COMMISSION NATIONALE
DE L'INFORMATIQUE ET DES LIBERTÉS

PLAINTE AU TITRE DE L'ARTICLE 38 DE LA LOI N° 78-17 DU 6 JANVIER 1978

POUR :

1°) **L'association « La Quadrature du Net » (LQDN), association régie par la loi du 1er juillet 1901 dont le siège social est situé au 115, rue de Ménilmontant à Paris (75020), enregistrée en préfecture de police de Paris sous le numéro W751218406, représentée par [redacted], membre du collège solidaire en exercice**

2°) **Les 15 248 plaignants ayant mandaté La Quadrature du Net**

CONTRE : **Le ministre de l'intérieur**

Table des matières

PROCÉDURE

1. Aux termes de l'article 38 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « loi Informatique et Libertés ») :

> « *Toute personne peut mandater* […] *une association ou une organisation dont l'objet statutaire est en relation avec la protection des droits et libertés lorsque ceux-ci sont méconnus dans le cadre d'un traitement de données à caractère personnel* […] *aux fins d'exercer en son nom les droits prévus aux articles 77 à 79 et 82 du règlement (UE) 2016/679 du 27 avril 2016. Elle peut également les mandater pour agir devant la Commission nationale de l'informatique et des libertés, contre celle-ci devant un juge ou contre le responsable de traitement ou son sous-traitant devant une juridiction lorsqu'est en cause un traitement relevant du titre III de la présente loi.* »

2. De même, aux termes du 1 de l'article 77 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 ») :

> « *Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement.* »

3. La Quadrature du Net est une association de loi 1901 déclarée en préfecture le 5 février 2013. Elle prévoit dans ses statuts que « *l'Association a pour objet désintéressé et non lucratif la promotion et la défense des droits et des libertés fondamentales dans l'environnement numérique* », notamment, « *la promotion et la défense du droit à l'intimité, à la vie privée, à la protection de la confidentialité des*

communications et du secret des correspondances et à la protection des données à caractère personnel » et « *la lutte contre la surveillance généralisée ou politique, d'origine privée ou publique* ».

4. Du 24 mai au 24 septembre 2022, en application de l'article article 38 de la loi Informatique et Libertés, La Quadrature du Net a invité tout individu résidant en France à la mandater via son site `https://technopolice.fr/plainte` pour qu'il exerce, en son nom, les droits que lui confère l'article 38 de la loi Informatique et Libertés afin d'introduire la présente réclamation devant la Commission nationale de l'informatique et des libertés (ci-après « la CNIL »).

5. 15 248 plaignants ont ainsi mandaté La Quadrature du Net pour ce faire (la liste de leurs noms est jointe en annexe, *cf.* pièce n° 1).

DISCUSSION

6. L'installation de caméras de vidéosurveillance sur la voie publique par les pouvoirs publics est légalement encadrée depuis 1995. Peu de décomptes officiels du nombre de caméras sont effectués par la CNIL et le plus récent et accessible, en 2012, en dénombrait 70 003 [1].

7. Les atteintes aux libertés fondamentales engendrées par la vidéosurveillance dans une démocratie sont multiples, aussi bien concernant le droit à la vie privée que concernant la liberté d'expression ou encore la liberté de manifestation. Depuis une quinzaine d'années, sous l'impulsion de politiques gouvernementales, le nombre de ces caméras a augmenté dans des proportions démesurées, sans qu'aucun contrôle législatif ou politique ne vienne limiter cette expansion et ses conséquences sur les droits et libertés. Cependant, des études universitaires (voir notamment les travaux de Guillaume Gormand [2] ou Florent Castagnino [3]) ont démontré l'absence d'effet de ces procédés de surveillance sur les objectifs de sécurité publique. Même la Cour des comptes conclut qu'« *aucune corrélation globale n'a été relevée entre l'existence de dispositifs de vidéoprotection et le niveau de la délinquance commise sur la voie publique, ou encore les taux d'élucidation* » (Rapport de la Cour des comptes sur les polices municipales, octobre 2020, p. 70 [4]).

8. La CNIL le constate elle-même [5] sur son site internet : « *Le nombre de caméras filmant la voie publique a fortement augmenté ces dernières années, notamment*

1. Camille Polloni, « *Les cinq chiffres (fous) de la vidéosurveillance* », Les Inrocks, 21 juin 2012, URL : https://www.lesinrocks.com/actu/les-cinq-chiffres-fous-de-la-videosurveillance-22359-21-06-2012/

2. Antoine Albertini, « *Une étude commandée par les gendarmes montre la relative inefficacité de la vidéosurveillance* », Le Monde, 22 décembre 2021, URL : https://www.lemonde.fr/societe/article/2021/12/22/une-etude-commandee-par-les-gendarmes-montre-la-relative-inefficacite-de-la-videosurveillance_6106952_3224.html

3. Emmanuel Vautier, « *Caméras de surveillance : "Faire croire que cela va résoudre la délinquance, c'est faux"* », Ouest France, 3 décembre 2021, URL : https://www.ouest-france.fr/pays-de-la-loire/nantes-44000/entretien-cameras-de-surveillance-faire-croire-que-cela-va-resoudre-la-delinquance-c-est-faux-afb5e890-52e0-11ec-bfae-9f51653fbe56

4. https://www.ccomptes.fr/system/files/2020-11/20201020-rapport-polices-municipales_0.pdf

5. CNIL, « La vidéosurveillance – vidéoprotection sur la voie publique », 3 décembre 2019, URL : https://www.cnil.fr/fr/la-videosurveillance-videoprotection-sur-la-voie-publique

sous l'impulsion des pouvoirs publics ». Si la CNIL vérifiait d'ailleurs elle-même les irrégularités et illégalités liés à ces systèmes dans ses rapports annuels, ces contrôles sont aujourd'hui de moins en moins nombreux.

