LES DRONES PRODUISENT-ILS DES DONNEES PERSONNELLES ?

XAVIER BIOY

Référence de publication : Bioy, Xavier (2020) "Usage des drones par la police et données personnelles - Pixéliser l'espace public ?", Note sous CE, Ord. Réf., 18 mai 2020, Association La quadrature du net, Ligue des droits de l'Homme, n°s 440442, 440445.
Actualité juridique. Droit administratif (AJDA) (27). p. 1552-1559.

LES DRONES PRODUISENT-ILS DES DONNÉES PERSONNELLES ?

Le juge des référés peut-il considérer qu'une liberté est déjà gravement violée par la seule mobilisation d'un dispositif technique qui n'est pas encore mis en oeuvre mais qui potentiellement peut l'être ? La réponse semble désormais positive, par l'application volontariste des textes relatifs à la protection des données personnelles au cas des drones (1).

La préfecture de police de Paris a en effet pensé bien faire en utilisant un drone pour surveiller les espaces publics et ainsi vérifier le respect de l'article 6 du décret n° 2020-545 du 11 mai 2020 (prescrivant les mesures générales nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire) imposant l'interdiction de « tout rassemblement, réunion ou activité à un titre autre que professionnel sur la voie publique ou dans un lieu public, mettant en présence de manière simultanée plus de dix personnes [...] ».

La préfecture n'a pensé devoir se conformer qu'aux exigences légales en matière de survol de la capitale. Selon son communiqué diffusé quelques jours après le début des rotations, « l'unité des moyens aériens inscrit son action dans le cadre de la réglementation civile définie par l'arrêté du 17 décembre 2015 relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord (modifié par l'arrêté du 30 mars 2017) et par l'arrêté du 17 décembre 2015 relatif à la conception des aéronefs civils ». Ces textes ont été complétés par la loi du 24 octobre 2016 relative au renforcement de la sécurité de l'usage des drones civils. Cet usage bénéficie donc d'un cadre dérogatoire par l'article 8 de l'arrêté du 17 décembre 2015, relatif à la conception des aéronefs civils qui circulent sans personne, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent, dit « conception des aéronefs civils » et l'article 10 de l'arrêté 17 décembre 2015, relatif à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord, pour les drones appartenant à l'Etat « utilisés dans le cadre de missions de secours, de sauvetage, de douane, de police ou de sécurité civile [...] lorsque les circonstances de la mission et les exigences de l'ordre et de la sécurité publics le justifient » (not. Arr. du 17 déc. 2015, art. 10).

En s'appuyant sur ces éléments, le tribunal administratif de Paris (Ord. n° 2006861 du 5 mai 2020) a jugé que les services de la préfecture de police n'ont pas utilisé les drones dans des conditions permettant d'identifier les individus au sol, ce qui constitue un usage « légitime », selon le mot du Conseil d'Etat, en police administrative, et qu'il n'en a été fait aucun usage en matière de police judiciaire. Ce qui conduit à écarter la qualification de traitement de données à caractère personnel quand bien même il aurait été, selon le tribunal, « procédé à la collecte, à l'enregistrement provisoire et à la transmission d'images ».

Ici en appel, les deux requêtes demandent la suspension de la décision d'usage des drones et l'injonction de cesser de capter des images, de les enregistrer, de les transmettre ou de les exploiter, puis de détruire toute image déjà captée dans ce contexte, le tout sous astreinte. Tout l'enjeu réside dans une série de qualifications qui déterminent le régime applicable au drone capteur d'images (même si on peut penser que le processus a été inverse dans l'esprit du juge).

Rien de plus déterminant en effet que la qualification des faits et situations en droit ; et pourtant l'acte juridictionnel de qualifier se détermine au regard de plusieurs éléments : généralement les classifications préexistantes dans les textes ou la jurisprudence, le langage courant utilisé, avec lequel il est prudent de ne pas prendre trop de distances, la cohérence des régimes qui seront ainsi déclenchés, le souhait d'inclure ou non l'objet considéré dans le raisonnement en vue de la solution projetée... Tous ces éléments sont surdéterminés par le contexte dans lequel se prononce le juge et donc la question que le procès pose.

