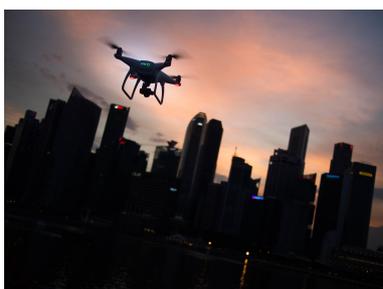


<https://www.observatoire-collectivites.org/spip.php?article8710>

Pas de surveillance de la voie publique par drone sans texte réglementaire protégeant les données personnelles

- Jurisprudence -



Date de mise en ligne : lundi 18 mai 2020

Copyright © Observatoire Smacl des risques de la vie territoriale - Tous

droits réservés

L'usage de drones pour vérifier le respect des règles de sécurité sanitaire applicables à la période de déconfinement est-il licite ?

[1]

Pas si les drones utilisés sont susceptibles de collecter des données identifiantes et ne comportent aucun dispositif technique de nature à éviter, dans tous les cas, que les informations collectées puissent conduire à rendre les personnes identifiables. Le juge des référés du Conseil d'Etat rappelle ainsi le nécessaire respect du cadre de la loi informatique et libertés du 6 janvier 1978 et pointe des risques d'un usage contraire aux règles de protection des données personnelles en l'absence de texte réglementaire en autorisant la création et en fixant les modalités d'utilisation devant obligatoirement être respectées ainsi que les garanties. Le recours à des drones pour la surveillance de l'espace public pour contrôler le respect des règles de sécurité sanitaire applicables à la période de déconfinement, est donc interdit tant qu'un arrêté ou décret ministériel n'aura pas été pris sur le sujet après avis de la CNIL, ou tant que les drones ne seront pas dotés d'un dispositif de nature à rendre impossible l'identification des personnes filmées.

Depuis le début du confinement, la police et la gendarmerie utilisent les drones pour surveiller le bon respect des règles du confinement : diffusion des consignes par haut-parleurs, surveillance de vastes espaces ou de zones difficiles d'accès, guidage des patrouilles au sol, détection d'éventuels contrevenants... Ainsi selon les données communiquées à la commission sénatoriale dans le cadre de la mission de suivi de la loi d'urgence pour faire face à l'épidémie de Covid-19, entre le 24 mars et le 24 avril, il a été recouru à des drones dans le cadre de 535 missions réalisées par la police nationale, dont 251 missions de surveillance et 284 missions d'information de la population.

En complément, les équipes de contrôle se sont également appuyées, afin d'orienter les patrouilles, sur les dispositifs de vidéo-protection des collectivités territoriales ainsi que sur les installations vidéo des réseaux SNCF et RATP.

Estimant que ce déploiement s'est fait en l'absence de tout cadre légal spécifique quant à l'utilisation des images filmées, deux associations [2] exercent un référé-liberté sollicitant la fin du déploiement de drones par la préfecture de police de Paris. Les deux associations s'appuient notamment sur deux documents publiés par Médiapart où la préfecture de Police de Paris reconnaît qu'il n'existe aucun cadre juridique spécifique pour les images captées par les drones, et cela alors qu'ils sont équipés de caméras haute-résolution permettant « la captation, la transmission et l'enregistrement des images » ainsi que « l'identification d'un individu ».

Le 5 mai 2020, le juge des référés du Tribunal administratif de Paris (TA Paris, 5 mai 2020, n° 2006861/9) rejette la demande : « il ne résulte d'aucune des pièces du dossier que les services de la préfecture de police auraient utilisé les drones dans des conditions permettant d'identifier les individus au sol ». Ainsi la préfecture de police n'a pas réalisé un traitement de données à caractère personnel quand bien même elle aurait « procédé à la collecte, à l'enregistrement provisoire et à la transmission d'images ».

Un but jugé légitime

Sur recours des deux associations, le juge des référés du Conseil d'Etat tranche dans un sens contraire. Certes il constate qu'en l'état de la pratique actuelle formalisée par une note du 14 mai 2020, les vols sont réalisés à une hauteur de 80 à 100 mètres de façon à donner une physionomie générale de la zone surveillée, qui est filmée en utilisant un grand angle sans activation du zoom dont est doté chaque appareil. Il concède également, dans le cadre de cette doctrine d'usage, que les drones ne sont plus équipés d'une carte mémoire de sorte qu'il n'est procédé à aucun enregistrement ni aucune conservation d'image.

Le juge des référés du Conseil d'Etat estime également que « la finalité poursuivie par le dispositif litigieux, qui est, en particulier dans les circonstances actuelles, nécessaire pour la sécurité publique, est légitime » et « qu'un usage du dispositif de surveillance par drone effectué conformément à la doctrine d'emploi fixée par la note du 14 mai 2020 n'est pas de nature à porter, par lui-même, une atteinte grave et manifestement illégale aux libertés fondamentales invoquées. »

Des données présentant un caractère personnel

Pour autant le Conseil d'Etat constate que le dispositif peut permettre l'identification des personnes. De fait les appareils en cause sont dotés d'un zoom optique et peuvent voler à une distance inférieure à celle fixée par la note du 14 mai 2020. Ils sont ainsi susceptibles de collecter des données identifiantes et ne comportent aucun dispositif technique de nature à éviter, dans tous les cas, que les informations collectées puissent conduire à rendre les personnes filmées identifiables. Dans ces conditions, poursuit le Conseil d'Etat, les données susceptibles d'être collectées par le traitement litigieux doivent être regardées comme revêtant un caractère personnel.

En effet l'article 3 de la directive du 27 avril 2016 définit, à son point 2, un traitement comme « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel 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 ».