9. Par la présente plainte, La Quadrature du Net et les 15 248 plaignants l'ayant mandatée pour agir en leur nom entendent contester la pratique du ministre de l'intérieur qui vise à imposer progressivement l'installation illégale dans les rues de France des dispositifs de vidéosurveillance. Pour ce faire, la présente plainte demande à la CNIL de sanctionner le ministre de l'intérieur en tant que co-responsable des dispositifs de vidéosurveillance, par voie de conséquence de contrôler la légalité des autorisations préfectorales ayant permis la mise en œuvre de caméras de vidéosurveillance et de tirer, enfin, des conséquences et des constats sur les dangers de ce système.

10. Les 15 248 plaignants ayant mandaté La Quadrature du Net pour déposer la présente plainte ont été filmées par des caméras sur la voie publique, ce qui implique que leurs données personnelles ont été traitées par ces dispositifs et sont donc des personnes concernées par ces traitements.

11. Il sera démontré dans un premier temps que le ministre de l'intérieur est co-responsable de l'ensemble des traitements de données engendrés par la vidéosurveillance mise en place par les autorités publiques (I) puis que la pratique du ministre d'imposer ces mêmes traitements est illégale (II).

I. Sur la détermination des responsables de traitement

12. Les autorisations préfectorales permettant l'installation des caméras de surveillance sont des actes fondant des traitements de données (A) dont le ministre de l'intérieur est co-responsable de traitement (B).

A. En ce qui concerne l'identification des traitements de données en cause

13. **En droit**, l'article L. 251-1 du code de la sécurité intérieure soumet les enregistrements visuels de vidéosurveillance sur la voie publique au titre V du livre II du code de la sécurité intérieure, à l'exclusion de ceux qui sont utilisés dans des traitements automatisés ou contenus dans des fichiers structurés selon des critères permettant d'identifier, directement ou indirectement, des personnes physiques.

14. L'article L. 251-2 du code de la sécurité intérieure prévoit notamment une liste exhaustive de onze finalités en vertu desquelles la transmission et l'enregistrement d'images prises sur la voie publique peuvent être mis en œuvre par les pouvoirs publics, après autorisation préfectorale.

15. En complément des dispositions du code de sécurité intérieure, ces traitements de données doivent respecter les exigences de protection des données issues de la loi Informatique et Libertés, notamment en ce qu'elle transpose 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 »), et celles issues du RGPD.

16. En effet, une image enregistrée par une caméra de vidéosurveillance « *constitue une donnée à caractère personnel au sens de la* [directive 95/46] *dans la mesure où elle permet d'identifier la personne concernée* » (CJUE, 11 décembre 2014, *Ryneš*, aff. C-212/13, pt. 22). Cette analyse est, bien entendu, applicable *mutatis mutandis* à la directive « police-justice », ainsi que l'a confirmé le Conseil d'État (*cf.* CE, 22 décembre 2020, *La Quadrature du Net*, n° 446155, Rec. T.).

17. Ainsi, en application de l'article L. 253-2 du code de la sécurité intérieure, la CNIL peut, de sa propre initiative, « *exercer un contrôle visant à s'assurer que le système est utilisé conformément à son autorisation et, selon le régime juridique dont le système relève, aux dispositions du présent titre ou à celles de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.* » Dans son

rapport annuel de l'année 2011 [6], la Commission avait d'ailleurs fait état de cette nouvelle compétence instituée par la loi n° 2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI) du 14 mars 2011, qui lui avait permis de constater de nombreuses illégalités dans les systèmes installés [7].

18. La compétence de la CNIL pour relever des illégalité manifestes dans les actes autorisant la mise en œuvre de système de vidéosurveillance est donc acquise.

19. **En l'espèce**, comme la CNIL le détaille sur son site Internet [8], l'ensemble des actes préfectoraux autorisant l'installation de caméras en France ont été pris pour l'application d'une des finalités prévues par le code de la sécurité intérieure, qui répondent aux dispositions du loi Informatique et Libertés, en particulier car entrant dans le champ d'application du RGPD ou de la directive « police-justice » transposée au titre III de la loi Informatique et Libertés.

20. **Il en résulte que** les autorisations préfectorales prises en application de l'article L. 252-1 du code de la sécurité intérieure autorisent la captation, la transmission et l'enregistrement d'images sur la voie publiques par des moyens de caméras de vidéosurveillance, constituant ainsi des autorisations de mises en œuvre de traitement de données personnelles soumis au code de la sécurité intérieure et conjointement – et en fonction des finalités – au RGPD ou à la directive « police-justice » telle que transposée au titre III de la loi Informatique et Libertés.

21. Ces actes constituent les traitements attaqués par la présente réclamation.

6. CNIL, *Rapport d'activité 2011*, URL : `www.cnil.fr/sites/default/files/typo/document/RA2011_CNIL_FR.pdf`

7. Par exemple, le rapport fait état à la page 14 de 30 % des contrôles révélant une absence d'autorisation préfectorale, ou 40 % d'une mauvaise information. Dans son rapport d'activité pour 2012, sur 173 contrôle, 14 ont donné lieu à une mise en demeure, sanction ou avertissement (*cf.* CNIL, *Rapport d'activité 2012*, URL : `https://www.cnil.fr/sites/default/files/typo/document/CNIL_RA2012_web.pdf`).

8. CNIL, « Vidéoprotection : quelles sont les dispositions applicables ? », 13 décembre 2019, URL : `https://www.cnil.fr/fr/videoprotection-quelles-sont-les-dispositions-applicables`

B. En ce qui concerne la co-responsabilité de traitement

22. En droit, le 7° de l'article 4 du RGPD définit le responsable de traitement comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* ».

23. Pour la bonne application de cette définition, le Comité européen de la protection des données (ci-après le « CEPD ») a adopté ses *Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD* au sein desquelles il dégage plusieurs critères permettant de qualifier une responsabilité conjointe de traitement [9].

