Délibération SAN-2021-003 du 12 janvier 2021

Commission Nationale de l'Informatique et des Libertés
Nature de la délibération : Sanction
Etat juridique : En vigueur
Date de publication sur Légifrance : Jeudi 14 janvier 2021

Délibération de la formation restreinte n°SAN-2021-003 du 12 janvier 2021 concernant le ministère de l'intérieur

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de Messieurs Alexandre LINDEN, président, Philippe-Pierre CABOURDIN, vice-président, et de Mesdames Anne DEBET et Christine MAUGÜE, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la directive (UE) 2016/680 du Parlement européen et du Conseil 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 ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 20 et suivants;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° 2020-076C du 7 mai 2020 de la présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification des traitements mis en œuvre par le ministère de l'intérieur ou pour son compte ;

Vu la décision de la présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 2 octobre 2020 ;

Vu le rapport de Madame Sophie LAMBREMON, commissaire rapporteure, notifié au ministère de l'intérieur le 30 octobre 2020 ;

Vu les observations écrites versées par le ministère de l'intérieur le 1er décembre 2020 ;

Vu les observations orales formulées lors de la séance de la formation restreinte, le 10 décembre 2020 ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte :

- Madame Sophie LAMBREMON, commissaire, entendu en son rapport ;

En qualité de représentants du ministère de l'intérieur :

- […] ;

- […] ;

Le ministère de l'Intérieur ayant eu la parole en dernier ;

La formation restreinte a adopté la décision suivante :

I. Faits et procédure

1. À la suite du confinement décidé par le Gouvernement au mois de mars 2020, plusieurs articles de presse ont fait état de l'utilisation, par les forces de police (notamment le commissariat de Cergy-Pontoise) et de gendarmerie (notamment le groupement de gendarmerie départementale de Haute-Garonne), de drones équipés d'une caméra afin de veiller au respect des mesures prises dans ce contexte. L'utilisation de tels drones lui paraissant susceptible de mettre en œuvre des traitements de données à caractère personnel, la présidente de la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission) a, par courrier du 23 avril 2020, demandé au ministère de l'intérieur des précisions quant aux traitements réalisés dans ce cadre.

2. En l'absence de réponse, la présidente de la Commission a, par la décision n° 2020-076C du 7 mai 2020, initié une procédure de contrôle à l'encontre du ministère. Cette procédure avait pour objet de vérifier le respect, par le ministère de l'intérieur, de l'ensemble des dispositions durèglement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après le Règlement ou le RGPD), dela loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après la loi du 6 janvier 1978 ou la loi Informatique et Libertés), de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 (ci-après la directive police-justice) et des dispositions prévues aux articles L251-1 et suivants du code de la sécurité intérieure. Dans le cadre de cette procédure, la présidente de la Commission a, le 8 mai 2020, fait parvenir au ministère de l'intérieur, à la préfecture de police de Paris, au commissariat de Cergy-Pontoise et au groupement de gendarmerie départementale de Haute-Garonne des questionnaires portant sur l'utilisation de drones afin de faire respecter les mesures de confinement déployées dans le cadre de l'état d'urgence sanitaire. Le ministère de l'intérieur a répondu à l'ensemble de ces questionnaires par courrier du 27 mai 2020.

3. Le 9 juillet 2020, une délégation de la CNIL s'est rendue dans les locaux de la préfecture de police de Paris afin de procéder à un contrôle sur place. Ce contrôle a notamment permis à la délégation de contrôle de faire procéder à un vol d'essai d'un drone utilisé par la préfecture de police de Paris.

4. Différents échanges sont intervenus par courriel entre le ministère et la délégation de contrôle entre les mois de juillet et de septembre 2020. Ces échanges concernaient la transmission de documents demandés à l'occasion du contrôle ainsi que de précisions demandées ultérieurement.

5. Aux fins d'instruction de ces éléments, la présidente de la Commission a, le 2 octobre 2020, désigné Madame Sophie LAMBREMON en qualité de rapporteure, sur le fondement de l'article 22 de la loi du 6 janvier 1978.

