GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

01673/15/FR
WP 231

Avis 01/2015 sur les questions de protection des données et de la vie privée liées à l'utilisation de drones

Adopté le 16 juin 2015

LE GROUPE DE TRAVAIL SUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

institué par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995,

vu les articles 29 et 30 de ladite directive,

vu son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

Synthèse

Compte tenu de l'intégration progressive des drones dans l'espace aérien civil européen et de la multiplication des applications des drones (activités de loisir, services, photographie, logistique, surveillance d'infrastructures, etc.), il est réellement indispensable d'étudier de manière approfondie les problèmes qu'un déploiement à grande échelle de la technologie des drones et des capteurs pourrait poser en ce qui concerne la vie privée et les libertés civiles et politiques individuelles, et d'examiner les mesures nécessaires pour garantir le respect des droits fondamentaux et la protection des données.

En effet, le traitement de données (comme les images, les sons et les données de géolocalisation ayant trait à une personne physique identifiée ou identifiable) effectué par l'équipement à bord d'un drone peut être à l'origine de menaces pour la vie privée. Il peut notamment s'agir d'un manque de transparence quant aux types de traitement, en raison de la difficulté de voir les drones depuis le sol ou, en tout état de cause, de savoir quel équipement de traitement de données est à bord, quelle est la finalité poursuivie par la collecte de données à caractère personnel et qui en est le responsable. En outre, l'agilité des drones et la possibilité de les interconnecter les rendent d'autant plus susceptibles d'occuper des points d'observation privilégiés, en raison, par exemple, de leur capacité d'éviter les obstacles ou les barrières, les murs ou les clôtures. Ils peuvent, de ce fait, recueillir facilement des informations très diverses sans même avoir besoin d'une ligne de visée directe, et ce pendant de longues périodes, sur des zones étendues et sans interruption (ce qui implique un risque de collecte de données massives et d'éventuelles utilisations à différentes fins illicites).

Les menaces qui pèsent sur les droits et libertés des individus sont encore plus importantes lorsque le traitement de données à caractère personnel au moyen de drones poursuit des fins répressives.

Afin de répondre comme il se doit à ces préoccupations, le présent avis formule, une fois sa portée définie compte tenu des exemptions prévues par la directive 95/46/CE (l'exemption relative aux activités domestiques, le traitement à des fins de journalisme ou à des fins répressives), des orientations permettant de traiter correctement les aspects liés aux règles en matière de protection des données en ce qui concerne les drones.

Vérifier la nécessité d'obtenir une autorisation particulière délivrée par les autorités de l'aviation civile lorsque la législation nationale permet l'utilisation de drones, définir les critères les plus appropriés pour un traitement légitime, veiller au respect des principes de limitation de la finalité, de minimisation des données et de proportionnalité (en choisissant la technologie et les mesures les plus proportionnées afin d'éviter la collecte de données à caractère personnel inutiles) ainsi que du principe de transparence, de la manière la plus appropriée au regard des circonstances (en informant les personnes concernées du traitement effectué), sont autant d'obligations auxquelles il conviendrait de satisfaire avant d'utiliser un drone. De même, il convient de prendre toutes les mesures de sécurité appropriées et de supprimer ou d'anonymiser les données à caractère personnel qui ne sont pas strictement nécessaires.

Par ailleurs, le groupe de travail «Article 29» (ci-après, le «groupe de travail») recommande d'adopter les mesures de respect de la vie privée dès la conception et par défaut. Il considère que l'analyse d'impact sur la protection des données est un outil approprié pour évaluer les incidences de l'utilisation de la technologie des drones sur le droit à la vie privée et la protection des données. En outre, pour sensibiliser les utilisateurs, il est particulièrement recommandé aux fabricants de drones de fournir, dans l'emballage (par exemple, dans le mode d'emploi), des informations suffisantes sur le caractère potentiellement intrusif de ces technologies et, si possible, des cartes indiquant clairement où l'utilisation des drones est permise.

Par ailleurs, le présent avis formule notamment des recommandations à l'intention des décideurs politiques européens et nationaux concernant le renforcement d'un cadre qui garantisse le respect de tous les droits fondamentaux en jeu, et pas uniquement la protection des données, en instaurant également des règles spécifiques garantissant un usage responsable des drones (lesquelles doivent nécessairement inclure le respect des espaces privés). En outre, le groupe de travail appelle les décideurs politiques à intégrer les aspects de la protection des données parmi les caractéristiques essentielles des dispositions nationales qui régissent l'usage commercial des drones (concernant la qualification et la formation des pilotes, les exigences d'aptitude au vol et de certification, tout en délivrant/révoquant des licences d'exploitation et des permis de travail aérien), et à encourager une coopération rigoureuse entre les autorités chargées de la protection des données et les autorités de l'aviation civile.

Le groupe de travail recommande également aux fabricants et aux opérateurs d'intégrer des choix et des paramètres par défaut respectueux de la vie privée dans le cadre d'une approche du respect de la vie privée dès la conception, d'associer un délégué à la protection des données (lorsque c'est possible) à la conception et à la mise en œuvre de politiques liées à l'utilisation de drones et de favoriser l'adoption de codes de conduite pouvant aider les différents acteurs et opérateurs de l'industrie à prévenir les infractions et à améliorer l'acceptabilité sociale des drones. Des recommandations spéciales sont également formulées en ce qui concerne l'utilisation à des fins répressives des données à caractère personnel collectées au moyen de drones. En particulier, dans le cadre d'un traitement des données exécuté au moyen de drones à des fins répressives, le suivi constant devrait, généralement, être impossible et l'équipement technique et de captage utilisé devrait correspondre à la finalité du traitement.

1. Introduction

Afin de permettre l'intégration progressive des systèmes d'aéronefs télépilotés (ci-après «RPAS» pour *Remotely Piloted Aircraft Systems*)[1] dans l'espace aérien civil[2], la Commission européenne a adopté la communication COM(2014) 207 intitulée «Une nouvelle ère de l'aviation – Ouvrir le marché de l'aviation à l'utilisation civile de systèmes d'aéronefs télépilotés, d'une manière sûre et durable», qui fait suite à la demande du secteur manufacturier et du secteur des services d'éliminer les entraves à l'introduction des drones à usage civil sur le marché unique européen[3].

L'ouverture du marché des drones nécessiterait la mise en place d'un cadre réglementaire approprié par l'adoption, lorsque c'est nécessaire, de politiques nationales et de normes européennes communes, qui devraient être élaborées par l'Agence européenne de la sécurité aérienne (AESA). Le groupe de travail relève, à cet égard, l'absence de cadre réglementaire approprié dans la plupart des États membres. Dans ce contexte, il convient d'encourager l'harmonisation et la modernisation des politiques des États membres en matière d'aviation en ce qui concerne les drones.

Le groupe de travail reconnaît les avantages sociaux et économiques que l'utilisation civile des drones présente, ainsi que les possibilités qu'elle offre pour la croissance et l'emploi, mais il estime qu'il est tout aussi important de mettre en évidence toutes les menaces et tous les risques qu'un déploiement à grande échelle de la technologie des drones fait peser sur la protection des données et la vie privée, et d'évaluer les mesures nécessaires pour garantir le respect de tous les autres droits fondamentaux en jeu[4].

En effet, le traitement de données à caractère personnel par les drones est de nature particulière en raison du point de vue unique qui accroît l'efficacité des capteurs embarqués et implique une moindre transparence et une plus grande intrusion dans la vie privée par rapport à des capteurs fixes similaires, et ce malgré les apparentes analogies. Il suffit de penser, par exemple, à la vidéosurveillance au moyen de drones par rapport à l'utilisation d'une caméra vidéo fixe.

L'intégration des drones sur le marché européen de l'aviation et leurs différents usages civils (notamment à des fins répressives) soulèveront des problèmes particuliers qu'il conviendra de résoudre afin de «*respecter les droits et principes consacrés par la charte des droits fondamentaux de l'UE, et plus précisément le droit au respect de la vie privée et familiale (article 7) et à la protection des données à caractère personnel (article 8)*»[5]. Dans cette perspective, la participation des législateurs au débat sur l'intégration des drones dans l'espace aérien civil sera indispensable.

---

[1] Les systèmes d'aéronefs télépilotés sont une sous-catégorie de véhicules aériens sans pilote, connus sous le nom de «drones». Dans le glossaire de sa circulaire 328 [«Unmanned Aircraft Systems (UAS), numéro d'ordre: CIR328, 2011], l'OACI définit le RPAS comme «un aéronef dont le pilote aux commandes n'est pas à bord». Par souci de simplicité, le terme «drone» sera utilisé tout au long du présent avis comme terme générique pour renvoyer à ces systèmes.

[2] Voir les conclusions du Conseil européen des 19 et 20 décembre 2013, Euco 217/13.

[3] Il convient de rappeler qu'un processus similaire est en cours aux États-Unis. Pour un aperçu actualisé des différentes mesures prises dans ce domaine par l'administration fédérale de l'aviation (FAA, Federal Aviation Administration), voir le site https://www.faa.gov/uas/.

[4] Tels que la dignité humaine, le droit à la liberté et à la sécurité, la liberté de pensée, de conscience et de religion, la liberté d'expression et d'information, la liberté de réunion et d'association, et le droit à la non-discrimination.