24. Au préalable, le CEPD rappelle comment identifier un responsable de traitement [10] :

> « *La détermination des finalités et des moyens revient à décider respectivement du "pourquoi" et du "comment" du traitement : pour une opération de traitement particulière, le responsable du traitement est l'acteur qui a déterminé la raison pour laquelle le traitement a lieu (c'est-à-dire "à quelles fins" ou "pourquoi") et comment cet objectif sera atteint (c'est-à-dire quels moyens doivent être mis en œuvre pour atteindre l'objectif). Une personne physique ou morale qui exerce cette influence sur le traitement de données à caractère personnel participe ainsi à la détermination des finalités et des moyens du traitement en question, conformément à la définition énoncée à l'article 4, paragraphe 7, du RGPD.* »

25. Le CEPD indique que peut être opérée une distinction entre « *moyens essentiels* » et « *moyens non essentiels* » afin d'aider à identifier qui détermine les moyens du traitement. Ainsi, le CEPD précise [11] :

9. CEPD, *Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD*, adoptées le 7 juillet 2021, URL : `https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_fr.pdf`

10. *Idem*., pt. 35.

11. *Idem*., pt. 40.

> « *On entend par "moyens essentiels" ceux qui sont étroitement liés à la finalité et à la portée du traitement, tels que le type de données à caractère personnel qui sont traitées ("quelles données sont traitées ?"), la durée du traitement ("pendant combien de temps sont-elles traitées ?"), les catégories de destinataires ("qui aura accès aux données ?") et les catégories de personnes concernées ("à qui appartiennent les données à caractère personnel traitées ?"). Outre la finalité du traitement, les moyens essentiels sont aussi étroitement liés à la question de savoir si le traitement est licite, nécessaire et proportionné.* »

26. Ainsi, **premièrement**, afin de qualifier une responsabilité conjointe pour une activité de traitement spécifique, le groupe des autorités de contrôle précise qu'une telle co-responsabilité existe « *lorsque différentes parties déterminent conjointement les finalités et les moyens de cette activité de traitement. Dès lors, pour apprécier l'existence de responsables conjoints du traitement, il convient d'examiner si la détermination des finalités et des moyens qui caractérisent un responsable du traitement est décidée par plus d'une partie. Le terme "conjointement" doit être interprété comme signifiant "ensemble" ou "pas seul", sous différentes formes et combinaisons* » [12].

27. **Deuxièmement**, pour apprécier la participation conjointe, il faut rechercher l'existence d'une décision commune ou de décisions convergentes, en ce sens qu'elles se complètent et sont nécessaires à la réalisation du traitement en ayant un effet concret sur la détermination des finalités et des moyens du traitement. Pour le CEPD, doit alors être examinée, **troisièmement**, la question de la nécessité de la participation de chaque acteur afin de déterminer lesquels sont responsables de traitement. Ainsi, « *un critère important pour identifier des décisions convergentes dans ce contexte est le fait que le traitement ne serait pas possible sans la participation des deux parties à la détermination des finalités et des moyens, en ce sens que le traitement par chacune des parties est indissociable de celui de l'autre, c'est-à-dire inextricablement lié.* » [13]

28. La Cour de justice de l'Union européenne a notamment précisé qu'en tout état de cause, la directive 95/46 (et, *mutatis mutandis*, le RGPD et la directive « police-justice ») « *n'exige pas, lorsqu'il y a une responsabilité conjointe de*

12. *Idem*., pt. 51.
13. *Idem*., pt. 55.

plusieurs opérateurs pour un même traitement, que chacun ait accès aux données à caractère personnel concernées » (*cf.* CJUE, gr. ch., *Madzhdi Shiri*, aff. C-201/16, 25 octobre 2017, pt. 38).

29. **Quatrièmement**, il peut être utile d'analyser si des moyens ont été déterminés conjointement afin de déterminer s'il existe, à travers cette étape, une influence d'une partie sur l'autre. Le CEPD affirme ainsi que« *différentes entités peuvent intervenir à des étapes différentes du traitement et à des degrés divers. Par conséquent, différents responsables conjoints du traitement peuvent définir les moyens de celui-ci dans une mesure variable, en fonction de celui qui est effectivement en mesure de le faire.* » [14] Le Comité précise également qu'il est possible que « *l'une des entités concernées fournisse les moyens du traitement et les mette à disposition pour les activités de traitement de données à caractère personnel effectuées par d'autres entités. L'entité qui décide d'utiliser ces moyens pour que des données à caractère personnel puissent être traitées pour une finalité particulière participe également à la détermination des moyens du traitement.* » [15]

30. **En l'espèce**, le ministre de l'intérieur participe activement à la mise en œuvre des traitements de données induits par les caméras de surveillance.

31. **D'une part**, la loi prévoit un contrôle du ministre de l'intérieur *via* le système d'autorisation préfectorale. En effet, aux termes de l'article L. 252-1 du code de la sécurité intérieure, « *L'installation d'un système de vidéoprotection dans le cadre du présent titre est subordonnée à une autorisation du représentant de l'État dans le département et, à Paris, du préfet de police donnée, sauf en matière de défense nationale, après avis de la commission départementale de vidéoprotection.* » L'article R. 252-1 du même code précise que « *Les attributions dévolues au représentant de l'Etat dans le département dans le cadre du présent titre sont exercées, à Paris, par le préfet de police et, dans le département des Bouches-du-Rhône, par le préfet de police des Bouches-du-Rhône.* »

32. Il convient de rappeler que le préfet est un représentant de l'État qui, aux termes de l'article 15 du décret n° 2004-374 du 29 avril 2004, « *prend les décisions dans les matières relevant des attributions des services déconcentrés des administrations civiles de l'État dans la région ou dans le département* ». Par cette repré-

14. *Idem*., pt. 63.
15. *Idem*., pt. 64.

sentation, le préfet agit et décide au nom de l'autorité de l'État.Pour Paris, le préfet de police est également, conformément à l'article R. 122-53 du code de la sécurité intérieure, le représentant de l'État et soumis hiérarchiquement au ministre de l'intérieur. Pour les Bouches-du-Rhône le préfet de police des Bouches-du-Rhône représente également l'État conformément à l'article 78-1 du décret n° 2004-374.

33. Ainsi, chaque autorisation préfectorale prise en application de l'article L. 251-1 du code de la sécurité intérieure est une décision prise par une autorité déconcentrée de l'État sur laquelle le ministre de l'intérieur a autorité.

