (CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige AB*, aff. C-203/15 et C-698/15, pt. 119). Un tel principe, dégagé à propos des données de connexion dans l'arrêt *Tele2 Sverige AB*, est bien entendu applicable aux données contenues dans un fichier.

La CJUE précise que l'accès aux données ne saurait ainsi « *être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction* » (même arrêt, pt. 119).

Le droit des données personnelles exige donc que l'accès aux données par la police ou la gendarmerie réponde à une logique de proportionnalité, ce qui signifie que les finalités du traitement doivent être interprétées de manière restrictive, en sorte que l'accès ne soit accordé que s'il permet de remplir concrètement l'objectif poursuivi. En outre, l'accès aux données ne doit pas être général mais avoir un lien direct, et recherché pour chaque accès, avec la finalité pour laquelle le traitement est autorisé.

Pour toutes ces raisons, La Quadrature du Net appelle à supprimer l'article 15 de la proposition de loi.

Articles 15 *ter* et 15 *quater* – Compromission des appareils et activation à distance des micros et des caméras

Les articles 15 *ter* et 15 *quater* de la proposition de loi visent à autoriser des techniques permettant d'activer, à distance, les appareils électroniques d'une personne à son insu pour capter des images et des sons. Une telle capacité de surveillance a déjà été censurée par le Conseil constitu-

tionnel (Cons. const., 16 novembre 2023, *Loi d'orientation et de programmation du ministère de la justice 2023-2027*, nº 2023-855 DC).

Cette technique de surveillance repose sur la compromission des 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 directement 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 concerneraient 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.

Il est, à cet égard, particulièrement inquiétant de voir que la France consacre dans le droit le fait d'exploiter les failles de sécurité des logiciels ou matériels utilisés plutôt que de s'attacher à les protéger en informant de l'existence de ces failles pour y apporter des remèdes. En effet, 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* conçu par l'entreprise NSO-Pegasus ont plutôt fait réagir la sphère politique et institutionnelle dans le sens d'une demande de restriction, voire d'interdiction, de ce type de pratiques. Ainsi, le Haut-Commissariat des Nations Unies aux droits de l'homme a condamné les possibilités offertes par les logiciels espions[23]. En juin 2023, le Parlement européen a adopté des recommandations pour lutter contre l'utilisation abusive des logiciels espions[24]. De nouveaux scandales concernant les « Perdator 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.

Plutôt que de voir un exemple à suivre dans ces pratiques extrêmement intrusives et de tenter de les rendre légitimes comme l'ont fait les sénateurs avec l'aval du gouvernement, il convient, bien au contraire, de les limiter et de les interdire fermement. La Quadrature du Net appelle donc à la suppression des articles 15 *ter* et 15 *quater*.

23. 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

24. « 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

Article 16 – Dossier coffre

L'article 16 de la proposition de loi introduit une procédure inédite dénommée « dossier-coffre », ou « procès-verbal distinct », consistant à ne pas verser au contradictoire certains actes de procédure.

Premièrement, cette mesure porte gravement atteinte aux principes fondateurs de la procédure pénale que sont le droit à se défendre et le contradictoire. Plus précisément une telle procédure empêchant les personnes poursuivies de connaître l'existence et les modalités de surveillance les concernant, donc de pouvoir les contester utilement, contrevient aux exigences européennes de protection des droits humains.

Ainsi, 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* » (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 Cour 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* » (*Ibid.*, 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* » (*Ibid*, 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* ». (CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e.a.*, préc., pt. 190 ; CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige AB*, préc., 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 (CEDH, gr. ch., 4 décembre 2015, *Roman Zakharov c/ Russie*, n° 47143/06).

Or en l'état, un tel recours effectif n'existe pas pour contester les techniques spéciales d'enquête mises en place par procès-verbal distinct.

Deuxièmement, la réécriture du mécanisme du dossier-coffre au Sénat par un amendement du gouvernement ne permet aucunement de pallier ces violations des droits fondamentaux. En effet, en l'état actuel du texte, un acte d'enquête pris sur le fondement d'une mesure de surveillance dont le procès-verbal n'est pas versé au contradictoire peut spécifier les éléments à « *corroborer* », afin d'orienter des « actes rebonds » ou de nouvelles investigations dont les résultats permettront d'incriminer des personnes. Or, à partir du moment où cette orientation de l'enquête repose sur le résultat d'une technique spéciale d'enquête non versée au contradictoire, la proportionnalité et le respect des règles procédurales de la première technique de surveillance ne pourront toujours pas être contestées.