Pour les requérants, un dispositif de captation d'images constitue en soi un traitement de données à caractère personnel. Il doit donc disposer d'une base légale et se conformer au règlement général sur la protection des données (RGPD) ainsi qu'à la législation subséquente, mais encore à l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, notamment quant à l'existence d'un délai de conservation des données (le préfet affirmant que celles-ci sont effacées dès la mission achevée), l'information des personnes concernées, l'existence de mesures techniques et organisationnelles (telles que la pseudonymisation) destinées à mettre en oeuvre la minimisation des données, leur accessibilité, leur adaptation à la finalité du traitement (quantité de données et type) et la proportionnalité au regard de l'objectif de surveillance, de façon effective et à assortir le traitement des garanties nécessaires pour protéger les droits de la personne concernée.

Pour le juge, la condition d'urgence n'a guère suscité de débats car la mesure court déjà depuis plusieurs jours et ne connaît pas de date limite temporelle. Sans compter les circonstances qu'invoque systématiquement le Conseil d'Etat dans ses ordonnances liées à la pandémie de covid-19 : les différentes mesures réglementaires prises par le ministre de la santé, le Premier ministre, d'abord selon les sources ordinaires, ensuite sur le fondement des lois du 23 mars 2020 et du 11 mai 2020 créant et prorogeant l'état d'urgence sanitaire. Ce rappel du contexte signifie en principe que la santé publique peut justifier un surcroît d'atteintes aux libertés, à condition que celles-ci soient adaptées et proportionnées à ces objectifs spécifiques, ce qui ne sera pas le cas ici. L'intervention de l'état d'urgence fixe au niveau législatif le type de mesures qui peuvent être adoptées, excluant, *a priori*, toute autre. Or, la surveillance des rassemblements par drone n'y figure pas. Ce dispositif, spontané, est conçu comme complémentaire, comme accessoire aux décrets qui limitent les rassemblements de personnes sur la voie publique. L'accessoire peut néanmoins se révéler pire que le principal du point de vue des libertés.

Quant au fond, le Conseil d'Etat a choisi de considérer les potentialités du drone plus que son usage réel ou attesté, exprimant une forme de défiance par rapport aux forces de l'ordre. Selon l'ordonnance ici commentée, « il est constant 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 » (pt 14). Par la suite, le juge y voit néanmoins un traitement de données personnelles sans garantie. Là où, en première instance, le tribunal a au contraire statué au regard des buts et pratiques attestés par l'administration, le Conseil d'Etat opte pour anticiper sur d'autres usages en puissance en exigeant des garanties supérieures. C'est pourquoi il considère que le drone n'est pas seulement les yeux embarqués d'un policier mais le moyen d'identifier éventuellement un individu, grâce au zoom ou autre procédé que le juge ne caractérise pas. Cette attitude apparaît singulière car, à plusieurs reprises déjà, des associations de défense des libertés ont demandé en référé des garde-fous contre des usages encore virtuels de dispositifs techniques. Le juge s'est alors retranché derrière l'existence de cadres légaux qui encadreraient si nécessaire ces usages non avérés. En particulier en référé-liberté, cadre qui entend faire cesser une atteinte actuelle et non future, à défaut d'être certaine.

Néanmoins, ici, cela débouche sur l'injonction de cesser de procéder aux mesures de surveillance par drone, tant qu'un texte réglementaire, pris après avis de la Commission nationale de l'informatique et des libertés (CNIL), n'a pas autorisé la création du traitement de

données ou bien que les drones soient équipés de dispositifs techniques de nature à rendre impossible, quels que puissent en être les usages retenus, l'identification des personnes filmées. Tout ceci dans le respect des dispositions de la loi du 6 janvier 1978 applicables aux traitements relevant du champ d'application de la directive du 27 avril 2016. Cette décision complète une jurisprudence relativement volontariste quant à l'implication du juge dans le contrôle des fichiers de police (M.-O. Diemer, Le contrôle des fichiers de police par le Conseil d'Etat, *in* E. Debaets *et alii*, *Les fichiers de police*, Institut universitaire Varenne, Coll. Colloques et Essais, 2019, p. 367 ; v. not. CE 17 juill. 2013, n° 359417, *Elkaim*, Lebon ; AJDA 2013. 2032, concl. E. Crépey, concernant le droit d'accès au fichier via son responsable).

Le Conseil d'Etat tranche implicitement un conflit de qualifications des techniques de surveillance, pour parvenir à établir l'existence d'un traitement de données, dont le régime doit être évalué au regard des libertés en jeu.