[5] Commission européenne, document de travail des services de la Commission européenne, «Towards a European strategy for the development of civil applications of Remotely Piloted Aircraft Systems (RPAS)», SWD(2012) 259 final, 4 septembre 2012, p. 21. Pour une reconnaissance de la nécessité d'une «évaluation générale des menaces qui pèsent sur la vie privée» liées à l'utilisation de drones, voir également le document du groupe de pilotage européen des RPAS «Roadmap for the safe integration of civil RPAS into the European aviation system», 20 juin 2013, et son annexe 3 intitulée «A Study on the Societal Impact», p. 28. Les aspects que présente l'utilisation des drones concernant la vie privée ont également été pris en considération dans l'avis récent sur l'éthique des

Trouver un équilibre entre les droits et intérêts en jeu représentera un défi que les décideurs politiques devront relever pour faire en sorte que l'Europe puisse être à l'avant-garde de ce nouveau secteur, sans oublier que «*l'Union se fonde sur les valeurs indivisibles et universelles de dignité humaine, de liberté, d'égalité et de solidarité*, *[et qu'elle] repose sur le principe de la démocratie et le principe de l'État de droit*»[6].

Le présent avis fait suite à la demande formulée par la Commission européenne[7] en vue de fournir des indications pratiques aux législateurs et autorités de régulation (aussi bien à l'échelon européen qu'à l'échelon national, y compris aux autorités de l'aviation civile[8]), aux entreprises, aux responsables politiques et au grand public. Les incidences sur la vie privée et la protection des données, ainsi que les conséquences d'un recours étendu aux différentes applications des drones pour tous les usages civils, sont notamment abordées. Y sont examinés les particularités et points critiques relatifs au respect d'exigences spécifiques au titre du cadre juridique actuel sur la protection des données. Pour conclure, le groupe de travail formule des recommandations sur la manière de réagir correctement aux risques que peuvent présenter les drones et leurs usages, afin de rendre le traitement de données à caractère personnel licite et conforme au cadre juridique régissant la protection des données.

2. Description du phénomène et de ses incidences sur la protection de la vie privée et des données

2.1 Définition, caractéristiques et applications potentielles des drones

Selon l'Organisation de l'aviation civile internationale (OACI), un système d'aéronef télépiloté (ici dénommé «drone»), est un «*ensemble d'éléments configurables composé d'un aéronef télépiloté, de sa/ses station(s) de télépilotage, des liaisons de commande et de contrôle requises et de tout autre élément du système susceptible d'être nécessaire à tout moment pendant les opérations aériennes*»[9].

De manière générale, les drones sont des véhicules aériens qui peuvent entrer dans différentes catégories et présentent une grande variété de spécifications, de caractéristiques et de fonctionnalités[10]. Les drones peuvent être conçus pour supporter une série de charges utiles dont la taille et les capacités techniques sont variables. Le modèle de drone le plus basique, composé uniquement doté de ses éléments vitaux[11], ne permettra peut-être pas de traiter de données à caractère personnel, mais il pourra tout de même provoquer une gêne et un trouble social pour

---

technologies de sécurité et de surveillance, présenté à la Commission européenne par le groupe européen d'éthique des sciences et des nouvelles technologies le 20 mai 2014.

[6] Charte des droits fondamentaux de l'Union européenne, préambule.

[7] Le 6 mai 2014, la DG Entreprises et industrie de la Commission européenne a adressé un courrier au groupe de travail «Article 29» par lequel elle invitait les autorités chargées de la protection des données (DPA) à publier des «*recommandations sur la manière de s'atteler aux problèmes liés à la protection de la vie privée et des données au niveau européen, en indiquant les actions à entreprendre pour appuyer l'instauration d'un cadre approprié*».

[8] Les règles de sécurité relatives aux grands RPAS (> 150 kg) relèvent de la compétence de l'AESA, tandis que la réglementation relative aux RPAS légers (< 150 kg) relève de la compétence des autorités nationales de l'aviation civile [voir l'article 4, paragraphe 4, et l'annexe II du règlement (CE) nº 216/2008].

[9] OACI, «Unmanned Aircraft Systems (UAS)», numéro d'ordre: CIR328, 2011, glossaire.

[10] Leurs dimensions peuvent aller de quelques centimètres à plusieurs mètres et leur domaine de vol peut également varier, depuis le vol au ralenti et les possibilités de vol stationnaire, comme pour de nombreux aéronefs à voilure tournante, jusqu'aux opérations à haute vitesse ou à haute altitude, comme dans le cas des aéronefs à hautes performances. La commande des drones par télépilotage repose généralement sur plusieurs liaisons de données et de commande assurées par des équipements radio ou des liaisons de données établies par l'internet via des liens d'accès sans fil numériques, tandis que les pilotes opèrent à distance à partir du sol (ou à bord d'un autre véhicule), souvent dans la ligne de visée. Pour les opérations hors de la ligne de visée, il est absolument nécessaire d'utiliser un système de navigation, reposant sur des systèmes de positionnement comme le GPS, et des dispositifs de télémesure, parfois enrichis d'images en temps réel transmises par des caméras embarquées, pour que le pilote connaisse la situation de l'appareil pendant le vol.

[11] Comme le châssis, les moteurs, les rotors, la batterie, le récepteur et le contrôleur de vol.

autrui. L'ajout de capteurs à d'autres fins, comme l'enregistrement de données audio ou vidéo, suscite évidemment des préoccupations en matière de protection des données et de vie privée. Il importe toutefois de rappeler que les drones disponibles dans le commerce ne sont pas nécessairement équipés de caméras embarquées ou d'autres capteurs par défaut et il dépend de l'utilisateur du drone que celui-ci comporte de telles fonctionnalités, selon le type d'usage prévu. Il se peut également que l'utilisateur conçoive et construise lui-même un drone en se procurant les composants auprès divers fournisseurs.

Parmi les équipements qui pourraient avoir une incidence sur la vie privée et la protection des données figurent:

- les équipements de prises de vue, comme les caméras intelligentes à distance focale fixe ou variable, capables d'enregistrer et de transmettre des images en temps réel, avec des possibilités de reconnaissance faciale, embarquées ou au sol, qui permettent aux drones d'identifier et de suivre certains individus, objets ou situations, de déterminer des modes de déplacement, de lire des plaques d'immatriculation sur les véhicules, tout en offrant une vue à 360°, de détecter l'énergie thermique dégagée par une cible, mais aussi de voler et d'enregistrer des images dans de mauvaises conditions de visibilité (dues au brouillard, à de la fumée ou à des débris) ou pendant la nuit;
- les équipements de détection, comme les capteurs optoélectroniques, les détecteurs d'horizon en infrarouge, les radars à ouverture synthétique pour identifier des objets, des véhicules et des navires et obtenir des informations sur leur position et leur trajectoire, même derrière des murs, de la fumée ou d'autres obstacles;
- les équipements à radiofréquences, comme les antennes qui captent la localisation de points d'accès Wi-Fi ou de stations cellulaires, les femtocellules et les «attrapeurs d'IMSI» utilisés par les autorités répressives pour contrôler les téléphones cellulaires et les réseaux, ou par les prestataires de services pour relayer les communications entre les réseaux et utilisateurs de terminaux;
- les capteurs spéciaux pour la détection de traces de substances nucléaires, biologiques ou chimiques ou d'engins explosifs.

Par ailleurs, les possibilités que les drones offrent d'être modifiés et adaptés à des situations précises et leur coût relativement faible font qu'ils sont utilisés dans une série de situations nouvelles[12]. En tout état de cause, il convient cependant de préciser que le point important, relativement à la vie privée et à la protection des données, n'est pas l'utilisation des drones en soi mais l'équipement de traitement de données à bord du drone et le traitement ultérieur de données à caractère personnel qui peut être réalisé. En effet, c'est le traitement d'images (notamment les images de personnes, de maisons, de véhicules, de plaques d'immatriculation, etc.), de sons, de données de géolocalisation ou d'autres signaux électromagnétiques liés à une personne physique identifiée ou identifiable, exécuté par l'équipement de traitement de données à bord d'un drone qui peut avoir une incidence sur la vie privée et la protection des données et, dès lors, justifier l'application de la législation en matière de protection des données[13].

---

[12] Leur déploiement dans des opérations «3D» (*dull, dirty or dangerous*, c'est-à-dire dans le cadre de missions monotones, sales ou dangereuses) est extrêmement intéressant du point de vue de la santé et de la sécurité car l'opérateur humain peut rester à distance du site présentant un danger. Ainsi, les drones peuvent être utilisés pour les tâches habituelles du travail aérien que sont la surveillance, la reconnaissance, les recherches et le sauvetage, la surveillance de l'environnement, l'agriculture, de même que dans d'autres domaines liés aux loisirs et au sport, au journalisme et à l'actualité, aux missions documentaires, logistiques et de transport, à la construction et aux travaux publics, à la surveillance et à l'entretien de réseaux et d'infrastructures, ainsi qu'à des fins répressives.

[13] Voir à cet égard la définition des «données à caractère personnel» et du «traitement des données» qui figurent à l'article 2, points a) et b), de la directive 95/46/CE. Il convient de souligner que la collecte de données sans enregistrement ou stockage constitue

2.2 Risques pour la protection des données

Compte tenu de toutes les applications existantes et de celles qui feront bientôt leur apparition, plusieurs risques ont déjà été mis en évidence en matière de sécurité, de responsabilité des tiers et de vie privée[14]. En effet, concernant ce dernier aspect, il est probable que, dans nombre de cas, les personnes concernées ne s'apercevront pas de la présence du drone ou du traitement de leurs données à caractère personnel étant donné qu'il n'est pas toujours facile de repérer ces engins depuis le sol. En tout état de cause, même si on s'aperçoit qu'un drone survole la région, il est difficile de savoir quel équipement de traitement de données est embarqué, à quelles fins ces données sont collectées et par qui. Il s'ensuivra une impression accrue d'être sous surveillance et, éventuellement, une diminution de l'exercice légitime des libertés et droits civils, phénomène mieux connu sous le nom d'«effet intimidant»[15].