L'analogie, faite par les défenseurs de ce dossier-coffre, avec la pratique de renseignement anonyme est totalement inopérante. En effet, pour ce type d'informations, l'exigence de confirmation par une autre technique d'enquête vient pallier la faible valeur probante et à la potentielle inexactitude des informations en question, qui ne peuvent être suffisantes pour fonder des poursuites. Tel n'est pas le cas dans la procédure du dossier-coffre, avec laquelle des éléments avérés et probants auront été collectés sans permettre à la défense de contrôler la légalité des moyens ainsi mis en œuvre, puis seront confirmés par une seconde mesure de surveillance qui n'agira alors que comme un vernis de légalité sur des faits que l'on sait certains mais obtenus par une technique très intrusive et potentiellement disproportionnée. Il s'agit, d'une certaine manière, d'organiser un « blanchiment de surveillance illégale ».

Troisièmement, une telle volonté de s'affranchir des règles de procédure pénale pour cacher certains éléments de l'enquête tend, d'une certaine manière, à vouloir transformer la police judiciaire en service de renseignement. Les services de renseignement sont la seule autorité pouvant à agir, au nom de l'efficacité, dans le secret. Mais cette action secrète, déjà éthiquement contestable et aux potentialités d'abus immenses, ne permet pas, en théorie, à l'administration de fonder la culpabilité des personnes. Il est impératif de rappeler que le secret n'est pas l'essence de l'autorité judiciaire. Celle-ci doit nécessairement rendre des comptes sur son action et la manière dont elle mène les enquêtes pour, sur cette base, déclarer la culpabilité et punir les personnes.

Enfin, une telle opacité sur les méthodes d'enquête de la police empêche toute documentation de la part de la population sur les capacités technologiques de surveillance que l'État peut mettre en place sur elle. Un tel rôle de vigie est notamment celui de La Quadrature du Net et de la presse d'investigation. Vouloir se soustraire à un tel contre-pouvoir, pourtant nécessaire en démocratie, est un affaiblissement majeur des conditions permettant la confiance des citoyens en l'État de droit.

Pour toutes ces raisons, nous appelons donc à la suppression de cet article 16.

Article 22 – Élargissement des personnes concernées par les enquêtes administratives

Le I de l'article 22 de la proposition de loi vise à élargir 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* ».

Pour rappel, ces enquêtes 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.

Comme l'explique la CNIL sur son site internet[25] :

> « *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 "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 présen-*

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

tant pas toutes le même degré de sensibilité[26] ». Certains de ces fichiers consultés appellent des commentaires plus précis.

Premièrement, le fichier 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. Comme rappelé précédemment à propos de l'article 15 de la proposition de loi, le fichier TAJ comprend de nombreuses données incorrectes. 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 enquête administrative* »[27].»

Deuxièmement, on trouve les 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 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 oeuvre 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 d'individus ayant fait le choix de postuler aux emplois concernés. 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 mili-

26. 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`

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

tantes [28].

Cet exemple démontre les conséquences concrètes que peut avoir la multiplication des fichiers de police liés à ce mécanisme d'enquête : être en capacité – à très grande échelle – d'exclure et contraindre des individus en dehors de tout cadre judiciaire et par des décisions administratives arbitraires qu'il est souvent compliqué pour les personnes de contester en justice. Cela peut se faire en dehors de toute condamnation passée, ou dans une forme de « double peine », possiblement à vie, en raison de condamnations pourtant parfois très limitées.

En étendant le champ des enquêtes administratives à une catégorie aussi large 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, l'article 22 crée de ce fait une potentialité de décisions discriminatoires, fondées uniquement sur des informations présentes dans des fichiers aux critères arbitraires et opaques. C'est pourquoi nous appelons à sa suppression.

Article 23 – Autorisation des drones dans le pénitentiaire

L'article 23 de la proposition de loi vise à autoriser l'administration pénitentiaire à utiliser des drones. Pour ce faire, cet article crée une section intitulée « Caméras installées sur des aéronefs » au code pénitentiaire, fortement inspiré du code de la sécurité intérieure qui autorise 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 actuelle 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. En effet, comme rappelé précédemment, le Conseil constitutionnel considère contraire au principe de séparation des pouvoirs de l'article 66 de la Constitution des dispositions confiant à l'autorité administrative des missions de police judiciaire (Cons. const., 19 janvier 2006, *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*, préc., cons. 5 ; Cons. const., 23 juillet 2015, *Loi relative au renseignement*, préc., cons. 9 ; Cons. const., 19 janvier 2023, *Loi d'orientation et de programmation du ministère de l'intérieur*, préc., pts. 70 et 80).

Or, l'article 23 de la position de loi permettrait à l'administration pénitentiaire de mobiliser des drones pour « *le constat des infractions et la poursuite de leurs auteurs par une collecte de*

28. « 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/

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 (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 (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*, n° 2019-778 DC, pt. 342).