I - La qualification des techniques de surveillance

Qu'est-ce qui compte pour qualifier juridiquement l'information perçue par le drone ? Est-ce la nature informative de l'image instantanée et réelle, quoique numérisée, mais alors quelle différence avec un policier juché sur un toit ? Est-ce l'objet électronique et informatique qui la produit ? Ou faut-il attendre la plus-value d'un traitement par algorithme qui peut ainsi révéler d'autres informations ? Ou sont-ce encore les usages, les finalités de la mission ? Faut-il seulement que l'information soit accessible éventuellement ou exige-t-on qu'elle soit effectivement révélée et utilisée, la donnée est-elle potentialité d'information ou information elle-même ? La qualification retenue par le juge porte sur ce que « peut faire » le drone, et non ce qu'il « fait » ou ce qu'il « est ».

A. La qualification du drone

Le drone se conçoit pour nous tous comme un objet volant télécommandé pouvant servir à bien des usages. Alors qu'il a été un temps considéré comme un ovni du droit (R. Hanicotte, Une nouvelle catégorie d'OVNI juridique : les drones, Gaz. Pal. 13 nov. 2014, n° 1996, p. 6 ;

S. Bergès et N. Laurendeau, Le drone aérien civil : un objet juridique volant identifié, LPA 15 févr. 2018, n° 1334, p. 5), le législateur a semblé vouloir l'inclure, dans l'abstrait, dans la catégorie des aéronefs sans pilote dans le but de sécuriser l'usage de l'espace aérien et les zones considérées comme « réglementées ou dangereuses » (L. n° 2016-1428 du 24 oct. 2016 renforçant la sécurité de l'usage des drones civils). Le but de cette qualification semble avoir été de soumettre ces objets à identification et à la législation sur le vol, parmi tous les autres navires volants « aéronefs », habités ou non. En 2012, deux arrêtés ont été adoptés (modifiés le 17 décembre 2015) pour réglementer d'une part, la « conception » et les conditions d'emploi des drones et d'autre part, leur « utilisation » dans l'espace aérien. Une déclaration en préfecture est obligatoire pour les vols en agglomération et en zone peuplée (Th. Wickers *et alii*, Sécurité / Police - Les drones et leurs usages [partie 2] Quel encadrement pour les personnes publiques ?, JCP Adm. 2018, n° 2240).

B. La notion de prévention des infractions

Le Conseil d'Etat a déjà indiqué que le critère essentiel dans la détermination du champ juridique applicable est la finalité poursuivie par le traitement et non son objet. Par exemple, un fichier qui permet de lutter contre la fraude fiscale n'a pas été mis en oeuvre avec une finalité pénale, il relève donc du RGPD (CE, ass., 19 juill. 2019, n° 424216, *Association des Américains accidentels*). Il inscrit les drones dans le champ de la directive dite « Police-justice » en raison de leur « finalité » en y voyant une activité de prévention des infractions. L'applicabilité de la directive n° 2016/680 du 27 avril 2016 n'allait pourtant pas de soi. D'ailleurs certains auteurs estiment que l'utilisation de drones dans le cadre d'une mission de police est limitée par le RGPD et non à la directive (v. M. Bourgeois et B. Touzanne, Les aéronefs civils télépilotés avec capteurs : des drones de droit, CCE 2015. Etude 22, spéc. n° 13 ; C. Rotily et L. Archambault, Drones civils professionnels et RGPD : enjeux liés à la collecte des données personnelles et au respect de la vie privée, Dalloz IP/IT 2019. 376).

La directive vise en effet principalement les activités de police judiciaire et se préoccupe de répression. Son champ est celui des « activités menées à des fins de prévention et de détection des infractions pénales ». Or le drone ici en cause se situe au coeur de la police administrative de maintien de l'ordre sanitaire et exclut tout lien avec les infractions pénales qu'il ne cherche ni à identifier ni à poursuivre (elles le seront au sol). La directive ne définit pas ce qu'elle entend

par prévention. L'article 1er expose qu'elle s'applique à l'égard du traitement utilisé « 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 ».