6. À l'issue de son instruction, la rapporteure a, le 30 octobre 2020, fait signifier au ministère de l'intérieur un rapport détaillant les manquements à la loi Informatique et Libertés qu'elle estimait constitués en l'espèce. La rapporteure proposait à la formation restreinte de la Commission de prononcer une injonction de mettre en conformité le traitement avec les dispositions de l'article 87 de la loi Informatique et Libertés, ainsi qu'un rappel à l'ordre. Elle proposait également que cette décision soit rendue publique et ne permette plus d'identifier nommément le ministère à l'expiration d'un délai de deux ans à compter de sa publication.

7. Le même jour, le ministère de l'intérieur a été informé que ce dossier était inscrit à l'ordre du jour de la séance de la formation restreinte du 10 décembre 2020.

8. Le 1er décembre 2020, le ministère a produit des observations.

9. Le ministère et la rapporteure ont présenté des observations orales lors de la séance de la formation restreinte.

II. Motifs de la décision

A. Sur l'existence d'un traitement de données à caractère personnel

10. La rapporteure observe que la préfecture de police de Paris, le commissariat de Cergy-Pontoise et le groupement de gendarmerie départementale de Haute-Garonne ont utilisé des drones afin de vérifier le respect des mesures de confinement. Par ailleurs, la préfecture de police de Paris a également utilisé ces dispositifs pour d'autres finalités, telles que des missions de police judiciaire (reconnaissance d'un lieu avant une interpellation, surveillance d'un trafic de stupéfiants), des opérations de maintien de l'ordre (surveillance de manifestations) ou de gestion de crise et des contrôles routiers (surveillance de rodéos urbains).

11. La rapporteure relève que les drones utilisés sont équipés d'une caméra permettant la captation d'images en haute résolution et possédant des capacités de zoom pouvant agrandir l'image entre six et vingt fois.

12. Au regard de ces capacités techniques, la rapporteure considère que l'utilisation de ces drones par le ministère de l'intérieur donne lieu à un traitement de données à caractère personnel dès lors que des personnes sont filmées dans des conditions permettant leur identification.

13. Le ministère de l'intérieur, quant à lui, a d'abord affirmé en réponse aux questionnaires envoyés par la présidente de la CNIL que le vol des drones ne donnait lieu à aucun traitement de données à caractère personnel, les personnes n'étant pas identifiables. Dans ses observations en réponse au rapport de sanction, il a ensuite considéré que l'incertitude juridique relative à la nature des données traitées démontrait la bonne foi de l'administration, qu'en tout état de cause, le système de floutage mis en œuvre excluait tout traitement de données à caractère personnel, tout en précisant que des considérations techniques empêchaient que ce système de floutage soit exécuté au niveau du drone captant les images et avant toute transmission de celles-ci.

14. La formation restreinte estime que la qualification de traitement de données à caractère personnel s'applique à un système de captation vidéo filmant des personnes pour les raisons suivantes.

15. **En premier lieu**, sur l'existence d'un traitement de données à caractère personnel, l'article 2 de la loi Informatique et Libertés dispose : *sauf dispositions contraires, dans le cadre de la présente loi s'appliquent les définitions de l'article 4 du règlement (UE) 2016/679 du 27 avril 2016* .

16. Aux termes de l'article 4 du RGPD, constitue un traitement de données à caractère personnel *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* . Ce même article définit une donnée à caractère personnel comme *toute information se rapportant à une personne physique identifiée ou identifiable […] ; est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence […] à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* .

17. Au regard de ces définitions, la formation restreinte relève que tout opération – notamment la captation, la transmission, la modification ou la consultation – portant sur l'image de personnes pouvant être reconnues constitue un traitement de données à caractère personnel.