34. En outre, les articles L. 252-2 et L. 252-3 précisent que, outre les finalités, l'autorisation préfectorale prescrit « *toutes les précautions utiles, en particulier quant à la qualité des personnes chargées de l'exploitation du système de vidéoprotection ou visionnant les images et aux mesures à prendre pour assurer le respect des dispositions de la loi* » ainsi que les destinataires, les modalités de transmission et d'accès des images et la durée de leur conservation.

35. Le représentant de l'État détermine donc les finalités des caméras mais également les modalités de leur utilisation, donc les moyens du traitement de données personnelles que le dispositif de vidéosurveillance constitue. Cette intervention du représentant de l'État est obligatoire et participe alors à la décision finale d'installation des dispositifs.

36. Autrement dit, pour chaque caméra autorisée, il existe une décision du ministre de l'intérieur, en tant que titulaire de l'autorité sur les représentants de l'État chargés de délivrer les autorisations préfectorales de vidéosurveillance. Le ministre de l'intérieur détermine donc les finalités et les modalités de ces traitements, qui s'ajoutent à la volonté des collectivités de mettre en place ces traitements de données une fois l'autorisation accordée. Ces deux acteurs, ministre de l'intérieur et collectivités, déterminent donc conjointement les modalités et la finalité du traitement, d'autant que l'autorisation préfectorale est une condition légale à l'installation des caméras de vidéosurveillance.

37. **D'autre part**, le ministre de l'intérieur participe activement, au travers de nombreuses politiques publiques, à l'installation et au renouvellement des caméras de vidéosurveillance.

38. En 2011, déjà, la Cour des comptes constatait que « *le ministère de l'intérieur a également chargé les préfets de département et les responsables des services territoriaux de la police et de la gendarmerie de promouvoir le développement de la vidéosurveillance. Depuis 2008, les instructions ministérielles aux préfets sur les objectifs annuels de la politique de sécurité intérieure leur ont systématiquement rappelé l'objectif de tripler le nombre de caméras installées sur la voie publique et demandé de mettre en œuvre un "plan départemental de développement de la vidéoprotection" dans les sites les plus sensibles.* » [16]

39. En effet, le ministre de l'intérieur incite à installer des caméras de vidéosurveillance en les finançant à travers le fonds interministériel de prévention de la délinquance (ci-après le « FIPD »). Créé en 2007, ce fond est « *destiné à financer la réalisation d'actions dans le cadre des plans de prévention de la délinquance et dans le cadre de la contractualisation mise en œuvre entre l'État et les collectivités territoriales en matière de politique de la ville* » [17]. Chaque année, une circulaire du ministère de l'intérieur fixe les orientations du gouvernement en matière de politiques publiques de prévention et indique quels sont les projets susceptibles de recevoir ces subventions. Depuis la création de ce fond en 2007, le FIPD incite les communes à installer des caméras de vidéosurveillance en subventionnant dans de grandes proportions leur mise en place.

40. Quinze ans plus tard, cette initiative est aujourd'hui bien ancrée dans les relations entre le gouvernement et les collectivités locales. Ainsi, la circulaire du 11 février 2022 relative aux orientations budgétaires des politiques de prévention de la délinquance et de la radicalisation pour 2022 énonce clairement et à plusieurs reprises que les subventions sont destinées à augmenter le parc de vidéosurveillance [18] :

« *Dans le prolongement des orientations déjà fixées l'an dernier, les*

16. Cour des Comptes, *L'organisation et la gestion des forces de sécurité publique*, juillet 2011, p. 128, URL : `https://www.ccomptes.fr/sites/default/files/EzPublish/Rapport_public_thematique-securite_publique.pdf`

17. Secrétariat général du Comité interministériel de prévention de la délinquance et de la radicalisation, « Le fonds interministériel de prévention de la délinquance (FIPD) et les subventions CERFA », URL : `www.cipdr.gouv.fr/le-cipdr/le-fipd/`

18. Circulaire du Ministère de l'intérieur n° INTK2204832J du 11 février 2022 relative aux orientations budgétaires des politiques de prévention de la délinquance et de la radicalisation pour 2022, page 1, URL : `https://www.cipdr.gouv.fr/wp-content/uploads/2022/02/INTK2204832J.pdf2022.pdf`

grandes priorités des politiques de prévention pour 2022 que vous vous demandons de déployer porteront sur : la poursuite du développement de la vidéo-protection de voie publique [...].

[...]

Tout d'abord, les crédits du FIPD s'inscrivent en hausse au terme de la loi de finances pour 2022, pour atteindre près de 80 millions d'euros, et soutenir en particulier le développement de la vidéo-protection dans le cadre des CSI et des décisions du comité interministériel aux ruralités. »

41. Plus précisément, le FIPD est divisé en plusieurs programmes parmi lesquels le programme S qui « *regroupe l'ensemble des subventions pour la vidéo-protection de voie publique et des lieux ouverts au public (hors des sites sensibles relevant du programme K), et la sécurisation des établissements scolaires* » (*cf.* page 7 de la circulaire précitée).

42. Il est prévu dans l'instruction complémentaire à la circulaire que les financements doivent être dépensés selon des règles fixées par le ministre de l'intérieur. Il est ainsi imposé aux collectivités les contraintes suivantes (*cf.* page 8 de la circulaire précitée) :

« *S'agissant de la vidéo protection de voie publique, vous veillerez à y consacrer au moins 75 % des crédits du programme S.* [...]

« *les transferts d'images vers les services de police et les unités de gendarmerie, ainsi que l'équipement des forces de sécurité de l'Etat, sous la forme des terminaux nécessaires à leur exploitation, dont le portage sera assuré principalement par les collectivités territoriales : le taux de subvention peut atteindre 100 %.* »

43. Surtout, il est indiqué qu'il « *conviendra de refuser le financement lorsqu'il s'agit d'assurer un simple renouvellement à l'identique de l'équipement* [...] », signifiant que les subventions ne sont accordées que si la collectivité installe de nouveaux équipements, créant une incitation directe et claire à l'expansion de la

vidéosurveillance. La marge de manœuvre et la discrétion des collectivités bénéficiant de ces financement sont donc fortement limitées, le ministre de l'intérieur ayant une influence factuelle forte sur les moyens et la finalités de ces dispositifs. Sa participation *via* les subventions occupe donc une grande place dans la décision finale de mise en œuvre du traitement de données.