La maniabilité des drones accroît en outre leur capacité à offrir des points de vue exceptionnels, par exemple en évitant les obstacles ou en se jouant des barrières, murs ou clôtures. Les drones peuvent donc pénétrer plus facilement dans les lieux privés de façon à recueillir aisément une grande variété d'informations à partir de différentes sources. En fonction des technologies embarquées, il serait possible de collecter des données sans qu'il soit nécessaire d'avoir une ligne de visée directe (c'est-à-dire à travers les toits, les débris ou les nuages), pendant de longues périodes, sur des zones étendues et sans interruption (ce qui implique un risque élevé de collecte massive de données et d'éventuelles utilisations à fins illicites diverses).

Il convient également de tenir compte de la possibilité de relier entre eux plusieurs drones afin de surveiller une zone étendue. Les essaims de drones, dotés de canaux de communication en temps réel entre eux et des éléments externes, présentent des risques encore plus grands pour la protection des données car ils pourraient aisément permettre une surveillance coordonnée, c'est-à-dire de suivre les déplacements de personnes ou de véhicules sur de grandes étendues.

Il y a donc un risque important que le traitement de données à caractère personnel par les drones entre dans la clandestinité et soit à l'origine d'ingérences graves dans les sphères personnelles les plus intimes. Parallèlement, compte tenu de la potentielle sophistication de l'équipement embarqué et de la facilité avec laquelle les données à caractère personnel collectées peuvent être associées à d'autres informations, il y a un risque indéniablement plus élevé de détournement d'usage (c'est-à-dire de changement ou d'extension de l'usage à des fins irrégulières).

Par ailleurs, l'incidence potentielle de l'intrusion dans la vie privée est accrue par la diversité des parties et entités concernées par l'utilisation des drones. Les fabricants de drones, par exemple, ont également un rôle à jouer dès la phase de conception puisque les caractéristiques opérationnelles peuvent, dans une plus ou moins grande mesure, servir à des applications intrusives au niveau de la

---

néanmoins une opération de traitement qui entraîne l'application de la législation en matière de protection des données et que «*l'identification peut être le résultat, dans les limites imposées par la directive, d'un appariement de données avec des informations gardées par des tiers, ou bien de l'utilisation, dans le cas en question, de techniques particulières ou de dispositifs spéciaux*» (groupe de travail «Article 29» sur la protection des données, avis 04/2004 sur le traitement des données à caractère personnel au moyen de la vidéo-surveillance, WP 89, p. 13). Pour des orientations approfondies sur l'interprétation à donner à la notion de données à caractère personnel, voir l'avis 04/2007 sur le concept de données à caractère personnel du groupe de travail «Article 29» sur la protection des données, WP 136.

[14] Voir, entre autres, «A Study on the Societal Impact», en annexe à «Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System», passim.

[15] Concernant le syndrome d'effet intimidant et de panoptique résultant d'une utilisation des drones à grande échelle, voir Rachel L. Finn, David Wright et Anna Donovan (Trilateral Research & Consulting, LLP), Laura Jacques et Paul De Hert (Vrije Universiteit Brussel), «Privacy, data protection and ethical risks in civil RPAS operations», 7 novembre 2014, à l'adresse http://ec.europa.eu/DocsRoom/documents/8550?locale=fr, p. 28 et suiv., et ailleurs.

vie privée (par exemple, dans le cas de drones de petite taille ou de microdrones capables de voler à l'intérieur de bâtiments).

La perception que le public a des drones est indissociable de leur viabilité sociale. À cet égard, l'application effective de la législation en matière de protection des données peut contribuer à l'acceptation des drones. Par conséquent, le groupe de travail encourage les initiatives et les projets de sensibilisation qui accompagnent l'introduction des drones sur le marché civil de l'Union européenne.

3. Analyse juridique

Bien que les États membres ne disposent pas de législation spécifique sur les conséquences de l'utilisation des drones en matière de protection des données, le cadre juridique applicable est constitué de la directive 95/46/CE relative à la protection des données (ci-après, la «directive») et, dans la mesure où les drones peuvent également être utilisés par les prestataires de services de communication électronique accessibles au public (par exemple, pour étendre la portée de ces services), la directive 2002/58/CE, telle que modifiée par la directive 2009/136/CE.

En outre, même si les incidences que l'utilisation de drones peut avoir sur la vie privée et la liberté individuelle diffèrent de celles des systèmes de caméras de vidéosurveillance, dans certaines circonstances, les dispositions juridiques nationales applicables aux systèmes de caméras de vidéosurveillance pourraient également s'appliquer à l'utilisation de drones, notamment s'agissant de drones utilisés à des fins de vidéosurveillance. Dans ce contexte, le groupe de travail souhaite renvoyer à son avis sur le traitement des données à caractère personnel au moyen de la vidéosurveillance, en insistant sur l'actualité de l'analyse juridique et des recommandations qu'il contient[16].

Cependant, en raison des particularités et des risques susmentionnés concernant les applications des drones, le groupe de travail estime qu'il importe de fournir des orientations spécifiques sur la manière de se conformer aux règles en matière de protection des données dans ce contexte.

Le cadre étant établi, il convient de se montrer très attentif à la question de la responsabilité du traitement, tout particulièrement eu égard à la vaste gamme de services reposant sur l'utilisation de drones qui sont déjà proposés aux organisations publiques et privées par des entreprises spécialisées. À ce titre, il est de la plus haute importance que le responsable du traitement et le sous-traitant soient clairement identifiés pour chaque type d'opérations à l'aide de drones, notamment par une évaluation des éléments essentiels permettant de distinguer le responsable du traitement des autres acteurs[17]. Des orientations claires pour déterminer les différentes combinaisons de responsabilités entre les différentes entités participant à un traitement conjoint sont disponibles dans l'avis 01/2010 du groupe de travail sur les notions de «responsable du traitement» et de «sous-traitant»[18].

---

[16] Groupe de travail «Article 29» sur la protection des données, avis 04/2004 sur le traitement des données à caractère personnel au moyen de la vidéosurveillance, id.

[17] Le responsable du traitement «détermine les finalités et les moyens du traitement de données à caractère personnel» [article 2, point d), de la directive]. On entend par «sous-traitant» la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement [article 2, point e), de la directive]. Par exemple, ce rôle pourrait être facile à définir lorsque le drone est utilisé directement par une société qui l'a acheté pour la livraison de colis (responsable du traitement), mais on pourrait envisager un cadre différent dans le cas d'une société qui engage un opérateur de drone afin de cartographier une zone (auquel cas la société est le responsable du traitement et l'opérateur est le sous-traitant).

[18] Groupe de travail «Article 29» sur la protection des données, avis 01/2010 sur les notions de «responsable du traitement» et de «sous-traitant», WP 169.

3.1 Applicabilité de la directive sur la protection des données

Bien que la Commission européenne se concentre sur les drones aériens télépilotés, le présent avis ne distingue pas les systèmes d'aéronefs sans pilote entièrement autonomes des systèmes sans pilote non autonomes, étant donné que cet aspect n'est pas pertinent au regard des problèmes que l'utilisation de cette technologie pose pour la protection des données. En outre, les lignes directrices devraient s'appliquer, moyennant les adaptations nécessaires, au traitement des données qui résulte de l'utilisation de n'importe quel véhicule aérien (avec ou sans pilote, aéronautique ou spatial) pour des opérations civiles.

Cependant, il convient de souligner que certains exemples de traitement de données à caractère personnel découlant de l'utilisation de drones dans le cadre d'opérations civiles peuvent échapper au champ d'application de ces lignes directrices eu égard aux exemptions ou dérogations que les États membres peuvent prévoir en vertu de la directive (voir notamment les articles 3, 9 et 13).

Conformément à l'article 3, paragraphe 2, de la directive, le traitement de données à caractère personnel effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques n'entre pas dans le champ du présent avis.

Néanmoins, la disposition de l'article 3, paragraphe 2, est une exception et, en tant que telle, elle est d'interprétation stricte. Dès lors, la Cour de justice a considéré que ladite «exemption relative aux activités domestiques» doit «*être interprétée comme visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes*»[19]. En outre, si l'utilisation d'un drone et l'équipement embarqué sont de nature à créer un système de vidéosurveillance, dans la mesure où il implique l'enregistrement et le stockage constants de données à caractère personnel et couvre «*même partiellement, [...] l'espace public et, de ce fait, est [dirigé] vers l'extérieur de la sphère privée de celui qui procède au traitement des données par ce moyen, [il] ne saurait être [considéré] comme une activité exclusivement «personnelle ou domestique», au sens de l'article 3, paragraphe 2, second tiret, de la directive 95/46*»[20].

Par ailleurs, aux termes de l'article 9 de la directive sur la protection des données, les États membres peuvent prévoir des exemptions et dérogations à certaines dispositions de la directive[21], pour les traitements de données à caractère personnel effectués aux seules fins de journalisme ou d'expression artistique ou littéraire[22]. Cependant, ces exemptions et dérogations ne sont possibles

---

[19] Cour de justice de l'Union européenne, arrêt du 6 novembre 2003 dans l'affaire C-101/01, Bodil Lindqvist, point 47.

[20] Cour de justice de l'Union européenne, arrêt du 11 décembre 2014 dans l'affaire C-212/13, František Ryneš/Úřad pro ochranu osobních údajů, point 33. Voir la suite du présent document pour les exigences que cette application entraînera en ce qui concerne la licéité, la proportionnalité, la transparence, les mesures de sécurité, etc., compte tenu du fait que, comme la Cour de justice l'a rappelé, «*l'application des dispositions de cette directive permet, le cas échéant, de tenir compte, conformément en particulier aux articles 7, sous f), 11, paragraphe 2, ainsi que 13, paragraphe 1, sous d) et g), de ladite directive, des intérêts légitimes du responsable du traitement, consistant notamment, comme dans l'affaire au principal, à protéger les biens, la santé et la vie de ce responsable ainsi que ceux de sa famille*».