18. La formation restreinte observe que cette analyse, adoptée de longue date par la CNIL, a été consacrée par la jurisprudence européenne dès 2014 : *l'image d'une personne enregistrée par une caméra constitue une donnée à caractère personnel au sens de la disposition visée au point précédent dans la mesure où elle permet d'identifier la personne concernée* (CJUE, 11 décembre 2014, Ryneš, affaire C-212/13, point 22). Elle a été rappelée très récemment par le Comité européen de la protection des données (ci-après le CEPD) dans ses lignes directrices 3/2019 du 29 janvier 2020 sur le traitement des données à caractère personnel par des dispositifs vidéo : *La surveillance systématique et automatisée d'un espace spécifique par des moyens optiques ou audiovisuels, principalement à des fins de protection des biens ou de protection de la vie et de la santé des personnes, est devenue un phénomène important de notre époque. Cette activité entraîne la collecte et la conservation d'informations picturales ou audiovisuelles sur toutes les personnes entrant dans l'espace surveillé qui sont identifiables sur la base de leur apparence ou d'autres éléments spécifiques. L'identité de ces personnes peut être établie sur la base de ces informations* .

19. S'agissant plus spécifiquement des drones équipés d'une caméra, le juge des référés du Conseil d'État a considéré que *le dispositif de surveillance litigieux […] qui consiste à collecter des données, grâce à la captation d'images par drone, à les transmettre, dans certains cas, au centre de commandement de la préfecture de police pour un visionnage en temps réel et à les utiliser pour la réalisation de missions de police administrative constitue un traitement* (Conseil d'État, ordonnance du 18 mai 2020, n^{os} 440442 et 440445). Constatant qu'aucun dispositif n'était mis en place pour empêcher, dans tous les cas, que les informations collectées puissent conduire à rendre les personnes identifiables, cette juridiction conclut que *les données susceptibles d'être collectées par le traitement litigieux doivent être regardées comme revêtant un caractère personnel* .

20. Enfin, dans un avis du 20 septembre 2020 relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques, le Conseil d'État a précisé que *eu égard notamment aux technologies actuellement disponibles et à leur évolution et aux moyens matériels dont disposent les autorités publiques, le Conseil d'État estime que les images de personnes captées au moyen de caméras aéroportées par ces autorités dans le cadre de missions de sécurité publique ou de sécurité civile doivent, en principe, être regardées comme des données personnelles et que, par suite, la collecte et l'utilisation de ces images sont soumises au respect des textes rappelés ci-dessus. Il pourrait toutefois en aller autrement en cas d'emploi dans des conditions particulières excluant l'existence de possibilités raisonnables d'identifier des personnes, ou dans l'hypothèse où seraient mis en œuvre des dispositifs techniques empêchant l'identification* (Conseil d'État, section de l'intérieur, séance du mardi 20 septembre 2020, n^{o} 401 214).

21. La formation restreinte rappelle qu'en l'espèce, la préfecture de police de Paris, le groupement de gendarmerie départementale de Haute-Garonne et le commissariat de Cergy-Pontoise ont reconnu avoir utilisé des drones équipés d'une caméra dans le cadre de vérifications du respect des mesures de confinement et, pour la préfecture de police de Paris, pour d'autres finalités, notamment judiciaires et de maintien de l'ordre. Ces drones ont volé à une altitude comprise, selon les acteurs, entre 30 et 120 mètres et étaient équipés d'un objectif de 12 millions de pixels pouvant agrandir l'image entre six et vingt fois.

22. La délégation de contrôle, ayant fait réaliser un vol d'essai de drone le 9 juillet 2020, a constaté que les caractéristiques techniques évoquées ci-dessus permettent l'identification des personnes.

23. **En second lieu**, s'agissant d'un éventuel dispositif de floutage qui pourrait permettre de rendre les personnes concernées non identifiables, la formation restreinte note, tout d'abord, que la préfecture de police de Paris, le groupement de gendarmerie départementale de Haute-Garonne et le commissariat de Cergy-Pontoise ont indiqué, dans leur réponse aux questionnaires envoyés, qu'aucun dispositif de floutage n'avait été mis en place.

24. Elle observe ensuite que la préfecture de police de Paris a ultérieurement indiqué, lors du contrôle réalisé le 9 juillet 2020, qu'un dispositif de floutage était en cours de développement. Le ministère de l'intérieur a précisé, durant la séance du 10 décembre 2020, que son déploiement était effectif depuis la fin du mois d'août 2020.