Concernant l'usage du moment, il faudrait envisager la mission de surveillance des drones comme une action de prévention, au sens de la directive, ce qui mettrait clairement en porte-à-faux la conception traditionnelle de la distinction française entre police administrative et police judiciaire ; la surveillance étant le coeur de la première. Si, comme le fait ici le juge, on envisage une identification possible des personnes, lesquelles peuvent alors faire l'objet de poursuites contraventionnelles pour la violation des décrets interdisant les rassemblements, alors on peut imaginer une forme de prévention.

Quant à savoir si on peut considérer que l'activité de police correspond bien à la prévention des infractions pénales, alors même que l'administration s'en défend, il est exact que le souci de surveiller la formation de groupes importants de personnes se retrouvant le long des points d'eau ou des parcs parisiens tend à empêcher la constitution d'une infraction pénale. L'article L. 3136-1 du code de la santé publique (CSP - modifié par la loi n° 2020-546 du 11 mai 2020) entend apporter une sanction au non-respect des mesures prises au titre de l'article L. 3131-15 du CSP, notamment en son 6e - « limiter ou interdire les rassemblements sur la voie publique ainsi que les réunions de toute nature ». Il le punit de l'amende prévue pour les contraventions de la quatrième classe (la procédure de l'amende forfaitaire s'appliquant), cinquième classe si cette violation est constatée à nouveau dans un délai de quinze jours (l'art. R. 49 du code de procédure pénale prévoit que les contraventions de la 4e classe sont réprimées par une amende de 135 €). Ces contraventions peuvent être constatées par les agents de police nationale et municipale, les gardes-champêtres, les agents de la ville de Paris chargés d'un service de police, les contrôleurs de la préfecture de police et agents de surveillance de Paris, à condition qu'elles ne nécessitent pas d'actes d'enquête. Ce n'est que sous cette condition ténue que la police administrative entre dans le champ de la directive.

C. La disqualification de la vidéo-protection

Les drones sont en pratique déjà utilisés pour des missions de police, de surveillance, notamment de grands rassemblements, de manifestations, de plages et de la baignade sur le fondement des dispositions combinées des articles L. 2212-2, L. 2212-3, et L. 2213-23 du code général des collectivités territoriales sans que personne n'ait songé à saisir le juge (L. Archambault et C. Rotily, De l'utilité des drones au service de la sécurisation des populations et des espaces : dans quel cadre juridique ?, Gaz. Pal. 19 juin 2018, n° 3243, p. 23). Les drones militaires pourvoient d'ailleurs régulièrement aux besoins de la surveillance en zone gendarmerie.

En pratique, on ne voit pas tout de suite ce qui différencie autant les caméras fixes de vidéo-protection de celles qui sont embarquées. Elles se trouvent pourtant soumises à deux régimes distincts quoique proches. *A priori*, l'utilisation de drones dans le cadre d'une mission de police pourrait être régie par les dispositions du code de la sécurité intérieure (CSI) relatives à la vidéo-protection (CSI, art. L. 251-1 à L. 263-1), sous réserve d'utiliser ces drones pour l'une des finalités visées par la liste limitative de l'article L. 251-2 du même code. La préfecture a ainsi entendu exclure le régime de vidéo-protection et se placer directement sous l'emprise des articles 9 du code civil et 226-1 du code pénal relatifs au respect la vie privée et le Conseil d'Etat n'examine pas même cette voie qui, en effet, se heurte à différentes difficultés de transposition.

D'abord quant aux finalités fixées à l'article L. 251-2 du CSI. Ces finalités, pourtant nombreuses, se relient à la protection des bâtiments publics, aux risques naturels, au contrôle des zones où la délinquance s'exerce plus favorablement ou des flux de transport. *A priori*, ces mobiles ne correspondent pas à la surveillance sanitaire. Cependant, le point 5° évoque « la prévention des atteintes à la sécurité des personnes et des biens », certes en lien avec des risques d'agression, de vol ou de trafic de stupéfiants ; mais si la zone se trouve déjà vidéo-surveillée, la police utilise déjà les caméras pour lutter contre la propagation de l'épidémie. L'ajout d'un drone ne changerait pas substantiellement les choses du point de vue des missions.

Ensuite, en raison de la limite tenant au numérique. L'article L. 251-2 du CSI exclut de la vidéo-protection les enregistrements 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, lesquels sont soumis à la loi relative à l'informatique, aux fichiers et aux libertés. Ce ne serait pas un problème ici, du moins avant la « lecture » du Conseil d'Etat.