[21] En particulier, celles relatives aux règles générales concernant la licéité du traitement, les règles sur les transferts aux pays tiers et les règles sur l'autorité de contrôle et le groupe de travail (article 6, paragraphe 1, article 10, article 11, paragraphe 1, et articles 12 et 21 de la directive).

[22] Des activités peuvent être qualifiées d'activités de journalisme si elles ont pour «finalité la divulgation au public d'informations, d'opinions ou d'idées, sous quelque moyen de transmission que ce soit. Elles ne sont pas réservées aux entreprises de média et peuvent être liées à un but lucratif» (arrêt de la Cour de justice du 16 décembre 2008 dans l'affaire C-73/07, Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy et Satamedia Oy, point 61). De même, la Cour européenne des droits de l'homme a jugé que «[l]'ouverture d'espaces de débat public fait partie du rôle de la presse. Cependant, l'exercice de cette mission n'est pas limité aux médias ou aux journalistes professionnels» (voir arrêt de la Cour européenne des droits de l'homme du 14 avril 2009 dans l'affaire Társaság a Szabadságjogokért c. Hongrie, point 27).

que «*dans la seule mesure où elles s'avèrent nécessaires pour concilier le droit à la vie privée avec les règles régissant la liberté d'expression*».

Le traitement de données à caractère personnel effectué au moyen de drones aux fins d'activités de journalisme devrait dès lors tenir compte des différentes législations et dispositions nationales applicables à ce type de traitement. Cependant, les États membres devraient être conscients du caractère potentiellement intrusif de ces instruments, surtout s'ils sont utilisés de manière irresponsable et contraire à l'éthique. Les États membres devraient également recenser clairement les devoirs et responsabilités que comporte l'exercice de la liberté d'expression au moyen de drones.

Le groupe de travail attache la plus haute importance à l'instauration d'un cadre adéquat au niveau national (s'il n'a pas déjà été mis en place) afin que l'utilisation de drones à des fins strictement personnelles et récréatives ou dans le cadre d'activités de journalisme[23] ne porte pas atteinte aux droits fondamentaux à la vie privée ou à la confidentialité des communications, et que le respect d'attentes raisonnables de protection de la vie privée, même dans les cas d'une collecte de données à caractère personnel effectuée dans des lieux publics, puisse être garanti. Comme la Cour européenne des droits de l'homme l'a rappelé, il existe «*une zone d'interaction entre l'individu et des tiers qui, même dans un contexte public, peut relever de la vie privée*»[24]. Par conséquent, les principes généraux et certaines suggestions particulières formulées dans le présent avis devraient également être pris en considération par les législateurs et les organismes de réglementation (à l'échelle nationale et européenne) lorsqu'ils établissent les exigences à respecter pour l'utilisation de modèles réduits d'aéronefs[25], ainsi que par le grand public, afin d'éviter d'enfreindre la législation en matière de protection des données et les autres dispositions législatives nationales qui préservent d'autres droits personnels[26].

3.2 Traitement de données à caractère personnel à des fins répressives

Les drones peuvent annoncer une transformation fondamentale des pratiques répressives, tout particulièrement en ce qui concerne le rôle des données dans l'orientation des actions répressives, allant de la surveillance d'une personne à la détermination de cibles à partir de l'examen de la vie et des activités d'une population donnée sur la base d'une surveillance continue. Ainsi, l'utilisation de drones exploités directement par la police et d'autres autorités répressives – ou leur demande d'accès aux données collectées par des drones exploités par des entités privées à leurs propres fins –

---

[23] À cet égard, l'adoption d'un code de conduite pour les activités de journalisme pourrait, par exemple, être conseillée afin de résoudre ce problème en tenant compte de tous les intérêts en jeu.

[24] Arrêt de la Cour européenne des droits de l'homme du 7 février 2012 dans l'affaire Von Hannover c. Allemagne (nº 2), point 95. Par analogie, voir Contrôleur européen de la protection des données, avis sur la communication «Une nouvelle ère de l'aviation. Ouvrir le marché de l'aviation à l'utilisation civile de systèmes d'aéronefs télépilotés, d'une manière sûre et durable», 26 novembre 2014, p. 7. En équilibrant minutieusement les différents intérêts en jeu, les États membres – qui sont tous parties à la Convention européenne des droits de l'homme (CEDH) – satisferaient également à l'obligation positive d'assurer le respect effectif du droit à la vie privée et familiale qui découle de l'article 8 de la Convention (voir Cour européenne des droits de l'homme, arrêt du 9 octobre 1979 dans l'affaire Airey c. Irlande, point 32; arrêt du 13 juin 1979 dans l'affaire Marckx, point 31).

[25] La circulaire 328 de l'OACI, précitée, rappelle (au point 2.4) que les modèles réduits d'aéronefs échappent aux dispositions de la convention de Chicago, mais pourraient faire l'objet de réglementations nationales pertinentes. Dans ce contexte, l'instauration de règles précises garantissant une utilisation responsable des drones pourrait être envisagée. Ces règles doivent nécessairement assurer le respect des espaces privés (tels que les jardins, les cours, les terrasses, etc.) et des «attentes raisonnables» en matière de vie privée dans les espaces publics. À cet effet, la création de périmètres virtuels pourrait être envisagée si nécessaire. À cet égard, voir par exemple le règlement italien sur les véhicules aériens télépilotés (article 23).

[26] La distribution d'une notice accompagnant le modèle réduit d'aéronef, par exemple, pourrait être utile pour attirer l'attention sur le respect nécessaire du principe de protection de la vie privée, le cas échéant, et d'autres dispositions législatives nationales. Un exemple intéressant de notice sur l'utilisation des drones à des fins personnelles («Règles d'un bon usage d'un drone de loisir») est disponible sur le site http://www.developpement-durable.gouv.fr/IMG/pdf/Drone-_Notice_securite-2.pdf. Voir également, à cet égard, la liste des choses à faire et à ne pas faire pour les modèles réduits d'aéronefs publiée aux États-Unis par la FAA sur le site http://www.faa.gov/uas/publications/model_aircraft_operators.

engendre des risques importants pour les droits et libertés individuels et interfère directement avec les droits au respect de la vie privée et à la protection des données à caractère personnel énoncés à l'article 8 de la CEDH et aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte»).

Par conséquent, en application de l'article 52, paragraphe 1, de la charte et de l'article 8, paragraphe 2, de la CEDH, cette limitation de l'exercice des droits et libertés reconnus par la charte doit être prévue par la loi («conformément à la loi»), ne peut être apportée que si elle est nécessaire et répond effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui («dans la poursuite d'une des finalités légitimes énoncées à l'article 8, paragraphe 2, de la CEDH et nécessaire dans une société démocratique»).

Ainsi, la police et les autres autorités répressives utilisant des drones doivent veiller à disposer d'une base juridique valable pour le traitement de données à caractère personnel.

Les drones ne doivent être utilisés que si leur nécessité et leur caractère approprié eu égard aux finalités spécifiques poursuivies sont démontrés concrètement. Dans ce contexte, le groupe de travail attire l'attention sur son avis 01/2014 sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif.

Il appartient aux autorités précitées de justifier pourquoi les instruments à leur disposition et d'autres solutions moins intrusives ne permettraient pas d'atteindre cet objectif (et une évaluation préalable par les autorités chargées de la protection des données peut s'appliquer et être envisagée à cette fin lorsque les pratiques nationales privilégient cette évaluation préalable).

En outre, lorsque les autorités répressives traitent des données collectées par des drones pour la répression de délits civils, elles doivent respecter les exigences établies par la directive. En particulier, de telles utilisations des drones devraient être limitées aux cas où le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées.

Une fois que la nécessité des drones pour la police ou à des fins répressives est établie, le cas échéant, en application de l'article 52, paragraphe 1, de la charte et de l'article 8 de la CEDH, leur utilisation devrait respecter le principe de proportionnalité et les exigences particulières en matière de protection des données: elle ne devrait pas aller au-delà de ce qui est nécessaire pour atteindre l'objectif légitime poursuivi.

Dans cette perspective, les principes énoncés dans la convention nº 108 du Conseil de l'Europe et la recommandation nº R(87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, adoptée par le Comité des ministres le 17 septembre 1987, devraient être suivis, de même que les principes pertinents de la décision-cadre 977/2008 relative à la protection des données.

Par ailleurs, le groupe de travail rappelle que le traitement de données au moyen de drones par des services publics devrait être effectué pour les finalités énoncées dans la législation applicable et ne devrait pas être utilisé aux fins d'une surveillance arbitraire, du traitement de données en masse, du regroupement de données et du profilage: des limites doivent être imposées à l'utilisation des drones pour les activités de surveillance, afin d'éviter que celles-ci se généralisent ou servent à signaler des cibles sur la base de l'analyse de données. En conséquence, les drones ne devraient être utilisés qu'aux fins strictement énoncées et justifiées qui pourraient être énumérées au préalable et, en tout état de cause, leur utilisation devrait être limitée dans l'espace et dans le temps. Au regard de l'«effet intimidant» que l'utilisation des drones peut produire sur les droits à la liberté d'expression et à la

liberté de réunion, il convient de prêter particulièrement attention à la nécessité de préserver, autant que possible, les manifestations publiques et rassemblements similaires de tout type de surveillance.