25. En conséquence, la formation restreinte relève, d'une part, qu'un tel dispositif n'était pas mis en œuvre lors des vols évoqués dans les questionnaires envoyés aux services opérationnels, et que des drones équipés d'une caméra ont donc procédé à de nombreux vols sans floutage des images collectées avant le déploiement du mécanisme. Elle considère, d'autre part, que le dispositif décrit durant la présente procédure ne saurait, pour autant, soustraire les images collectées à la règlementation applicable en matière de la protection des données à caractère personnel.

26. En effet, premièrement, le système de floutage évoqué ne s'applique pas aux images captées par la caméra présente sur le drone et transmises au pilote du drone. Si la visualisation d'images non floutées par le pilote du drone s'explique aisément par des impératifs de sécurité (contrôle de l'appareil pendant le temps de vol), ce que la formation restreinte ne remet pas en question, il reste que la captation d'images non floutées par la caméra et leur transmission au pilote constituent des opérations de traitement de données à caractère personnel.

27. Deuxièmement, il résulte des réponses apportées par la préfecture de police qu'elle a procédé à l'enregistrement d'images non floutées lors de l'utilisation de drones pour les besoins de missions de police judiciaire, ce qui constitue également un traitement de données à caractère personnel.

28. Enfin, et contrairement aux déclarations faites par le ministère de l'intérieur durant la séance, il ressort des pièces communiquées en défense, et plus particulièrement de la note relative au floutage intitulée Traitement de flux vidéo provenant des drones , datée du 23 novembre 2020, que les flux floutés peuvent être consultés en clair par les agents de la préfecture de police : *Le dispositif de floutage étant maîtrisé par la DILT* (direction de l'innovation, de la logistique et des technologies)*, il est impossible à la DOPC* (direction de l'ordre public et de la circulation) *d'accéder aux flux non floutés.L'accès aux flux non floutés nécessiterait une modification de la configuration actuellement en œuvre ; seul un ingénieur ayant les droits sur l'ensemble du dispositif peut faire ce travail laborieux. Les ingénieurs ayant ces droits sont placés sous un commandement différent de celui du DOPC.* La formation restreinte déduit de ce document que, bien que laborieux , l'accès à des flux non floutés demeure possible par des personnes placées sous la responsabilité du responsable de traitement. Dès lors, le traitement doit être qualifié de traitement de données à caractère personnel.

B. Sur l'identification du responsable de traitement

29. La formation restreinte souligne que l'ensemble des traitements visés par la présente procédure, ayant pour finalités de s'assurer du respect des mesures de confinement adoptées dans le cadre de l'état d'urgence sanitaire, d'intervenir au profit de missions de police judiciaire, de missions de maintien de l'ordre, ou dans le cadre de la gestion de crise ou de contrôle routier, relèvent de la compétence du ministère de l'intérieur, conformément aux dispositions du décret n° 2017-1070 du 24 mai 2017 relatif aux attributions du ministre de l'intérieur, lequel dispose *le ministre de l'intérieur prépare et met en œuvre la politique du Gouvernement en matière de sécurité intérieure, de libertés publiques, d'administration territoriale de l'État, d'immigration, d'asile et de sécurité routière* .

30. Elle souligne également que les services concernés (groupement de gendarmerie départementale de Haute-Garonne, commissariat de Cergy-Pontoise et préfecture de police de Paris) agissent tous sous la tutelle du ministère de l'intérieur.

31. Le ministère de l'intérieur se considère bien comme le responsable de traitement, ses services centraux ayant d'ailleurs rédigé une instruction de commandement prévoyant le recours aux drones notamment dans le cadre du confinement.

32. Dès lors, la formation restreinte, retient que ce dernier doit être considéré le responsable des traitements concernés par la présente procédure.

C. Sur la loi applicable

33. Le premier paragraphe de l'article 87 de la loi Informatique et Libertés, premier article du titre III de la loi, dispose : *le présent titre s'applique, sans préjudice du titre I^er^, aux traitements de données à caractère personnel mis en œuvre, 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, par toute autorité publique compétente ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique, ci-après dénommés autorité compétente* .