44. Les chiffres et les faits le démontrent : le FIPD contribue directement au choix des communes à mettre en place de la vidéosurveillance. L'étude du laboratoire d'innovation numérique de la CNIL (ci-après le « LINC ») sur le développement de la vidéosurveillance dans les villes et les villages [19] confirme l'existence d'une volonté étatique de promotion de la vidéosurveillance qui sont désormais illustrés par des résultats : le LINC indique notamment que le FIPD « *porta ses fruits puisqu'en février 2014, selon les chiffres du ministère de l'intérieur, 2820 communes et 173 établissements publics de coopération intercommunale (EPCI) avaient été accompagnés pour installer 26 614 caméras, pour un montant total de 148,52 millions d'euros de subventions.* »

45. D'autres aides financières, pilotées par le ministère de l'intérieur lorsqu'elles sont appliquées à des projets de sécurité, encouragent également l'installation des caméras de vidéosurveillance dans les communes :

— **La dotation d'équipement des territoires (DETR)**. En 2021, ces subventions ont bénéficié à 449 projets de mise en place d'un système de vidéosurveillance [20]. Un commandant de gendarmerie indique ainsi à la Banque des territoires que « *l'objectif est de faire en sorte que le coût financier ne soit pas un sujet pour les communes* », précisant que « *l'État a d'abord apporté 400.000 euros en 2014, lors de la création de la salle de déport, via le Fonds interministériel de prévention de la délinquance (FIPD), puis à nouveau 100.000 euros en 2018 pour favoriser l'extension et la modernisation du réseau.* » Il indique que les caméras sont subventionnées dans la préfecture de Loir-et-Cher « *à hauteur de 80 % dans le cadre de la DETR* [21] ».

19. Antoine Courmont et Jeanne Saliou, « Etat, régions, départements : des incitations financières multiples à la vidéosurveillance », LINC, 19 novembre 2021, URL : `https://linc.cnil.fr/fr/etat-regions-departements-des-incitations-financieres-multiples-la-videosurveillance`

20. Compte-rendu d'exécution 2021 du DETR, p. 8, URL : `https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2022-07/detr-2021-synthese-globale-2.pdf`

21. « *Petites Villes de demain : le cercle "Sécurité du quotidien" sur le terrain* », Banque des Territoires, 28 février

— **La dotation politique de la ville (DPV)**. En 2021, plus d'1,3 millions d'euros ont permis de renforcer le système de vidéo-surveillance de 10 communes (Mulhouse, Creil, Bruay-la-Bussière, ...) [22].

— **La dotation de soutien à l'investissement local**. En 2021, 21 projets liés à l'installation ou au renforcement de la vidéosurveillance ont été financées par cette aide [23]

46. La participation du ministre de l'intérieur dans la décision d'installer des caméras de surveillance et dans l'usage qui en sera fait est donc très importante. Non seulement de nombreux financements sont fléchés uniquement pour la vidéo-surveillance, comprenant également de l'analyse algorithmique des images captées, mais il en existe également de nombreuses et diverses sources de subventions en fonction des différentes échelles et contextes des territoires, témoignant d'une véritable volonté active de faire construire ces équipements partout en France. Les chiffres cités sont parlants : sans ces politiques financières, le nombre de caméras en France serait bien moindre, et les communes ne prendraient pas la décision d'installer ou développer leur parc de caméras ni de s'équiper de dispositifs de vidéosurveillance algorithmique.

47. Non seulement le ministre de l'intérieur participe directement à la détermination des moyens et des finalités par les circulaires et instructions de subventions, mais il exerce aussi dans les faits une influence directe sur la volonté des communes de choisir de mettre en place des dispositifs de vidéosurveillance dans le cadre de leur politique locale de sécurité. Par ces financements et ces instructions, la participation du ministre est nécessaire pour le traitement décidé ensuite par la collectivité locale, les deux étant indissociables et inextricablement liées.

48. **Il en résulte que** le ministre de l'intérieur doit donc être considéré comme co-responsable de traitement de l'ensemble des dispositifs de vidéosurveillance autorisés conformément au titre V du livre II du code de sécurité intérieure.

2022, URL : https://www.banquedesterritoires.fr/petites-villes-demain-le-cercle-securite-du-quotidien-sur-le-terrain

22. Compte rendu d'exécution 2021 de la DPV, p. 10, URL : https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2022-07/dpv-2021-synthese-globale.pdf

23. Compte-rendu d'exécution 2021 de la DSIL, p. 11, URL : https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2022-07/dsil-2021-synthese-globale.pdf

49. Enfin, les documents produits en annexe (*cf.* pièce n° 2) illustrent différentes situations, à titre d'exemples, où des communes ont bénéficié de ces subventions démontrant l'existence de cette co-responsabilité des traitements dont La Quadrature du Net et les plaignants représentés contestent la légalité.

II. Sur l'illégalité de la pratique du ministre de l'intérieur autorisant les dispositifs de vidéosurveillance

A. En ce qui concerne la disproportion de la pratique du ministre de l'intérieur d'autoriser des dispositifs de vidéosurveillance

50. **En premier lieu**, la pratique récurrente et volontariste du ministre consistant à imposer des dispositifs de vidéosurveillance est contraire à la loi Informatique et Libertés, au RGPD, à la directive « police-justice » et à la Convention européenne des droits de l'homme et des libertés fondamentales (ci-après « CESDH ») en ce qu'elle ne justifie jamais la proportionnalité des traitements ainsi autorisés.