3.3 Licéité du traitement et principe de limitation de la finalité

Pour être licite, le traitement de données à caractère personnel résultant de l'application civile de la technologie des drones devrait se fonder sur un des critères de légitimation énoncés à l'article 7 de la directive[27]. Compte tenu de l'avis relatif à l'intérêt légitime, qui fournit des orientations détaillées sur cet aspect[28], et des particularités du traitement des données à caractère personnel effectué au moyen d'équipements à bord de drones, différentes bases juridiques pourraient être considérées comme applicables aux différentes finalités du traitement en jeu:

- le consentement libre, spécifique et informé [article 7, point a)]:
  Certes le consentement est une base juridique commune sur laquelle il convient de se fonder, mais il semble que, dans le présent contexte, il ne pourrait s'avérer approprié que dans quelques cas, en particulier lorsque les données sont collectées dans des espaces publics. Le consentement doit en effet être libre, spécifique et informé. Dans la plupart des cas en question, il serait difficile de satisfaire à toutes ces exigences puisque, par exemple, le consentement ne sera pas «libre» dès lors qu'une personne n'est pas libre de pénétrer dans une zone surveillée ou de la quitter sans être sous surveillance; le consentement ne sera pas «informé» si la personne ne reçoit pas toutes les informations nécessaires sur le traitement; et il ne sera pas non plus «spécifique» s'il est impossible à la personne de déterminer à chaque fois la finalité du traitement auquel il lui est demandé de consentir[29].
  Le consentement pourrait constituer une base juridique appropriée pour le traitement de données à caractère personnel effectué au moyen de caméras à bord d'un drone, par exemple, dans le cas d'une séance d'entraînement d'une équipe de sport (c'est-à-dire sans que des spectateurs soient présents);
- le traitement nécessaire à l'exécution d'un contrat auquel la personne concernée est partie [article 7, point b)]:
  Le traitement de données à caractère personnel est licite en vertu de l'article 7, point b), de la directive par exemple lorsque quelqu'un achète un produit qui est livré à son domicile par un vendeur au moyen d'un drone, ou lorsque des services d'enregistrement vidéo limités aux biens des personnes concernées sont proposés par des sociétés exploitant des drones. Cependant, il faut prendre en compte le fait que le traitement incident de données de tiers non affectés n'est jamais couvert par l'exécution des obligations des parties à un contrat et, dès lors, dans les exemples précités, il faudrait éviter la collecte de données à caractère personnel de tiers ou bien trouver une autre base juridique pour la légitimer;
- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ou à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées [article 7, points c) et e)]:
  Ces bases juridiques pourraient servir dans les cas où l'obligation imposée par la loi doit être remplie par le responsable du traitement, comme la surveillance d'un site archéologique requise par une disposition particulière ou, par exemple, dans le cadre de certains usages «liés à la

---

[27] Cependant, dans tous les cas où l'utilisation de drones pourrait impliquer le traitement de catégories particulières de données, l'article 8 de la directive s'applique.

[28] Voir groupe de travail «Article 29» sur la protection des données, avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, WP 217, p. 16 et suiv.

[29] Voir groupe de travail «Article 29» sur la protection des données, avis 15/2011 sur la définition du consentement, WP 187.

sécurité», comme le contrôle de la contrebande, uniquement lorsque le recours à des drones est strictement nécessaire et proportionné;

- le traitement est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée [article 7, point d)]:
  Cette base juridique pourrait être pertinente pour certains usages «liés à la sécurité» comme les secours en cas de catastrophe, l'inspection d'une scène d'incendie, le sauvetage de victimes d'accidents dus à la neige ou en montagne, etc. Cependant, étant donné que l'article 7, point d), est censé être de stricte interprétation, il se peut qu'envisager ces usages sous l'angle de l'article 7, points c), e) ou f), constitue une meilleure approche en fonction des circonstances de l'espèce[30];
- le traitement est nécessaire à la réalisation de l'intérêt légitime [article 7, point f)]:
  Les données à caractère personnel peuvent également être traitées si cela est nécessaire à la réalisation des intérêts légitimes poursuivis par le responsable du traitement ou par le tiers, sauf si les intérêts de la personne concernée ou ses droits et libertés fondamentales priment sur ces intérêts (il est à prévoir qu'un tel critère puisse être envisagé, par exemple, lorsque l'exploitation d'un drone est nécessaire pour inspecter des tuyaux ou des lignes électriques ou pour la surveillance d'infrastructures critiques ou la photogrammétrie aérienne, la recherche sur l'atmosphère et la recherche météorologique, le suivi de l'énergie éolienne, le suivi des ouragans, la cartographie de sites archéologiques, la surveillance de la glace marine, la recherche sur la faune sauvage)[31], à condition que des garanties appropriées soient mises en œuvre dans le système.

En outre, et compte tenu des risques susmentionnés que présente par la collecte d'une grande quantité de données par des applications de drones et dudit «détournement d'usage», il convient de rappeler que les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités [article 6, paragraphe 1, point b), de la directive][32].

Par conséquent, tout traitement ultérieur de données à caractère personnel pour une finalité différente de celle pour laquelle elles ont été collectées devrait être conforme aux dispositions de la directive et, partant, se fonder sur une base juridique autonome. Il conviendra également d'apprécier au cas par cas sa compatibilité avec la finalité initiale[33].

De plus, conformément au principe de licéité [article 6, paragraphe 1, point a), de la directive], toute utilisation de drone impliquant le traitement de données à caractère personnel devrait, avant toute

---

[30] Voir groupe de travail «Article 29» sur la protection des données, avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE, WP 217, p. 20 et 21.

[31] De précieuses orientations concernant cette base juridique figurent dans l'avis du groupe de travail sur la notion d'intérêt légitime (ibid.). Cependant, vu la gravité potentielle des atteintes à la protection des données et à la vie privée des personnes que provoque l'utilisation de drones, force est de constater, conformément à l'arrêt de la Cour de justice de l'Union européenne dans l'affaire Google Spain, que ce traitement ne saurait être justifié par le seul intérêt économique que le responsable du traitement a dans celui-ci (arrêt de la Cour de justice de l'Union européenne du 13 mai 2014 dans l'affaire C-131/12, Google Spain SL et Google Inc./Agencia Española de Protección de Datos et Mario Costeja González, point 81).

[32] Ainsi, par exemple, il ne devrait pas être possible de continuer d'utiliser les images de terres agricoles, prises afin de vérifier le bon épandage des pesticides, pour enregistrer des données sur les terres voisines ou les techniques utilisées, ni pour filmer une zone en vue de la protéger et d'utiliser les images pour infliger des amendes aux personnes qui n'ont pas payé leur entrée.

[33] Voir groupe de travail «Article 29» sur la protection des données, avis 03/2013 sur la limitation de la finalité, WP 203. Pour un autre exemple significatif d'utilisation incompatible des données à caractère personnel, voir groupe de travail «Article 29» sur la protection des données, avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), WP 128, p. 15. En outre, le respect du principe de limitation de la finalité revêt une importance cruciale, par exemple en cas de mutualisation (voir ci-dessus, point 2.1).

chose, respecter la législation générale applicable[34], y compris les réglementations nationales en matière de vidéosurveillance et d'utilisation de drones[35].

3.4 Principes de proportionnalité, de qualité des données et de minimisation des données: la fonction appropriée du respect de la vie privée dès la conception et par défaut

Comme les données à caractère personnel peuvent être traitées seulement si elles sont adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont collectées, il faudrait effectuer une évaluation rigoureuse de la nécessité et de la proportionnalité des données traitées (article 6 de la directive). Les données à caractère personnel ne peuvent être traitées que si et tant que les finalités ne peuvent être réalisées par le traitement d'informations qui ne comprend pas de données à caractère personnel.

En outre, on pourrait respecter le principe de minimisation des données en choisissant une technologie proportionnée et en adoptant des mesures de protection des données et de respect de la vie privée par défaut, c'est-à-dire en appliquant des paramètres de confidentialité aux services et produits qui, par défaut, devraient éviter la collecte et le traitement ultérieur de données à caractère personnel inutiles[36]. Une charge utile moins intrusive devrait toujours être privilégiée et, le cas échéant, la mise en œuvre de techniques d'anonymisation, tel qu'il est exposé dans l'avis 05/2014 sur les techniques d'anonymisation[37], pourrait par exemple être envisagée chaque fois que le traitement de données à caractère personnel est inutile.

De plus, en ce qui concerne les différentes technologies capables de lire et de traiter électroniquement des données biométriques (reconnaissance faciale, identification du comportement), une analyse actualisée ainsi que des explications et des recommandations utiles figurent dans l'avis du groupe de travail sur l'évolution des technologies biométriques[38]. Par exemple, lorsqu'ils utilisent des drones équipés de caméras vidéo, les responsables du traitement peuvent recourir à des dispositifs techniques pour traiter automatiquement les images en employant le floutage ou d'autres effets visuels, afin d'éviter la collecte d'images de personnes identifiables chaque fois que cela n'est pas nécessaire.

L'application de mesures de protection des données par défaut implique que le principe de protection des données dès la conception soit respecté au préalable par les fabricants et les opérateurs. La protection des données devrait être intégrée dans le cycle de vie complet de la technologie, dès les premières étapes de la conception jusqu'à son déploiement et son utilisation ultime et son élimination finale. Cette technologie devrait être conçue de manière à éviter le traitement de données à caractère personnel inutiles (par exemple, dans le cas d'infrastructures stratégiques ou critiques, on pourrait recommander de concevoir les micrologiciels des drones de

---

[34] La législation en matière de protection des données ainsi que d'autres lois applicables, comprenant les dispositions législatives nationales garantissant les droits personnels, le droit à l'image, la vie de famille et la sphère privée.

[35] Pour ces raisons, dans les États membres où l'utilisation de drones enfreint les règles nationales en matière d'aviation, le traitement de données à caractère personnel collectées pendant les missions sera considéré comme non conforme au principe de licéité.