34. Ce titre III s'applique donc aux traitements qui répondent à une double caractéristique relative à leur finalité, d'une part, et à la qualité du responsable de traitement, d'autre part.

35. S'agissant des finalités poursuivies par les traitements nés des vols de drones équipés d'une caméra, il ressort des déclarations effectuées par le groupement de gendarmerie départementale de Haute-Garonne, par le commissariat de Cergy-Pontoise et par la préfecture de police de Paris que les images ont été utilisées, par ces trois acteurs, afin de s'assurer du respect des mesures de confinement adoptées dans le cadre de l'état d'urgence sanitaire et, pour le dernier d'entre eux uniquement, pour d'autres finalités, telles que des missions de police judiciaire, de maintien de l'ordre, de gestion de crise et de contrôle routier.

36. La formation restreinte considère que les missions précitées entrent dans le champ des finalités visées par l'article 87 de la loi Informatique et Libertés, soit parce qu'elles visent à prévenir ou détecter des infractions pénales – par exemple, lorsque les drones sont utilisés afin de veiller au respect des mesures de confinement ou de contrôle routier –, à enquêter ou poursuivre en matière pénale – par exemple pour les missions de police judiciaire – à la protection contre les menaces pour la sécurité publique et la prévention de telles menaces – par exemple pour les missions de maintien de l'ordre ou de gestion de crise.

37. La formation restreinte considère également que, dans le cadre de ces missions, le ministère de l'intérieur doit être regardé comme l'autorité compétente, au regard de l'article 1^er^ du décret n° 2020-874 du 15 juillet 2020 relatif aux attributions du ministre de l'intérieur (précédemment décret n° 2017-1070 du 24 mai 2017), précité.

38. En conséquence, la formation restreinte considère qu'en l'espèce, les traitements mis en œuvre par le ministère de l'intérieur pour les différentes finalités ci-dessus évoquées doivent respecter les dispositions du titre III de la loi Informatique et Libertés.

D. Sur les manquements

1. Sur le manquement relatif à la licéité du traitement et à l'absence d'étude d'impact

39. Le second paragraphe de l'article 87 de la loi Informatique et Libertés prévoit que les traitements visés par le titre II de la loi *ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée, pour l'une des finalités énoncées au premier alinéa, par une autorité compétente au sens du même premier alinéa et où sont respectées les dispositions des articles 89 et 90* .

40. Aux termes du I de l'article 89 de la loi, *si le traitement est mis en œuvre pour le compte de l'État pour au moins l'une des finalités énoncées au premier alinéa de l'article 87, il est prévu par une disposition législative ou réglementaire prise dans les conditions prévues au I de l'article 31 et aux articles 33 à 36* . En application du II du même article, si le traitement porte sur des données visées par l'article 6 de la loi (dites données sensibles), il doit être prévu par une disposition législative ou réglementaire prise dans les conditions prévues au II de l'article 31. L'article 31 de la loi auquel il est fait référence impose que les traitements de données en cause soient autorisés par arrêté du ministre ou des ministres compétents, pris après avis motivé et publié de la Commission et, en cas de traitement de données sensibles, par un décret en Conseil d'État pris après avis motivé et publié de la CNIL.

41. L'article 90 de la loi dispose : *si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 6, le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel* .

42. À titre liminaire, la formation restreinte relève que le ministère de l'intérieur ne conteste pas la caractérisation de ce manquement, ayant considéré à tort que les traitements en cause ne portaient pas sur des données à caractère personnel.

43. Au regard des dispositions de l'article 89, la formation restreinte relève qu'aucun cadre législatif ou réglementaire ne vient autoriser et encadrer les traitements de données à caractère personnel nés de l'utilisation par le ministère de l'intérieur de drones équipés d'une caméra. En indiquant que des travaux sont engagés pour élaborer un cadre légal dans les plus brefs délais, le ministère de l'intérieur confirme ce point.