51. **En droit**, il est de jurisprudence constante qu'un dispositif de vidéosurveillance constitue une atteinte à la liberté d'aller et venir, au droit à la vie privée (*cf.* Cons. const., 18 janvier 1995, *Loi d'orientation et de programmation relative à la sécurité*, n° 94-352 DC, cons. 3) et au droit à la protection des données personnelles (*cf.*CJUE, 14 février 2019, *Buivids*, aff. C-345/17, pt. 31 ; CJUE, 11 décembre 2014, *Ryneš*, préc., pt. 22).

52. Les opérations de vidéosurveillance ne peuvent être constitutionnellement autorisées que « *dans des lieux et établissements ouverts au public particulièrement exposés à des dangers d'agression ou de vol afin d'y assurer la sécurité des personnes et des biens* » et « *la mise en œuvre de tels systèmes de surveillance doit être assortie de garanties de nature à sauvegarder l'exercice* » des libertés publiques constitutionnellement garanties (*cf.* Cons. const., 18 janvier 1995, préc., cons. 4).

53. Le code de la sécurité intérieure aménage ces garanties en prévoyant les finalités et modalités de mise en œuvre des caméras de vidéosurveillance. Ainsi, son article L. 251-2 du code dispose que « *la transmission et l'enregistrement d'images*

prises sur la voie publique par le moyen de la vidéoprotection peuvent être mis en œuvre par les autorités publiques compétentes » aux fins d'assurer différents objectifs de prévention de l'ordre public limitativement énumérés. L'article L. 252-1 du même code précise que « *l'installation d'un système de vidéoprotection dans le cadre du présent titre est subordonnée à une autorisation du représentant de l'État dans le département et, à Paris, du préfet de police donnée, sauf en matière de défense nationale, après avis de la commission départementale de vidéoprotection.* »

54. Ces garanties doivent être interprétées à la lumière des grands principes de protection de la vie privée et du droit des données personnelles, et principalement le principe de nécessité et proportionnalité.

55. Ainsi, aux termes de l'article 4 de la directive « police-justice » : « *Les États membres prévoient que les données à caractère personnel sont : a) traitées de manière licite et loyale ; b) collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités ; c) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ;* […] » Le 1° de l'article 8 de cette même directive « police-justice » précise que « *Les États membres prévoient que le traitement n'est licite que si et dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1er, paragraphe 1, et où il est fondé sur le droit de l'Union ou le droit d'un État membre.* » Ces dispositions de la directive « police-justice » ont été transposées aux articles 4 et 5 de la loi Informatique et Libertés.

56. Le 1° de l'article 5 du RGPD prévoit en substance les mêmes exigences de licéité, nécessité et proportionnalité du traitement.

57. De même, l'article 8 de la CESDH dispose à son § 1 que « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* » et à son § 2 qu'« *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à a sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.* »

58. La Cour européenne des droits de l'homme (ci-après « CEDH ») estime qu'une mesure de surveillance « *est considérée comme "nécessaire dans une société démocratique" pour atteindre un but légitime si elle répond à un "besoin social impérieux" et, en particulier, si elle est proportionnée au but légitime poursuivi et si les motifs invoqués par les autorités nationales pour la justifier apparaissent "pertinents et suffisants"* » (*cf.* CEDH, gr. ch., 4 décembre 2008, *S et Marper c. Royaume-Uni*, n^{os} 30562/04 et 30566/04, § 101).

59. Ces exigences s'appliquent à la mise en œuvre de caméras de vidéosurveillance, ces dispositifs devant être nécessaires pour atteindre l'objectif poursuivi. En 2011, la Cour des comptes rappelait que le préfet qui délivre l'autorisation « *doit notamment contrôler que les projets présentés correspondent aux buts définis par la loi* » et que « *la décision d'autoriser l'implantation d'un tel dispositif doit résulter d'une appréciation de la proportionnalité entre la réduction de l'insécurité et l'augmentation du risque d'atteinte à la vie privée résultant de chaque dispositif* »[24].

60. La Cour administrative d'appel de Nantes a directement appliqué ces principes en exigeant que des autorisations préfectorales de vidéosurveillance soient nécessaires et proportionnées à la préservation de l'ordre public (*cf.* CAA Nantes, 9 novembre 2018, *Commune de Ploërmel*, n^{o} 17NT02743, pt. 5).

61. La Cour a ainsi jugé que devait être regardé comme disproportionné un dispositif autorisé par un arrêté préfectoral pour les finalités de « prévention des atteintes aux biens - sécurité des personnes, - secours à personnes, - protection des bâtiments publics, - régulation du trafic routier, prévention d'actes terroristes, - prévention du trafic de stupéfiants » mais qui n'explique pas en quoi les lieux où les caméras sont implantées seraient « *particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants* » (*cf.* CAA Nantes, 9 novembre 2018, préc. pt. 6). Dès lors, pour justifier de tout projet de mise en œuvre de vidéosurveillance, il est nécessaire de démontrer le lien, appuyé de preuves telles que des statistiques relatives à la délinquance dans la commune, entre l'installation des caméras dans la zone concernée avec la poursuite des finalités prévues par le code de la sécurité intérieure, afin de justifier que ces équipements soient nécessaires à atteindre l'objectif poursuivi.

24. Cour des Comptes, *L'organisation et la gestion des forces de sécurité publique*, juillet 2011, p. 129, préc.

62. Tel a également été le raisonnement de la Cour administrative d'appel de Douai, cette fois-ci concernant l'information des conseillers municipaux pour prendre la décision de mise en place d'un système de vidéosurveillance. La Cour a estimé que ceux-ci ne pouvaient mesurer l'implication de leurs décisions dès lors que la note explicative qui leur étaient adressée se bornait à « *mentionner le nombre de caméras projeté et le coût prévisionnel de l'installation du dispositif* » (*cf.* Cour administrative d'appel de Douai, 24 novembre 2020, *Commune de Nieppe*, n° 19DA01349, pt. 9) :