[36] Par exemple, si les données sont stockées à bord d'un appareil, elles devraient être supprimées dès que c'est raisonnablement possible et conservées par le responsable du traitement en toute sécurité, conformément à des politiques de conservation clairement définies. Le stockage à long terme de données sur un appareil expose inutilement à un risque de perte ou de vol lors d'une mission aérienne ultérieure. Par ailleurs, il n'est a priori pas nécessaire de doter les drones utilisés pour la livraison de colis de caméras permettant la reconnaissance faciale ou de fonctionnalités d'enregistrement audio. Il ne devrait pas être nécessaire qu'un appareil servant à surveiller un toit en cas de dégâts dus aux tempêtes enregistre des images pendant toute la durée du vol, en particulier si l'endroit à surveiller se trouve à une certaine distance du lieu de décollage et d'atterrissage. À cet égard, il pourrait être conseillé d'associer un délégué à la protection des données (lorsque c'est possible) à la conception et la mise en œuvre des politiques relatives à l'utilisation de drones.

[37] Voir groupe de travail «Article 29» sur la protection des données, avis 05/2014 sur les techniques d'anonymisation, WP 216.

[38] Groupe de travail «Article 29» sur la protection des données, avis 03/2012 sur l'évolution des technologies biométriques, WP 193.

manière à empêcher la collecte de données à l'intérieur de zones préalablement définies comme zones d'exclusion aérienne)[39].

Étant donné la variété d'applications des drones, on pourrait réaliser une analyse d'impact relative à la protection des données afin d'évaluer l'incidence de ces applications sur les droits et les libertés individuelles et, en particulier, sur le droit à la vie privée et à la protection des données. Cette analyse permet aux opérateurs de constater les risques pour la vie privée (le cas échéant) associés à l'utilisation de nouvelles applications, d'évaluer si le traitement de données à caractère personnel par des drones est légitime, nécessaire et proportionné à la finalité et d'aborder entre autres les questions relatives à la transparence et à la sécurité, tout en documentant les mesures prises pour maîtriser ces risques[40].

Par conséquent, le groupe de travail invite les décideurs politiques compétents au niveau européen ou national, lorsqu'ils s'attelleront au nouveau cadre juridique pour l'intégration des drones dans l'espace aérien civil européen, à établir s'il convient d'encourager, en tant que bonne pratique et pour chaque type d'opération de drone susceptible d'impliquer le traitement de données à caractère personnel, la réalisation d'une analyse d'impact relative à la protection des données en fonction des risques prévisibles résultant des applications prévues, en fournissant aussi aux parties intéressées (fabricants et opérateurs) un ensemble de critères faciles à utiliser.

En particulier, comme les règles en matière de protection des données devraient être respectées dès lors que des données à caractère personnel sont traitées, il faudrait envisager une analyse d'impact relative à la vie privée et à la protection des données pour les fabricants de drones «conçus et produits» à des fins de surveillance et pour les opérateurs utilisant des drones dotés de tout type d'équipement «audiovisuel», compte tenu – comme il a été dit précédemment – des charges utiles et des finalités que poursuivent la collecte et le traitement ultérieur de données à caractère personnel[41].

Lorsque les drones sont équipés d'un système de reconnaissance d'image, il conviendrait d'envisager l'instauration d'un mécanisme qui facilite l'exercice de l'objection par la personne concernée, sous la forme d'étiquettes actives ou passives qui indiqueraient clairement les intentions des personnes concernées quant au traitement de leur image ou des appareils qu'elles utilisent, comme les étiquettes visuelles actuellement utilisées dans le but d'indiquer aux photographes, lors de conférences publiques, comment l'image des personnes photographiées peut être utilisée[42].

3.5 Transparence et information des personnes concernées

Conformément au principe de traitement loyal [article 6, point a), de la directive], les personnes concernées doivent être informées de la collecte et du traitement de leurs données à caractère personnel. Elles doivent donc être informées conformément à l'article 10 de la directive, sous

---

[39] Des mécanismes visant à garantir que, par défaut, seules seront traitées les données à caractère personnel nécessaires à chaque finalité spécifique du traitement, ces données n'étant, en particulier, pas collectées ou conservées au-delà du minimum nécessaire à ces finalités sont envisagés dans la proposition de règlement du Parlement européen et du Conseil 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, COM(2012) 11 final (voir, à ce sujet, l'article 23).

[40] Pour chaque application de drones, on devrait, avant toute chose, effectuer une évaluation préalable pour déterminer les types de données nécessaires/standard susceptibles d'être collectées. Par exemple, la collecte des seules données relatives au vol d'un drone (telles que l'altitude, la vitesse aérodynamique, la longueur du vol) ne justifie peut-être pas le respect immédiat des obligations en matière de protection des données, sauf si le pilote ou une autre personne est identifiable à l'aide de ces données (par exemple, le nom du pilote ou le numéro d'employé qui serait enregistré dans les métadonnées du journal).

[41] La réalisation d'une analyse d'impact relative à la protection des données est envisagée dans certains cas particuliers par la proposition de règlement du Parlement européen et du Conseil 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, précitée (voir en particulier l'article 33).

[42] Le mécanisme utilisant des étiquettes signalant le consentement des personnes concernées quant à l'utilisation et à la publication de leur image a été décrit dans le projet «Offlinetags» (voir http://offlinetags.net/en).

réserve des exemptions prévues aux articles 11 et 13. Dès que cela est raisonnablement réalisable et si la communication à un tiers est envisagée, les personnes concernées devraient, conformément à l'article 11 de la directive, recevoir, au moins lors de la première divulgation, les informations suivantes: l'identité du responsable du traitement et de son représentant, les finalités du traitement, toute information supplémentaire telle que les catégories de données concernées, les destinataires ou les catégories de destinataires des données, l'existence d'un droit d'accès aux données les concernant et de rectification de ces données.

Pour satisfaire à cette exigence de transparence et d'information à l'égard des personnes concernées, les responsables du traitement doivent envisager une approche par plusieurs moyens[43]. Les dispositifs habituels comme les écriteaux ou fiches d'information pour un événement (par exemple, le pack distribué au départ d'une course d'aviron) ou la documentation correspondante (par exemple, les programmes sportifs) pourraient aisément être utilisés en cas d'utilisation de drones dans des endroits déterminés (à l'occasion d'événements sportifs ou de concerts, sur les sites archéologiques, dans les parcs naturels, etc.) et peuvent se présenter sous une forme concise et avec des symboles pour faciliter la reconnaissance. On pourrait aussi envisager de recourir aux réseaux sociaux, aux zones d'affichage public dans les endroits fermés (par exemple, les écrans de télévision dans les stades), à l'émission de signaux sans fil, à des lumières clignotantes, des avertisseurs sonores et des couleurs vives. De plus, faire en sorte que l'utilisateur de drone soit bien visible permet aux autres personnes d'exercer plus facilement leurs droits. L'exigence de présenter une marque d'enregistrement (similaire à une plaque d'immatriculation pour les véhicules) n'est pertinente que si les drones sont visibles depuis le sol ou lorsqu'il y a perte de contrôle et que les données stockées doivent être renvoyées à l'opérateur. Exiger la transmission d'un signal sans fil servant de marque d'enregistrement pouvant être croisé avec une base de données en ligne est une autre solution intéressante. Cependant, il convient également de garder à l'esprit les préoccupations relatives à la protection et à la sécurité des données qu'un système d'enregistrement suscite[44].

En outre, en guise de bonne pratique, le groupe de travail recommande que les opérateurs de drones publient des informations sur leur site internet ou sur des plateformes spécialisées afin d'informer en permanence sur les différentes missions qui ont eu lieu ou qui sont prévues, tandis que dans les zones isolées ou là où il est peu probable que les individus consultent le site internet, les informations peuvent être publiées dans les journaux, dans des brochures, sur des affiches ou être communiquées par courrier[45].

Dans certains États membres, les autorités de l'aviation civile publient la liste des opérateurs autorisés à faire un usage professionnel de drones, ou des autorisations délivrées pour chaque mission. Il faut s'en féliciter car de telles listes facilitent l'accès aux informations concernant les opérations impliquant un traitement de données. En outre, étant donné que, dans de nombreux États membres où l'utilisation des drones est réglementée, pour différentes raisons, il est interdit d'utiliser

---

[43] En effet, le groupe de travail «Article 29» reconnaît que l'utilisation de RPAS pose problème quant à la manière d'informer les personnes concernées et de les inciter à consulter des informations à propos d'un appareil qui peut être si peu visible qu'elles ne remarqueront pas sa présence ou la collecte de données. Si l'on peut aisément concevoir d'informer les personnes concernées participant à un événement en plein air au moyen de panneaux d'avertissement sur le respect de la vie privée placés à l'entrée de la zone surveillée par RPAS, la question se pose quant à la manière de fournir des informations sur les RPAS qui survoleront l'espace public, sans délimitation précise de la portée territoriale.

[44] Par exemple, si une pharmacie effectue régulièrement des livraisons à l'aide d'un drone au domicile d'une personne, il est possible d'en déduire que l'occupant souffre d'un grave problème médical. Exiger d'un particulier qu'il soumette les plans de vol d'un drone ou prévoir la possibilité de consulter l'historique des vols d'un utilisateur de drone individuel ou d'une organisation y ayant recours, dont les sites de décollage et d'atterrissage, risque de susciter de sérieuses inquiétudes quant à la protection des données.

[45] Par exemple, un agent immobilier qui utilise un drone pour enregistrer des images d'une propriété à vendre, pourrait écrire aux voisins à l'avance, mais aussi rendre visite aux propriétés voisines le jour de l'enregistrement pour avertir du traitement.

des drones dans certaines zones, la publication de cartes (réalisées par les autorités de l'aviation civile et auxquelles les fabricants peuvent renvoyer, par exemple en publiant un lien vers une source d'informations gérée par les autorités de l'aviation civile) indiquant les zones où les drones peuvent être utilisés serait très utile (c'est-à-dire que la publication de ces cartes aiderait les personnes à repérer les zones dans lesquelles les drones peuvent être exploités).