44. S'agissant des dispositions de l'article 90, la formation restreinte considère que les traitements mis en œuvre en l'espèce sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Ce risque élevé naît, d'une part, des caractéristiques des drones, qui sont des objets volants embarquant une caméra capable de filmer dans des résolutions importantes, en tout lieu et à tout moment. Ils sont donc capables de filmer toute personne circulant dans l'espace public, de la suivre et de traiter des données personnelles intangibles telles que les traits de son visage. Le risque naît, d'autre part, de l'utilisation faite des drones par le ministère de l'intérieur, notamment lors de manifestations, occasions au cours desquelles les opinions politiques, les convictions religieuses ou philosophiques des personnes, ou leur appartenance syndicale, sont susceptibles d'être révélées. Enfin, le risque est aggravé par le fait que les traitements sont potentiellement mis en œuvre à l'insu des personnes, celles-ci n'étant souvent pas conscientes de la présence de drones, de l'activation de la caméra et de la captation de leur image. Ce risque est à cet égard aggravé, en l'espèce, par l'absence d'information des personnes à l'occasion des vols réalisés.

45. La formation restreinte note que l'article 90 de la loi Informatique et Libertés précise que ce risque peut aussi naître *en raison de l'utilisation de nouveaux mécanismes* , ce qui est bien le cas en l'espèce.

46. En conséquence, la formation restreinte considère que l'utilisation de drones équipés d'une caméra fait naître un risque élevé pour les droits et les libertés des personnes physiques et que, dès lors, il revenait au ministère de l'intérieur de réaliser une analyse d'impact relative à la protection des données à caractère personnel.

47. La formation restreinte relève qu'aucune analyse d'impact n'a été réalisée.

48. Il ressort de l'ensemble de ces éléments que les conditions de licéité des traitements mis en œuvre ne sont pas remplies. La formation restreinte considère donc que des manquements aux articles 89 et 90 de la loi Informatique et Libertés sont constitués.

2. Sur le manquement relatif à l'information des personnes

Aux termes de l'article 104 de la loi Informatique et Libertés, *Le responsable de traitement met à la disposition de la personne concernée les informations suivantes :*

1° L'identité et les coordonnées du responsable de traitement et, le cas échéant, celles de son représentant ;

2° Le cas échéant, les coordonnées du délégué à la protection des données ;

3° Les finalités poursuivies par le traitement auquel les données sont destinées ;

4° Le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés et les coordonnées de la commission ;

5° L'existence du droit de demander au responsable de traitement l'accès aux données à caractère personnel, leur rectification ou leur effacement, et l'existence du droit de demander une limitation du traitement des données à caractère personnel relatives à une personne concernée .

49. À titre liminaire, la formation restreinte relève que le ministère de l'intérieur ne conteste pas la caractérisation de ce manquement, rappelant seulement les engagements pris pour assurer, à l'avenir, l'information des personnes concernées.

50. La formation restreinte note que le groupement de gendarmerie départementale de Haute-Garonne et le commissariat de Cergy-Pontoise ont indiqué, dans leur réponse au questionnaire envoyé, que les personnes étaient informées de la présence du drone par un message vocal les invitant à se disperser. La préfecture de police de Paris a indiqué qu'aucun dispositif spécifique d'information n'avait été mis en place.

51. Il ressort des réponses apportées qu'aucune information répondant aux exigences de l'article 104 de la loi Informatique et Libertés n'a été communiquée aux personnes concernées.

52. La formation restreinte relève que, si l'article 107 de la loi Informatique et Libertés permet, sous certaines conditions, des restrictions aux droits des personnes et notamment au droit à l'information, ces restrictions doivent être *prévues par l'acte instaurant le traitement* . En l'espèce, en l'absence de tout acte instaurant les traitements en question, aucune limitation au droit à l'information ne pouvait être prévue.

53. Il ressort de l'ensemble de ces éléments que l'information délivrée aux personnes, quand elle existait, ne répondait pas aux exigences légales. La formation restreinte considère donc qu'un manquement à l'article 104 de la loi Informatique et Libertés est constitué.

III. Sur les mesures correctrices et leur publicité

54. Aux termes du III de l'article 20 de la loi du 6 janvier 1978 :

Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes :

1° Un rappel à l'ordre ;

2° Une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ; (…) .