Ainsi, en prévoyant que les drones que peut déployer l'administration pénitentiaire puissent poursuivre une finalité de constatation d'infractions, qui n'est pas présente dans le code de la sécurité intérieure en ce qui concerne les déploiements par la police nationale ou la gendarmerie nationale, irait 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 ne sont pas nécessaires. Il est constant qu'une mesure portant atteinte au droit à la vie privée ou à la liberté d'expression doit être nécessaire (Cons. const., 27 décembre 2019, *Loi de finances pour 2020*, n° 2019-796 DC pt. 82). Si le Conseil constitutionnel a laissé aux juridictions administratives le soin d'apprécier 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 (Cons. const., 20 janvier 2022, *Loi relative à la responsabilité pénale et à la sécurité intérieure*, n° 2021-834 DC, pt. 27).

Or, les juridictions administratives ont déjà établi l'absence de nécessité dans l'usage de drones pour surveiller des centres de rétention administrative (CRA). 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, 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 (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, cet article 23 ne prévoit 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 (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 (CJUE, gr. ch., 26 juillet 2017, *Accord PNR UE-Canada*, avis 1/15, pt. 219 ; CJUE, gr. ch., 21 décembre 2016, *Tele2 Sverige AB*, 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).

À titre d'exemple, alors que le préfet des Bouches-du-Rhône a vu un premier arrêté autorisant la surveillance du CRA du Canet à Marseille suspendu (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, adopté une stratégie de publication *in extremis* d'autorisations de drones, aux motifs tous quasiment identiques, quelques heures seulement avant le début de l'autorisation. Ce faisant, cette pratique du le préfet des Bouches-du-Rhône rend impossible toute saisine du juge administratif, y compris en référé. Aujourd'hui, cette pratique de contournement de la justice perdure, le préfet des Bouches-du-Rhône ayant, à ce jour, pris 15 arrêtés, publiés la veille ou quelques heures avant le début de la surveillance [29].

Le régime actuel de publication des arrêtés préfectoraux est donc déjà largement inefficace et ne permettre aucunement l'exercice du droit au recours effectif. C'est donc une refonte radicale du mécanisme d'autorisation qu'il faudrait entamer, accompagnée d'une publicité renforcée des autorisations, voire un abandon de la possibilité de mener des opérations de maintien de l'ordre à l'aide de drones, dont l'efficacité n'a, à ce jour, jamais été démontrée.

L'usage de drones est devenu massif – le journal *Le Monde* a comptabilisé 1 800 autorisations

29. 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&page=2&start_date=2024-12-22&sort=desc

sur la seule année 2024 [30] – alors que cette surveillance est censée être exceptionnelle. La légitimité de cette surveillance, présentée par ses défenseurs comme limitée aux situations où aucune autre mesure de maintien de l'ordre ne serait possible, devrait être discutée face à un déploiment de fait massif.

Cet article 23 s'engage pourtant dans la voie de l'opacité de ces mesures, qui pourront donc être massivement utilisées par l'administration pénitentiaire, alors que l'apport en matière de prévention des troubles à l'ordre public n'est pas démontré et qu'il est possible de poursuivre autrement cet objectif.

Or, l'actuel article 23 va à rebours de ces constations. En organisant l'opacité des autorisations de drone par l'administration pénitentiaire, il ne fait pas qu'empêcher purement et simplement toute contestation devant le juge. Il pose également les bases d'un déploiement de drones toujours plus large, toujours plus incontrôlé, pour des finalités toujours plus triviales et sans garantie effective pour les droits des personnes concernées. La Quadrature du Net vous invite donc à supprimer cet article.

* *

*

Pour ces raisons, La Quadrature du Net vous invite à rejeter les articles 1er, 6, 8, 12, 12 *bis*, 15, 15 *ter*, 15 *quater*, 16, 22 et 23. Si celles-ci demeuraient dans la version finale du texte, nous vous invitons à rejeter l'ensemble de la proposition de loi relative au narcotrafic.

Je vous prie de croire, Mesdames et Messieurs les députés, en l'assurance de ma plus respectueuse considération.

Pour La Quadrature du Net,

[redacted]

30. Arthur Carpentier, Léa Sanchez, « Comment la surveillance par drone s'est généralisée en 2024 : plus de 1 800 autorisations dans toute la France », Le Monde, 13 janvier 2025, URL : https://www.lemonde.fr/les-decodeurs/article/2025/01/13/comment-la-surveillance-par-drone-s-est-generalisee-en-2024-plus-de-1-800-autorisations-dans-toute-la-france_6495939_4355770.html