La même approche par plusieurs moyens pourrait être conseillée dans les cas où les drones servent à surveiller de vastes infrastructures (les réseaux ferroviaires ou les réseaux électriques, par exemple). Les informations pertinentes peuvent être communiquées à l'aide d'écriteaux et de symboles et, si possible, sur des sites internet. Ces informations pourraient signaler de manière générale que l'infrastructure fait l'objet d'une surveillance sans qu'il soit nécessaire de fournir des détails sur les vols passés ou à venir, par exemple.

Enfin, comme pour les applications de drone qui peuvent couvrir des zones étendues, lorsque la communication d'informations aux personnes concernées s'avère difficile ou quasiment impossible, il a été suggéré de créer une source d'informations nationale ou multinationale (plus facile à consulter que les sites internet des opérateurs individuels) pour permettre aux personnes de déterminer les missions et les opérateurs associés à chaque drone[46]. Le groupe de travail reconnaît qu'une telle solution est souhaitable et invite la Commission européenne à recourir à des instruments de financement pour soutenir les recherches et les investissements dans ce domaine, sur d'éventuelles plaques d'immatriculation intelligentes pour les drones et dispositifs similaires[47].

3.6 Sécurité du traitement des données et questions connexes, périodes de conservation, contrôle préalable

Conformément à l'article 17 de la directive, les responsables du traitement et les sous-traitants, le cas échéant, doivent appliquer les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés. Cette disposition s'applique également aux attaques électroniques et cybernétiques (c'est-à-dire les interventions à distance sur l'appareil visant soit à prendre le contrôle total ou partiel de celui-ci soit à accéder aux capteurs ou aux données stockées).

Cette protection devrait également être assurée pour la phase de transmission de données à caractère personnel du drone vers la station de base. Il est recommandé que les concepteurs de drones et d'équipement fabriqués sur mesure pour être montés sur le drone engagent des experts en sécurité compétents afin de veiller à ce que les failles de sécurité soient dûment prises en compte.

---

[46] Groupe de travail sur la protection des données dans les télécommunications, «Working paper on Privacy and Aerial Surveillance», 54e réunion, Berlin, septembre 2013, publié sur le site www.berlin-privacy-group.org.

[47] Dans certaines situations très délicates, on pourrait également envisager d'instaurer des mécanismes de retour d'informations qui permettent de vérifier l'exécution de mesures spécifiques relatives à la protection des données. En ce qui concerne les mesures spécifiques envisagées dans le cadre des programmes Horizon 2020 et COSME afin de soutenir le développement du marché des RPAS, voir la communication de la Commission européenne intitulée «Une nouvelle ère de l'aviation – Ouvrir le marché de l'aviation à l'utilisation civile de systèmes d'aéronefs télépilotés, d'une manière sûre et durable», ibid. (action 6). La tâche de faire fonctionner ce dispositif (qui pourrait être un site internet dédié indiquant à l'avance, en temps réel et a posteriori la trajectoire que suivent les drones, ou un registre central accessible au public) pourrait être confiée, par exemple, à l'AESA, aux autorités nationales de l'aviation civile ou aux autorités chargées de la protection des données. L'obligation de leur faire rapport pourrait également être introduite par le législateur – non seulement pour les vols planifiés, mais aussi en ce qui concerne la finalité du traitement de données à caractère personnel qui aura lieu. À cet égard, il convient de rappeler que, en tout état de cause et dans la plupart des cas, les autorités nationales de l'aviation civile devront être informées de toutes les activités des drones afin de les autoriser. À ce sujet, voir le point 3.8 du présent avis.

De plus, les données à caractère personnel traitées à l'aide de drones ne peuvent être conservées plus longtemps que nécessaire aux fins du traitement[48]. Les données qui ne sont pas associées à une plainte ou à un problème devraient être effacées ou anonymisées immédiatement après.

L'incorporation de programmes de stockage et de suppression pourrait être recommandée. Dès lors, les dispositifs embarqués sur les drones devraient être conçus de manière à permettre de définir une durée de stockage précise des données à caractère personnel enregistrées et, ainsi, la suppression automatique régulière des données à caractère personnel qui ne sont plus nécessaires selon les programmes de suppression.

Concernant tous ces aspects, le groupe de travail souhaiterait attirer l'attention des responsables du traitement, au moins, sur les points suivants:

- limitation du nombre, à préciser, de personnes autorisées à visionner ou consulter les images enregistrées;
- octroi aux personnes précitées d'un accès limité selon le principe du «besoin d'en connaître»;
- stockage et transmission chiffrés des informations lorsque c'est nécessaire;
- consignation de tous les cas d'accès au matériel enregistré et d'utilisation de celui-ci;
- application rigoureuse de périodes de conservation des données et suppression ou anonymisation automatiques une fois la période de conservation écoulée;
- notification à l'autorité chargée de la protection des données des violations de données (dans la mesure où il s'agit d'une obligation imposée par la loi).

Selon les législations nationales applicables en matière de protection des données, des mesures et dispositifs additionnels pourraient découler de la première évaluation du traitement conformément au mécanisme de contrôle préalable (voir article 20 de la directive).

4. Rôle de la coopération entre les différents acteurs et importance des outils d'autorégulation

La coopération entre les autorités chargées de la protection des données et les autorités de l'aviation civile sera déterminante pour ce qui est de sensibiliser les fabricants, les opérateurs et les pilotes aux problèmes de protection des données liés à l'utilisation de drones équipés de capteurs. On pourrait recourir à des cours de formation, des événements publics ou de simples brochures pour aborder ce thème. Il faudrait aussi déterminer si le traitement actuellement réalisé par les autorités de l'aviation civile pour délivrer des licences aux pilotes de drones et certifier les opérateurs comprend certaines étapes qui pourraient offrir une bonne occasion d'aborder les aspects ayant trait à la vie privée ou à la protection des données dans l'utilisation des drones.

Dans la plupart des cas, des certificats ou des autorisations très spécifiques sont octroyés par les autorités de l'aviation civile qui régissent l'utilisation de drones civils: la zone et la trajectoire de survol, l'appareil ainsi que l'opérateur et le responsable du traitement font tous fréquemment l'objet d'un examen dans ce contexte[49]. Dans certains pays, le respect des exigences en matière de protection des données fait déjà partie d'un examen discrétionnaire réalisé par les autorités aéronautiques compétentes au moment d'accorder les permis de pilotage d'aéronefs[50]. Le cadre étant

---

[48] Par exemple, les images/vidéos capturées par les drones en vue de sécuriser la zone à ciel ouvert d'un festival ne seront conservées que pour la durée nécessaire à l'examen d'éventuelles plaintes ou questions de sécurité.

[49] Concernant cet aspect, voir les résultats d'une étude réalisée parmi les autorités nationales de l'aviation civile, publiée dans Rachel L. Finn, David Wright et Anna Donovan (Trilateral Research & Consulting, LLP), Laura Jacques et Paul De Hert (Vrije Universiteit Brussel), «Privacy, data protection and ethical risks in civil RPAS operations», p. 145 et suiv. Pour une description du cadre réglementaire européen et national actuel en matière de drones, voir p. 363 et suiv.

[50] (ibid.). Par exemple, l'examen en vue d'obtenir la licence de pilote de RPAS pourrait comporter un contrôle des connaissances de base concernant la législation en matière de respect de la vie privée et de protection des données à caractère personnel, afin de garantir que les pilotes sont informés des obligations juridiques imposées en cas de traitement de données à caractère personnel.

établi, le fait d'informer l'autorité de l'aviation civile compétente du respect de toutes les exigences énoncées par la législation en matière de protection des données, du traitement de données à caractère personnel envisagé et des finalités que ce dernier poursuit constitue une bonne pratique à encourager car elle pourrait aussi permettre d'attirer l'attention des opérateurs sur les aspects liés à la protection des données avant un vol autorisé[51], et de créer une base de données centrale, accessible au public, qui pourrait au moins contenir une liste d'opérateurs (reprenant une description générale des finalités pour lesquelles ils pourraient traiter des données à caractère personnel)[52]. Cela ne signifie pas que les autorités de l'aviation civile se chargeront de vérifier que l'opérateur de drone a pris les mesures appropriées pour se conformer à la législation nationale en matière de protection des données, mais qu'elles constitueront un point de contrôle précieux qui permettra à l'opérateur de drone de prendre une décision en connaissance de cause concernant les mesures à mettre en œuvre et de savoir s'il peut considérer ces dernières comme suffisantes.

On pourrait envisager de promouvoir des codes de conduite et des programmes de certification pour les fabricants et les opérateurs afin de mieux informer les opérateurs de drones civils et de leur permettre de mieux comprendre les problèmes liés à la protection des données, mais aussi pour aider les autorités chargées de la protection des données à contrôler la conformité. La fonction importante que les codes de conduite pourraient remplir dans ce contexte se conçoit d'autant mieux que les autorités chargées de la protection des données ne peuvent pas statuer ou engager des poursuites en cas d'atteinte à la vie privée dépassant leurs pouvoirs légaux, alors que c'est sur ce point que la responsabilisation des opérateurs de drones peut s'avérer utile.

Enfin, les labels de protection de la vie privée pourraient également jouer un rôle utile. Même si de tels programmes ne dispensent pas les responsables du traitement de connaître leurs engagements en matière de protection des données et de respect de la vie privée, la participation d'opérateurs et de fabricants de drones, dans le cadre d'une approche générale en matière de label de protection de la vie privée, pourrait être préconisée comme moyen de favoriser la responsabilisation et la conformité.

5. Indications et recommandations finales

À la lumière des risques potentiels et des conséquences que l'ouverture du marché de l'aviation aux drones entraînerait pour la vie privée et les libertés civiles et politiques individuelles, le groupe de travail tient à attirer l'attention des législateurs européens et nationaux, des fabricants de drones et d'équipements connexes, ainsi que des opérateurs/utilisateurs de drones, sur les indications et recommandations finales ci-après, qui sont destinées à fournir des orientations supplémentaires à celles déjà contenues dans les avis et documents du groupe de travail cités dans le présent avis.