55. La rapporteure propose à la formation restreinte que soient prononcés un rappel à l'ordre ainsi qu'une injonction de mettre le traitement en conformité avec les dispositions la loi Informatique et Libertés. Elle propose également que cette décision soit rendue publique.

56. En défense, le ministère de l'intérieur estime que le prononcé d'une mesure correctrice ne se justifie pas, une mise en demeure lui semblant suffisante en l'espèce, et que la publicité de l'éventuelle mesure à intervenir n'apparaît pas nécessaire. Enfin, il considère que l'injonction de cesser l'usage des drones n'est pas envisageable, cet usage constituant désormais une nécessité opérationnelle indéniable.

57. La formation restreinte considère que, dans le cas d'espèce, les manquements précités justifient que soit prononcé un rappel à l'ordre à l'encontre du ministère de l'intérieur pour les motifs suivants.

58. La formation restreinte relève la gravité du manquement relatif à la licéité des traitements, ce manquement privant l'ensemble des traitements mis en œuvre de base légale. Elle souligne également que les personnes concernées étaient privées de l'ensemble des garanties dont elles auraient dû bénéficier, notamment une information relative aux traitements ainsi que sur l'exercice de leurs droits.

59. Elle relève également les risques importants pour les droits et libertés des personnes, précédemment évoqués, liés à la possibilité offerte par ces nouveaux dispositifs d'identifier toute personne circulant sur l'espace public, y compris dans des circonstances pouvant révéler des informations particulièrement sensibles, par exemple liées à leurs opinions politiques, leurs convictions religieuses ou philosophiques ou leur appartenance syndicale.

60. Elle note aussi que les évolutions technologiques rendent les drones de plus en plus discrets avec des capacités augmentées de captation de leurs caméras qui donnent au ministère de l'intérieur la possibilité de faire voler ses drones à des altitudes de plus en plus importantes, tout en conservant une image d'une grande précision. Les personnes sont donc peu susceptibles de prendre conscience des traitements opérés et de la captation de leur image.

61. Enfin, la formation restreinte considère que le perfectionnement de technologies telles que la reconnaissance faciale pourrait entraîner, à l'avenir, des risques encore plus importants pour les droits et libertés individuelles si elles étaient couplées à l'utilisation de drones. Elle considère donc que leur déploiement en dehors de tout cadre légal doit être sévèrement sanctionné.

62. La formation restreinte estime que les éléments précités rendent également nécessaire qu'une injonction soit prononcée. En outre, le ministère ayant indiqué lors de la séance qu'il n'entendait pas renoncer, y compris temporairement, à l'usage de drones équipés d'une caméra, le prononcé d'une injonction constitue la mesure appropriée pour l'amener à n'utiliser des drones à cet effet que lorsqu'un cadre légal l'y autorisant aura été adopté.

63. Enfin, et pour les mêmes raisons, la formation restreinte estime nécessaire que sa décision soit rendue publique. Elle relève, sur ce point, que le public a démontré, au cours des derniers mois, un intérêt légitime pour les questions relatives au

traitement de ses données à caractère personnel par l'État. La publicité d'une décision de sanction par l'autorité spécialement chargée de la protection des données à caractère personnel apparaît ainsi pleinement justifiée.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide de :

· **prononcer à l'encontre du ministère de l'intérieur un rappel à l'ordre pour les manquements aux articles 89, 90 et 104 de la loi Informatique et Libertés ;**

· **prononcer à l'encontre du ministère de l'intérieur une injonction de mettre en conformité les traitements visés avec les obligations résultant de l'article 87 de la loi Informatique et Libertés, et en particulier :**

o **pour les finalités relevant du titre III de la loi Informatique et Libertés, ne recourir à la captation de données à caractère personnel à partir de drones qu'après l'adoption d'un cadre normatif autorisant la mise en œuvre de traitements de telles données ;**

· **rendre publique, sur le site de la CNIL et sur le site de Légifrance, sa délibération, qui n'identifiera plus nommément le ministère à l'expiration d'un délai de deux ans à compter de sa publication.**

Le président

Alexandre LINDEN

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.