Le régime de la vidéo-protection aurait pourtant satisfait les exigences de la protection des données personnelles et même au-delà en prévoyant les garanties que la directive appelle et qui restent à déterminer pour les drones. En particulier, le visionnage des images ne peut être opéré que par les personnes spécifiquement et individuellement habilitées, formées et sensibilisées aux règles de mise en oeuvre. Le régime prévoit d'emblée de couvrir autant la police administrative que les actes de police judiciaire, ce qui eut évité au juge de suspecter la police d'être tentée de passer de l'un à l'autre. Le régime d'autorisation préfectorale et la durée de conservation des images sont déjà fixés. De plus, l'article R. 252-11 du CSI prévoit que le titulaire de l'autorisation tient un registre mentionnant notamment les enregistrements réalisés, la date de destruction des images, le cas échéant, la date de leur transmission au parquet.

Cependant, d'autres raisons conduisent à approuver la solution du Conseil d'Etat. D'abord parce que l'autorisation issue du régime des données personnelles devra émaner du ministre directement et non seulement du préfet pour lui-même. Ainsi les motifs et objectifs de la mesure seront circonstanciés et limités aux missions de police administrative (si c'est toujours le cas). Ensuite parce que certaines garanties de la vidéo-protection sont difficilement transposables aux drones, même si ce n'est pas impossible. Par exemple, l'obligation d'informer la population à l'entrée des zones surveillées (pour le drone, un message diffusé par le haut-parleur embarqué ou une publicité par les voies habituelles pour la période de crise concernée). La base légale du traitement, les destinataires des données personnelles et certains usages pourront ainsi être mentionnés via un site internet. Il en est de même du recueil de l'avis d'une commission départementale présidée par un magistrat ou de l'obligation, désormais applicable à la vidéo-protection, d'une étude d'impact préalable au déploiement des caméras (concept de « *privacy by design* »). Enfin, et surtout, les autorisations sont valables cinq ans, durée qui correspond aux usages pérennes qui en sont faits et qui ne convient sans doute pas à l'usage ponctuel (seul souhaitable) des drones. Ceci étant dit, une procédure accélérée d'autorisation provisoire (quatre mois) existe, en cas d'urgence et de risques particuliers d'actes de terrorisme, ou pour la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens (CSI, art. L. 223-4).

II - La qualification de la technique de surveillance

Cette première étape conduit directement aux qualifications de « donnée » et de « traitement ».

A. L'image numérisée peut être une donnée personnelle

Pour la préfecture de police, « les images sont prises en utilisant un grand angle pour filmer des flux de circulation, des rassemblements, des zones urbaines ou rurales ou la progression de cortèges. Elles ne permettent donc pas l'identification d'un individu, sauf lorsqu'elles sont utilisées dans un cadre judiciaire que ce soit en flagrance, en préliminaire ou au titre d'une instruction. [...] Dès la fin de la mission, les images sont supprimées de la carte mémoire. Elles ne font l'objet d'aucun recoupement avec des fichiers de police ». Cette exclusion trop empressée d'un usage judiciaire a convaincu le juge de première instance de l'absence de toute captation de donnée personnelle, mais au contraire alerté le Conseil d'Etat. D'ailleurs, la CNIL s'interroge de longue date sur l'applicabilité de la loi Informatique et libertés aux éléments traités par une caméra embarquée (Usages des drones et protection des données personnelles, Actualités CNIL, 3 oct. 2012).

Selon le considérant 21 de la directive n° 2016/680 du 27 avril 2016, les principes relatifs à la protection des données s'appliquent à toute information concernant une personne physique identifiée ou identifiable « [...] en considérant l'ensemble des moyens raisonnablement susceptibles d'être utilisés [...] pour identifier la personne physique directement ou indirectement, [...] tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes [...] ». Dans la mesure où la police affirme n'avoir ni l'intention, ni les moyens, pour l'heure d'utiliser des moyens biométriques identifiants, on pourrait penser que la notion de donnée personnelle ne s'applique pas ici. Le Conseil admet bien que l'absence d'identification des personnes filmées et l'absence de toute conservation d'images exclut toute identification, même indirecte, ce qui exclurait la qualification de donnée personnelle.