5.1 Démarches à entreprendre avant d'exploiter un drone:

1. vérifier si la législation nationale permet l'utilisation de drones et s'il est nécessaire d'obtenir une autorisation spéciale auprès des autorités de l'aviation civile;

---

[51] Par exemple, en 2012, les autorités allemandes ont modifié la réglementation sur la circulation aérienne [Luftverkehrs-Ordnung (LuftVO)] pour ajouter le respect d'exigences relatives à la protection des données dans l'examen discrétionnaire auquel les autorités aéronautiques compétentes des Länder allemands procèdent lorsqu'elles délivrent des permis de piloter des aéronefs.

De même, la réglementation sur les véhicules aériens télépilotés qui a été adoptée en Italie le 16 décembre 2013 dispose que «lorsque les missions réalisées par un RPAS sont susceptibles de donner lieu à un traitement de données à caractère personnel, ce fait doit être rapporté dans les documents produits aux fins de l'octroi de l'autorisation visée» (article 22).

[52] Cela pourrait également répondre à des préoccupations concernant la sécurité car il ressort d'informations récentes que des drones ont survolé illégalement des bâtiments stratégiques situés en zone urbaine, sans aucune possibilité d'identifier les personnes qui pilotaient ces drones.

2. définir le rôle des différents acteurs possibles: dans la mesure où le traitement n'est pas effectué directement par le responsable du traitement, veiller à ce que le traitement soit régi pas un contrat ou un acte juridique qui lie le sous-traitant vis-à-vis du responsable du traitement et à ce que ce sous-traitant agisse uniquement sur les instructions du responsable du traitement;
3. évaluer l'incidence sur la protection des données en tenant compte de la finalité des opérations et du type de drones (dimension, visibilité, etc.), ainsi que des combinaisons particulières de technologies de captage embarquées; définir la base juridique la plus appropriée (consentement des personnes concernées, exécution d'un contrat, obligation légale, intérêt légitime, etc.) et déterminer s'il est nécessaire d'informer/consulter les autorités chargées de la protection des données compétentes conformément à la législation nationale en matière de protection des données;
4. choisir la technologie embarquée la plus proportionnée et adopter toutes les mesures de respect de la vie privée par défaut appropriées: définir les services et les produits de manière à éviter la collecte ou le traitement ultérieur de données à caractère personnel inutiles;
5. trouver la façon la plus appropriée d'avertir au préalable les personnes susceptibles d'être affectées par le traitement des données: informer au moyen d'écriteaux ou de fiches d'information en cas d'opération visuelle dans une zone précise; dans le cas d'un événement, informer le public par les réseaux sociaux, les journaux, des brochures ou des affiches; toujours donner des informations claires sur les sites internet concernés: les notes d'information devraient toujours indiquer clairement qui est le responsable du traitement et quelles sont les finalités poursuivies par le traitement, mais aussi informer clairement les personnes concernées sur l'exercice de leur droit d'accès aux enregistrements visuels ou non visuels les concernant;
6. prendre toutes les mesures techniques et d'organisation appropriées afin de garantir un niveau de sécurité adéquat compte tenu des risques que le traitement présente et de la nature des données à traiter, en particulier pour empêcher tout traitement non autorisé, y compris pendant la phase de «transmission»;
7. supprimer ou anonymiser les données à caractère personnel inutiles peu après la collecte ou dès que possible.

5.2 Recommandations à l'intention des décideurs politiques et des organismes de réglementation du secteur

L'ouverture du marché de l'aviation à l'usage civil de drones devrait aller de pair avec:

1. la mise en place, aux niveaux européen et national, d'un cadre visant à garantir non seulement la sécurité des vols mais aussi le respect de tous les droits fondamentaux. Dans cette perspective, le groupe de travail encourage la participation de toutes les parties intéressées au débat sur l'intégration des drones dans l'espace aérien civil;
2. l'harmonisation et la modernisation des politiques des États membres relatives aux drones, y compris la question des dispositions législatives applicables à l'exploitation transfrontière de drones;
3. l'inscription, dans le cadre susmentionné, de règles spécifiques assurant une utilisation responsable des drones, lesquelles doivent nécessairement inclure le respect des espaces privés (comme les jardins, les cours, les terrasses, etc.); à cet effet, l'instauration, lorsque c'est nécessaire, de périmètres virtuels – ou de zones d'exclusion aérienne – pourrait être envisagée. En outre, comme l'utilisation de drones peut être limitée à des zones très précises dans de nombreux États membres, la publication de cartes par les autorités de l'aviation civile aiderait les utilisateurs à comprendre à quels endroits l'utilisation de drones est permise (étant entendu que les autres principes sont respectés);

4. l'instauration d'une obligation, au niveau européen ou national, pour les fabricants de ne commercialiser que des drones de petite taille, dans l'emballage desquels sont fournies des informations suffisantes (par exemple, dans le mode d'emploi) sur le caractère potentiellement intrusif de ces technologies et rappelant la nécessité de respecter les législations et réglementations européennes et nationales en matière de protection de la vie privée, des données à caractère personnel et des autres droits fondamentaux;
5. l'élaboration et l'instauration par les décideurs politiques compétents au niveau européen ou national, en étroite concertation avec les représentants du secteur, de critères d'évaluation de l'incidence sur la protection des données que les entreprises et opérateurs peuvent utiliser aisément;
6. l'ajout des aspects de la protection des données aux principaux éléments des dispositions nationales régissant l'utilisation des drones à des fins commerciales (concernant la qualification et la formation des pilotes, les exigences d'aptitude au vol et de certification, lors de la délivrance/révocation des licences d'exploitation et des permis de travail aérien, etc.). En particulier, on pourrait prévoir comme condition d'octroi d'une autorisation la fourniture d'une déclaration attestant que les exigences en matière de protection des données ont été satisfaites;
7. la promotion de programmes de certification en matière de protection des données afin de mieux informer les opérateurs et de leur permettre de mieux comprendre les problèmes liés à la protection des données, mais aussi en vue de veiller à la conformité;
8. par ailleurs, le groupe de travail recommande à la Commission européenne de recourir aux programmes de financement pour soutenir la recherche et les investissements en faveur de nouvelles technologies destinées à accroître la transparence (nouvelles technologies pour informer le grand public des survols de drones, des finalités de ces derniers et de l'exercice de ses droits d'accès), par exemple des plaques d'immatriculation intelligentes ou un site internet sur lequel seraient publiées des informations en temps réel sur toutes les exploitations de drones.

5.3 Recommandations aux fabricants ou aux opérateurs:

1. intégrer des choix de conception et des paramètres par défaut respectueux de la vie privée dans le cadre d'une approche du respect de la vie privée dès la conception;
2. associer un délégué à la protection des données (lorsque c'est possible) à la conception et la mise en œuvre de politiques liées à l'utilisation de drones;
3. promouvoir l'adoption de codes de conduite pouvant aider les entreprises et les différentes catégories d'opérateurs à éviter les infractions et à accroître l'acceptabilité sociale des drones. Ces codes devraient comporter des sanctions en cas de non-respect par les signataires;
4. rendre le drone aussi visible et repérable que possible (au moyen de signaux sans fil, de lumières clignotantes ou d'avertisseurs sonores, de couleurs vives);
5. lorsqu'il se trouve dans la ligne de visée, rendre l'opérateur bien visible et identifiable en tant que responsable du drone au moyen d'une signalétique;
6. lors de la planification et de l'exécution d'un vol, même lorsqu'il est permis que le drone survole des zones peuplées, éviter autant que possible de voler au-dessus ou à proximité des espaces privés et des immeubles.

5.4 Recommandations relatives à l'utilisation de données à caractère personnel collectées au moyen de drones à des fins répressives

Comme pour l'usage de drones à des fins commerciales, l'utilisation de données à caractère personnel collectées au moyen de drones par la police ou d'autres autorités répressives devrait:

1. respecter les principes de nécessité, de proportionnalité, de limitation de la finalité, de minimisation des données et de respect de la vie privée dès la conception. Une période de conservation stricte et justifiée devrait être fixée;
2. le principe de transparence devrait être respecté: la loi devrait prévoir/prescrire que le traitement des données qu'implique l'utilisation de drones soit transparent et prévisible pour les personnes concernées, ces dernières devant être informées autant que possible du traitement et de leurs droits à cet égard;
3. le traitement de données à des fins répressives effectué au moyen de drones ne devrait pas permettre le suivi constant des personnes ou, à tout le moins, dans les cas où le suivi constant s'avère strictement nécessaire, celui-ci doit être restreint aux enquêtes des forces de l'ordre autorisées par un mandat. Les équipements techniques et de captage doivent être utilisés en accord avec la finalité du traitement;
4. l'interdiction de l'exécution automatique des décisions s'applique également à ces usages. Les données traitées par les drones doivent être examinées ultérieurement par un opérateur humain avant que toute décision faisant grief à une personne ne soit prise;
5. les juridictions devraient généralement être à même d'examiner l'utilisation de drones aux fins du renseignement et de l'application de la loi au regard des pratiques nationales;
6. il convient de réaliser un réexamen régulier de la nécessité de traiter des données à caractère personnel au moyen de drones et de la conformité de cette utilisation avec l'évolution des cadres juridiques;
7. en outre, l'utilisation de drones à des fins répressives, même en cas d'enquête autorisée par un mandat – comme la surveillance ciblée –, devrait exiger un régime d'approbation suffisamment élevé dans la hiérarchie de l'organisation. En fonction de la législation nationale, les données à caractère personnel collectées au moyen de drones pour ces types d'enquêtes doivent être intégrées dans les dossiers administratifs susceptibles d'être utilisés devant les tribunaux.