> « [La note adressée aux conseillers municipaux] *ne précise en revanche ni la localisation des caméras, ni les espaces publics filmés, ne comporte aucune analyse relative à la situation de la commune de Nieppe en matière de sécurité publique et aux motifs, limitativement énumérés par les dispositions de l'article L. 251-2 du code de la sécurité intérieure précitées, pouvant fonder le recours à un tel dispositif, et ne fait état d'aucun élément relatif à la conciliation entre les exigences de sécurité et la préservation des libertés publiques, ni concernant les enjeux budgétaires et financiers de l'installation du dispositif en cause. Les membres du conseil municipal n'ont, ainsi, pas été mis en mesure d'appréhender le contexte ni de comprendre les motifs de fait et de droit des mesures envisagées et de mesurer les implications de leurs décisions.* »

63. Ainsi, l'application de l'article L. 251-2 du code de la sécurité intérieure nécessite non seulement que l'autorisation préfectorale détermine les finalités pour lesquelles les caméras vont être installées, mais également justifie et démontre en quoi ce traitement sera nécessaire pour atteindre l'objectif poursuivi, en application du principe de proportionnalité et de nécessité constitutionnellement et conventionnellement garanti.

64. Or, **en l'espèce**, les autorisations préfectorales ne font *jamais* état du lien entre les caméras devant être installées et la finalité pour laquelle le système est autorisée.

65. À titre d'exemple, il est fait état en annexe de nombreuses autorisations préfectorales qui se bornent à mentionner la ou les finalités du code de la sécurité

intérieure pour lesquelles les dispositifs de vidéosurveillance sont censés être mis en œuvre, sans aucun démonstration de la pertinence de l'utilité de ces moyens pour parvenir à ces objectifs(*cf.* pièce n° 2). Dans ces cas cités en exemple, qui ne sont qu'une illustration de la pratique générale des autorisations préfectorales en France aujourd'hui, la nécessité et la proportionnalité des caméras autorisées et donc des traitements de données en questions, ne sont jamais justifiées, en violation des dispositions du code de la sécurité intérieure.

66. **Il en résulte que** les dispositifs de vidéosurveillance autorisés par le ministre de l'intérieur ne sont ni nécessaires, ni adéquats, ni proportionnés aux finalités poursuivies.

B. En ce qui concerne l'illégalité de la pratique du ministre de l'intérieur d'autoriser de la vidéosurveillance algorithmique

67. **En deuxième lieu**, la pratique du ministre de l'intérieur d'autoriser des dispositifs de vidéosurveillance couplés à des solutions d'analyse algorithmique des images est contraire au RGPD, à la directive « police-justice », à la loi Informatique et Libertés et à la CESDH en ce qu'elle n'est pas prévue par la loi ni proportionnée.

68. **En droit**, aux termes de l'article 8 de la CESDH, toute ingérence dans le droit à la vie privée doit être « *prévue par la loi* ».

69. La CEDH a ainsi considéré que l'ingérence devait avoir « *une base en droit interne* », être par ailleurs « *suffisamment accessible* », le citoyen devant « *pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné* » et enfin que ne pouvait être considéré comme une loi au sens de la CESDH « *qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite ; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé* » (*cf.* CEDH, 25 mars 1983, *Silver et autres c. Royaume-Uni*, n° 5947/72, §§ 85–88).

70. De la même façon, il a été jugé que :

« *Les mots* “prévue par la loi” *veulent d'abord que la mesure incriminée ait une base en droit interne, mais ils ont trait aussi à la qualité de la loi en cause : ils exigent l'accessibilité de celle-ci à la personne concernée, qui de surcroît doit pouvoir en prévoir les conséquences pour elle, et sa compatibilité avec la prééminence du droit* [...]. *Cette expression implique donc notamment que la législation interne doit user de termes assez clairs pour indiquer à tous de manière suffisante en quelles circonstances et sous quelles conditions elle habilite la puissance publique à recourir à des mesures affectant leurs droits protégés par la Convention* » (*cf.* CEDH, 12 juin 2014, *Fernandez Martinez c. Espagne*, n° 56030/07, § 117)

71. Il a ainsi suffi à la Cour européenne de constater que la mesure incriminée n'était pas prévue par la loi pour conclure à la violation de l'article 8 de la Convention (*cf.* CEDH, 8 avril 2003, *M. M. c. Pays-Bas*, n° 39339/98, §. 46 ; voir dans ce sens également : CEDH, *Guide sur l'article 8 de la Convention - Droit au respect de la vie privée et familiale*, §. 14).

72. Il en résulte que toute ingérence dans la vie privée des personnes doit être fondée sur un cadre juridique clair et précis, suffisamment accessible, permettant au citoyen de disposer de renseignements suffisants sur les normes juridiques applicables à un cas donné.

73. Cette exigence de la CESDH est reprise en substance par l'article 4 de la directive « police-justice » et 4 de la loi Informatique et Libertés. Aux termes du 1. de l'article 4 de la directive « police-justice », « *les États membres prévoient que les données à caractère personnel sont : a) traitées de manière licite et loyale ;* [...] ». La loi Informatique et Libertés reprend ce critère en exigeant à son article 4 que « *les données à caractère personnel doivent être : 1° Traitées de manière licite, loyale et, pour les traitements relevant du titre II, transparente au regard de la personne concernée ;* [...] ».

74. La définition de la licéité est donnée à l'article 8 de la directive « police-justice » :

« *1. Les États membres prévoient que le traitement n'est licite que si et*

dans la mesure où il est nécessaire à l'exécution d'une mission effectuée par une autorité compétente, pour les finalités énoncées à l'article 1er, paragraphe 1, ***et où il est fondé sur le droit de l'Union ou le droit d'un État membre****.*

2. Une disposition du droit d'un État membre qui réglemente le traitement relevant du champ d'application de la présente directive ***précise au moins les objectifs du traitement, les données à caractère personnel devant faire l'objet d'un traitement et les finalités du traitement****.* »

75. L'article 5 de la loi Informatique et Libertés reprend une définition similaire à celle de la directive « police-justice ».

76. **En droit**, toujours, en ce qui concerne le cas particulier des traitements de données sensibles, l'article 10 de la directive « police-justice » pose un principe d'interdiction et, par exception, « *uniquement en cas de nécessité absolue, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée* », les autorise seulement « *lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre* », « *pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique* » ou « *lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée* ».