Mais il va forcer le destin en imposant cette qualification par une sorte de précaution. Le Conseil

d'Etat écarte l'usage actuel, pourtant codifié par l'administration elle-même, pour imaginer ce qui serait « susceptible » de se produire : un usage du zoom qui permettrait d'identifier les personnes. Force est de se demander comment cette identification se pourrait en l'absence de dispositif biométrique mais il est vrai qu'elle devient possible pour qui reconnaîtrait des visages. Ainsi le critère de qualification retenu ne réside plus dans la finalité fixée par l'administration mais dans la capacité technique (elle-même surestimée) intrinsèque du dispositif. C'est donc la finalité (dont l'appréciation a été déjà volontariste) qui détermine une partie du choix du régime (la directive) mais c'est la technique seule qui achève de l'imposer. En réalité, la technique a commandé la qualification de donnée et la finalité lui a affecté la directive Police-justice plutôt que le RGPD.

B. Le transfert vers le centre de vidéo-protection est un traitement de données

Selon la police, les images captées sont transmises sur une tablette à disposition de l'autorité responsable du dispositif ou sur un poste fixe dédié, installé dans le centre de commandement de la direction en charge de la conduite des opérations.

Selon le 2. de l'article 2 de la directive, elle s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. Un « traitement », selon la directive, consiste en « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel [...] telles que la collecte, [...] la consultation, l'utilisation, la communication par transmission [...] ». A cet égard, toute captation numérique d'image entre dans la notion de traitement.

Cette conception conduit à une forme de « totalitarisme » de la donnée qui devient la catégorie à tout dire et tout rassembler. Or, qu'est-ce qu'une donnée personnelle ? Une information identifiante qui permet de révéler quelque chose du mode de vie d'un individu. La donnée est le moyen de bloquer l'accès à la vie privée. Par une exagération du droit (sans doute salutaire), de moyen elle devient la fin.

On constate généralement une tendance délétère à la confusion entre « donnée personnelle » et

« information », ici le renseignement révélé par les images du drone. L'hypertrophie de la notion de donnée tend à phagocyter tout ce qui, jusqu'ici était seulement un savoir, une information, une donnée non personnelle, en l'occurrence objet de l'activité de police. Faire de toute information susceptible de s'appliquer à une personne lointainement identifiable conduit à faire disparaître l'espace public, qui, sous cet angle, se compose uniquement de données privées. Un policier qui croise une personne qu'il connaît, ou qu'il est susceptible d'identifier par une autre information dont il peut disposer, détient ainsi une « donnée personnelle ». Certes, il ne s'agit pas encore d'un traitement, faute d'une automatisation externe et technique, mais l'information est de même nature qu'une donnée personnelle. Cette même information change alors de nature selon qu'elle est vue par un outil ou par un oeil, une oreille, le toucher corporel. Sans pouvoir le développer ici, il faut garder à l'esprit que la différence entre intelligence humaine et artificielle, pour des usages courants comme l'identification d'un individu, n'est guère marquée ; il s'agit de comparer une information à un ensemble d'autres. Une simple photo d'un visage a déjà une nature biométrique. Un robot qui identifierait un individu en comparant sa photo à celle contenue dans un fichier, ne fait pas une opération différente du policier. Si bientôt nous créons des humains (policiers) « augmentés » par des neurotransmetteurs, tels qu'utilisés déjà par les militaires, leur regard sera traitement de donnée et il faudra alors « laver les cerveaux » après les opérations ! Se fonder sur la seule existence d'une technique dévoie le droit de sa fonction de contrôle des usages. On perd de vue que le régime des données personnelles, plus encore des données sensibles, a été institué pour permettre à un individu de refuser de révéler sa vie à d'autres, non pour cacher ce qui est vu de tous et de ce fait vider l'espace public de sa substance collective en le voyant comme une collection de données personnelles. Il y a là une question de « droit politique » essentielle.

III - Un dispositif conforme aux libertés, sous réserves

Les vertus de ce « réductionnisme numérique » méritent examen du point de vue du spectre des libertés.