Tel est bien le cas du 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 au sens de cette directive. Ainsi le dispositif litigieux constitue un traitement de données à caractère personnel qui relève du champ d'application de la directive du 27 avril 2016 et des dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Une autorisation par arrêté du ou des ministres compétents ou par décret, selon les cas, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés (CNIL) est donc nécessaire.

« Compte tenu des risques d'un usage contraire aux règles de protection des données personnelles qu'elle comporte, la mise en œuvre, pour le compte de l'Etat, de ce traitement de données à caractère personnel sans l'intervention préalable d'un texte réglementaire en autorisant la création et en fixant les modalités d'utilisation devant obligatoirement être respectées ainsi que les garanties dont il doit être entouré caractérise une atteinte grave et manifestement illégale au droit au respect de la vie privée. »

Un texte réglementaire ou des dispositifs techniques rendant impossible l'identification des personnes

Le juge des référés enjoint donc à l'Etat de cesser de procéder aux mesures de surveillance par drone, du respect à Paris, des règles de sécurité sanitaire applicables à la période de déconfinement tant qu'il n'aura pas été remédié à l'atteinte caractérisée au point précédent, soit par l'intervention d'un texte réglementaire, pris après avis de la CNIL, soit en dotant les appareils utilisés par la préfecture de police de dispositifs techniques de nature à rendre impossible, quels que puissent en être les usages retenus, l'identification des personnes filmées.

Cet obstacle juridique peut donc être levé par la publication d'un décret, pris après avis de la CNIL, pour créer une procédure d'autorisation de ce traitement de données personnelles par drone à des fins de mission de police administrative.

Quid des drones utilisés par les collectivités ?

Les collectivités territoriales suivront avec attention l'évolution de la réglementation en la matière. Rappelons que dans une réponse à une question parlementaire ([Réponse du 11 janvier 2018 à la Question écrite n° 01425 de M. Jean Louis Masson](#)), le Ministère de la cohésion des territoires avait clairement indiqué qu'une collectivité ne pouvait utiliser des drones pour constater des infractions aux règles d'urbanisme. En effet la captation d'images par la voie des airs au moyen d'un drone survolant une propriété privée peut être considérée comme une ingérence dans la vie privée. Ainsi la captation d'images opérée par des policiers dans un lieu inaccessible depuis la voie publique doit, en application des dispositions de l'article 8 de la Convention européenne des droits de l'homme, être fondée sur une prévision législative, telle que l'article 706-96 du code de procédure pénale. À défaut, aucune intrusion ne peut être valablement effectuée en un tel lieu. En conséquence, le constat d'une infraction sur une propriété privée à l'aide d'un drone peut être considéré comme illicite dès lors que la zone contrôlée est inaccessible aux regards.

L'ordonnance du juge des référés du Conseil d'Etat du 18 mai va au-delà puisqu'il juge, qu'en l'absence de textes

réglementaire l'autorisant et le réglementant, ce n'est non seulement la surveillance des lieux privés qui n'est pas possible mais également celle des lieux publics si les drones utilisés peuvent fournir des données identifiantes. L'occasion de rappeler que l'usage des caméras mobiles dont peuvent être équipés les policiers municipaux est strictement réglementé et soumis à autorisation préfectorale accompagné d'un engagement de conformité auprès de la CNIL. Les enregistrements ne peuvent être effectués que pour trois raisons [3], les données enregistrées par les caméras individuelles doivent être transférées sur un support informatique sécurisé et ne peuvent être conservées plus de six mois, les caméras doivent être portées de façon apparente par les agents avec un signal visuel spécifique indiquant si la caméra enregistre, le déclenchement de l'enregistrement fait l'objet d'une information des personnes filmées... Il aurait été incohérent que ces règles puissent être contournées par l'usage d'un drone. L'ordonnance du Conseil d'Etat du 18 mai 2020 lève toute ambiguïté à ce sujet.

Post-scriptum :

- La captation d'images par drone pour un visionnage en temps réel et pour la réalisation de missions de police administrative constitue un traitement de données à caractère personnel qui relève du champ d'application de la directive du 27 avril 2016 et des dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
 - Un texte réglementaire pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés (CNIL) est nécessaire pour qu'un tel usage soit licite. Le texte doit autoriser la création, fixer les modalités d'utilisation devant obligatoirement être respectées, et les garanties dont il doit être entouré caractérisent une atteinte grave et manifestement illégale au droit au respect de la vie privée.
 - En l'absence d'un tel texte les drones ne peuvent être utilisés pour la surveillance de la voie publique à moins qu'ils soient dotés de dispositifs techniques de nature à rendre impossible, quels que puissent en être les usages retenus, l'identification des personnes.
-

Etes-vous sûr(e) de votre réponse ?

- [Un agent refusant de se soumettre à un système de pointage impliquant un traitement de ses données personnelles \(ici un contrôle biométrique\) peut-il être sanctionné disciplinairement même en l'absence d'information individuelle préalable sur l'existence d'un tel dispositif comme l'impose pourtant la loi "Informatique et libertés" ?](#)
 - [Une association peut-elle être sanctionnée pour avoir insuffisamment protégé les données personnelles de ses utilisateurs sur son site internet bien que celui-ci ait été développé par un prestataire professionnel ?](#)
-

[1] Photo : Goh Rhy Yan sur Unsplash

[2] La Quadrature du Net et la Ligue des droits de l'Homme

[3] Prévention des incidents au cours des interventions des agents de la police municipale ; constat des infractions et la poursuite de leurs auteurs par la collecte de preuves ; la formation et la pédagogie des agents de police municipale