77. Ce principe d'interdiction de traiter des données sensibles sans base légale spécifique a été transposée dans la loi Informatique et Libertés à l'article 88 qui, tout en posant un même principe d'interdiction traiter des données sensibles, l'autorise par exception uniquement par « *une disposition législative ou réglementaire* », ou bien « *s'il vise à protéger les intérêts vitaux d'une personne physique, soit s'il porte sur des données manifestement rendues publiques par la personne concernée* ». Cette exception, à l'instar de tout exception, doit être interprétée strictement.

78. En matière de vidéosurveillance algorithmique, la CNIL a appliqué ce raisonnement pour constater que ces dispositifs ne peuvent avoir pour base légale les dispositions du code de la sécurité intérieure relatives à la vidéosurveillance [25] :

25. CNIL, *Caméras dites « intelligentes » ou « augmentées » dans les espaces publics – Position sur les conditions de déploiement*, 19 juillet 2022, p. 11, URL : `https://www.cnil.fr/sites/default/files/atoms/files/cameras-intelligentes-augmentees_position_cnil.pdf`

> « *À l'inverse, du fait de la nature distincte des traitements en cause, la CNIL considère que les caméras encadrées par le CSI ne sont pas de facto "autorisées" à utiliser des technologies de vidéo "augmentée" y compris pour les finalités ayant permis leur implantation : le législateur n'a entendu encadrer par le CSI que des dispositifs de vidéo "simples", qui ne captent pas le son et ne sont pas équipés de traitements algorithmiques d'analyse automatique.* »

79. **En droit**, enfin, toute ingérence dans le droit à la vie privée doit être proportionné à l'objectif poursuivi, la démonstration de cette proportionnalité reposant sur le responsable de traitement (*cf. supra*, §§ 50 et s.).

80. **En l'espèce**, le ministre de l'intérieur, à travers le FIPD, incite les collectivités locales à doter leurs dispositifs de vidéosurveillance de traitements algorithmiques des flux d'images. En effet, l'instruction complémentaire à la circulaire indique que (*cf.* p. 8 de la circulaire précitée) :

> « *Sera au contraire privilégiée l'amélioration de la technologie, conformément à la SNPD 2020-2024 qui incite à expérimenter le traitement automatisé de l'image, dans les limites légales rappelées (ex. recours possible au traitement permettant d'identifier une situation dangereuse : mouvement de foule inhabituel, cris soudains, intrusion dans un espace interdit, départ d'incendie, etc.).* »

81. Cette exigence est en effet une mise en œuvre concrète de la proposition 26 de la stratégie nationale de prévention de la délinquance (SNPD) 2020-2024 qui précise : « *En matière de vidéoprotection : expérimenter le traitement automatisé de l'image, dans le respect des libertés individuelles* »[26]. Cette action, dont il est précisé que l'État en est un des pilote et partenaire, consiste à tester la « *connexion avec des logiciels de détection de situations comportant un danger manifeste : mouvement de foule inhabituel, cris soudains, intrusion dans un espace interdit, départ d'incendie, etc.* »

82. Or, à ce jour, ces logiciels d'analyse algorithmique d'images constituent

26. Stratégie nationale de prévention de la délinquance, tome 2, page 39, URL : `https://www.cipdr.gouv.fr/wp-content/uploads/2020/03/Tome-2-SNDP-E%CC%81XE%CC%81-INTERACTIF.pdf`)

des traitements de données biométriques interdits et illégaux [27].

83. De même, la pratique du ministre de l'intérieur consistant à autoriser des dispositifs de vidéosurveillance algorithmique échoue à toute démonstration de la proportionnalité de telles autorisations (*cf. supra*, §§ 63 et s.).

84. **Il en résulte que** le ministre de l'intérieur incite les collectivités à acquérir des logiciels d'analyse algorithmique des images de vidéosurveillance sans base légale ni proportionnalité.

85. À tous égards, la sanction de la pratique du ministre de l'intérieur consistant à promouvoir et autoriser des dispositifs de vidéosurveillance en France s'impose.

27. Voir l'analyse en ce sens de La Quadrature du Net et sa position à la consultation officielle de la CNIL en lien dans l'article « *En quoi la vidéosurveillance algorithmique est-elle illégale ?* », URL : `https://www.laquadrature.net/2022/04/07/en-quoi-la-videosurveillance-algorithmique-est-elle-illegale/`

PAR CES MOTIFS, l'association La Quadrature du Net et les 15 248 plaignants l'ayant mandatée concluent qu'il plaise à la CNIL de :

SANCTIONNER le ministre de l'intérieur pour sa pratique consistant à autoriser des dispositifs de vidéosurveillance disproportionnés, et des dispositifs de vidéosurveillance algorithmique disproportionnés et dépourvus de base légale, en tant que co-reponsable de traitement ;

ENJOINDRE au ministre de l'intérieur de cesser, sans délai, cette pratique d'incitation au déploiement de dispositifs de vidéosurveillance ;

ENJOINDRE au ministre de l'intérieur d'exiger, *via* une circulaire ou tout autre moyen contraignant, aux représentants de l'État chargés de délivrer les autorisations de mise en œuvre de dispositifs de vidéosurveillance de contrôler *a posteriori* la proportionnalité des autorisations déjà délivrées ;

CONTRÔLER la proportionnalité des dispositifs listés à dans la pièce n° 2 et **ENJOINDRE** aux auteurs des autorisations de les retirer, en application de l'article R. 253-2 du code de la sécurité intérieure.

Fait à Marseille, le 24 septembre 2022

[redacted]

Membre du collège solidaire de La Quadrature du Net

[redacted]

BORDEREAU DES PRODUCTIONS

Pièce n° 1 : Liste des 15 248 plaignants ayant donné mandat à La Quadrature du Net pour déposer en leur nom la présente plainte ;

Pièce n° 2 : Illustrations de communes ayant bénéficié des subventions étatiques et exemples d'autorisations préfectorales illégales.