A. Les garanties apportées par l'injonction

Dire que le dispositif technique permet un usage liberticide mais que celui-ci n'a pas eu lieu, revient à considérer qu'il y a atteinte putative. Ce faisant, le juge semble exprimer une forme de défiance par rapport aux engagements de la police mais surtout il entend tenir compte d'un usage potentiel et non avéré contraire aux libertés. Certes, il use du référé pour faire cesser une situation actuelle, mais qui n'est pas encore contraire à une liberté, seulement « susceptible de l'être ». Cette option semble être assez nouvelle et quelque peu surprenante. Car généralement le juge se refuse à intervenir dans l'urgence lorsqu'une liberté ne se trouve pas d'ores et déjà méconnue par une pratique passée. Le reste de la jurisprudence relative à la covid-19 en atteste. Lorsque les requérants invoquent une potentialité de violation, le juge ne s'estime pas en position d'enjoindre un comportement préventif. Certes, il s'agissait le plus souvent d'exiger des moyens matériels face à l'abstention de l'administration pour lutter contre des faits et certes, le juge a prescrit des modifications normatives (légères, très légères) dans une ordonnance récente (CE, ord., 28 mars 2020, n° 439674, *Syndicat des médecins d'Aix et région*, AJDA 2020. 700) enjoignant de préciser la portée d'une dérogation et réexaminer le maintien d'une autre, enfin évaluer les risques pour la santé publique) mais la solution ici retenue tient de l'audace.

Du point de vue de la convention européenne des droits de l'homme (v. K. Blay-Grabarczyk, Le contrôle des fichiers de police par la CEDH, *in* E. Debaets *et alii, Les fichiers de police*, préc., p. 291), il y a fort à parier que la solution ici retenue soit vue comme conforme aux attentes de Strasbourg en matière de fichiers de police. Certes, une simple mémorisation, sans autre usage, constitue déjà une ingérence dans le droit à la vie privée (CEDH 26 mars 1987, n° 9248/81, *Leander c/ Suède*) et les garanties doivent être proportionnelles aux menaces (CEDH 4 déc. 2008, n° 30562/04, *S. et Marper c/ Royaume-Uni*, AJDA 2009. 872, chron. J.-F. Flauss ; D. 2010. 604, obs. J.-C. Galloux et H. Gaumont-Prat ; AJ pénal 2009. 81, obs. G. Roussel ; RFDA 2009. 741, étude S. Peyrou-Pistouley ; RSC 2009. 182, obs. J.-P. Marguénaud). Mais s'agissant ici d'un traitement sans enregistrement et compte tenu de la faiblesse des risques pour les données personnelles, il est difficile d'établir une comparaison avec l'une des affaires jugées par la Cour, lesquelles portent principalement sur la pertinence et l'adéquation de la collecte (CEDH 18 avr. 2013, n° 19522/09, *M. K. c/ France*, D. 2013. 1067, et les obs. ; et 2014. 843, obs. J.-C. Galloux et H. Gaumont-Prat ; RSC 2013. 666, obs. D. Roets) ou la durée de conservation (CEDH 17 déc. 2009, *Bouchacourt, Gardel, M.B. c/ France ;*

CEDH 22 juin 2017, n° 8806/12, *Aycaguer c/ France*), le droit d'accès et d'effacement (CEDH 18 oct. 2011, n° 16188/07, *Khelili c/ Suisse*), autant d'éléments peu pertinents en l'absence d'enregistrement des images mais qui s'imposeront avec le régime des données.

B. Les autres libertés, réservées

Imposer le régime des données personnelles suffit-il à conjurer l'atteinte à la vie privée ? Le Conseil d'Etat omet de répondre à l'argument tenant à la violation de la vie privée par le regard en altitude d'un drone sur les espaces privés ainsi dévoilés. Le point 14 suggère la bénédiction du juge alors que l'analogie avec le régime de la vidéo-protection le compromet. La vie privée se résume-t-elle aux données personnelles ? A l'évidence non, d'une part parce que la tendance est à autonomiser le régime des données par rapport au respect du secret de la vie privée ; d'autre part parce que des règles générales protègent l'intimité des lieux.

Quant au premier point, les requérants soutenaient en ce sens que l'ordonnance du tribunal était entachée d'une erreur de droit en ce qu'elle subordonnait la caractérisation d'une atteinte au droit à la vie privée à la condition que le dispositif en cause constitue un traitement de données personnelles. Les deux notions sont-elles confondues ? L'autonomisation du droit au respect des données personnelles par la charte des droits fondamentaux de l'Union atteste de ce que la notion de vie privée est à la fois plus large et potentiellement distincte de celle des données personnelles. Néanmoins, sans ignorer cette autonomie sur le terrain du droit de l'Union et en dépit de la mention de la charte des droits fondamentaux de l'Union européenne et de la directive n° 2016/680 du 27 avril 2016, le Conseil d'Etat procède à son propre aménagement, plus proche de celui du Conseil constitutionnel (E. Debaets, *Le droit à la protection des données personnelles, Recherche sur un droit fondamental*, thèse Paris-I, 2014) qui intègre, « pour l'application de l'article L. 521-2 du code de justice administrative », le droit à la protection des données personnelles au droit au respect de la vie privée.

Quant au second point, pour le juge civil, la prise de vue aérienne par drone d'une propriété privée sans l'accord des propriétaires constitue une atteinte à leur vie privée, même si elle n'en montre pas les occupants. Elle peut dès lors être considérée comme une preuve illicite (Paris, 15 mai 2019, n° 18/26775, RTD civ. 2019. 870, obs. H. Barbier ; Gaz. Pal. 5 nov. 2019, n° 361u6, p. 57, obs. H. Herman). Sur le plan pénal, pour les autres personnes que l'Etat, l'article

226-1 du code pénal visant aussi bien l'enregistrement que la captation, la fixation et la transmission, l'atteinte à la vie privée peut résulter d'un « drone se limitant à transmettre à son utilisateur, en temps réel, des sons captés au cours du vol sans aucun enregistrement » (N. Cazé-Gaillarde, Atteintes à la vie privée, Rép. pén., Dalloz, 2019). Même des enquêteurs de la police judiciaire ne sauraient photographier clandestinement les plaques d'immatriculation des véhicules se trouvant à l'intérieur d'une propriété privée non visible de la voie publique, aux fins d'identification des titulaires des cartes grises, sans l'appui d'aucune disposition de procédure pénale, cela viole l'article 8 de la convention européenne (Crim. 21 mars 2007, n° 06-89.444, D. 2007. 1204, obs. A. Darsonville ; et 1817, chron. D. Caron et S. Ménotti ; AJ pénal 2007. 286, obs. G. Royer ; RSC 2007. 841, obs. R. Finielz ; et 897, obs. J.-F. Renucci ; et 2008. 655, obs. J. Buisson).

Le régime de la vidéo-protection interdit formellement aux autorités publiques de filmer les propriétés privées, non au nom des données personnelles mais de la protection du secret de la vie privée. S'il s'agit d'un drone, toute personne qui souhaite réaliser des enregistrements d'images ou de données dans le champ du spectre visible au-dessus du territoire national est tenue de souscrire une déclaration au plus tard quinze jours avant la prise de vue (C. aviat., art. D133-10). Ici, finalement, le Conseil d'Etat ne répond pas à l'argument des requérants sur ce fait précis et, une fois purgée l'illégalité par une autorisation du ministre ou un dispositif désactivant le zoom, les drones pourront reprendre leur activité et le juge administratif être à nouveau saisi de ce point qu'il aurait pu régler directement.

Il eut donc été souhaitable que le Conseil d'Etat vérifie la proportionnalité de ce dommage collatéral des drones. D'ailleurs, il évoque aussi, enfin, sans y donner suite, la liberté d'aller et venir qu'il vient de renforcer dans le même contexte pandémique (CE, ord., 30 avr. 2020, n° 440179, *Fédération française des usagers de la bicyclette*, AJDA 2020. 919). « Comme l'a souligné avec justesse la CNIL (Rapp. d'activité 2003, Doc. fr., p. 135.), l'anonymat est une condition nécessaire à la liberté d'aller et de venir. Si une personne est, à la faveur de ses déplacements, géolocalisable et identifiable à chaque instant, il n'est plus de liberté » (R. Hanicotte, préc.).

Ce dernier point permet de confirmer les risques d'une attractivité excessive de la notion européenne de donnée personnelle, déjà suffisamment large sans que l'on prenne le risque, sur le terrain du maintien de l'ordre, d'en étendre encore les contours. Pour paraphraser Benjamin

Constant (*Principes du politique*) parlant de la Constitution, faire de tout de la donnée personnelle, c'est faire de tout des dangers pour elle et pour d'autres droits.

---

(1) Je remercie le professeur Olivier Le Bot de son aimable relecture. Le contenu de cette note m'est néanmoins exclusivement imputable.