

IP INNOVATION & PROSPECTIVE



Retrouvez-nous sur notre site [www.cnil.fr/ip] en flashant le code ou sur :



web

IP - ÉTUDES ET ENQUÊTES

Quand la surveillance se donne des ailes

Sujet médiatique croissant, les drones sont des plateformes mobiles de capteurs qui semblent "bonnes à tout faire", à la fois comme outil de surveillance et comme outil de service. Comment les utiliser sans pour autant porter atteinte à l'intimité des personnes ?

3 questions à... Ryan Calo

Professeur de droit à l'université de Washington et auteur de l'article *The Drone as a Privacy Catalyst*.

IP - FOCUS

Le "do it yourself" drone, nouvelle plateforme préférée des hackers ?

En bref...

Les chiffres marquants

Drones, innovations, vie privée et libertés individuelles

Pourquoi s'intéresser aux drones lorsqu'on est en charge de la protection des données personnelles ?

Parce que ces engins volants bardés de capteurs, peuvent être de formidables machines à observer, à emmagasiner et à analyser de l'information, et qu'il s'agit de débattre dès à présent du cadre applicable à ces nouvelles formes possibles de surveillance de nos comportements, de nos déplacements, en bref de notre vie privée.

Ce questionnement ne doit pas bien sûr nous faire sombrer dans la technophobie.

En effet, si comme le souligne le professeur Ryan Calo, les drones sont, à certains égards, "l'incarnation technologique et froide de la surveillance", ils témoignent aussi d'une inventivité débordante dans les usages et recèlent d'importantes potentialités pour de nouveaux services. Le cadre de régulation à créer doit donc à la fois tracer des lignes rouges et offrir un espace de liberté aux innovations. L'exercice est délicat. Le sujet étant au carrefour de l'éthique, du droit, de l'économie, du social, etc., la réflexion doit être pluridisciplinaire et impliquer l'ensemble des acteurs concernés parmi lesquels les industriels du secteur, les autorités en charge de la réglementation aérienne, la société civile.

Elle doit bien sûr être menée aussi au plan international, notamment dans le groupe de l'article 29 (G29) réunissant les CNILs européennes. Pour sa part, la CNIL s'est fortement engagée dans ces travaux. Elle le fait avec d'autant plus de volontarisme que, comme le montre cette lettre IP, le sujet « drones » est à bien des égards une première esquisse de la problématique autrement plus large de l'éthique de la robotique.



Édouard GEFFRAY,
Secrétaire général de la CNIL ■

Quand la surveillance se donne des ailes...

Un drone est au sens strict un appareil sans pilote à bord. Dans l'esprit collectif c'est un appareil volant, même si en réalité la problématique s'étend à tout véhicule autonome partiellement "robotisé". Il est généralement piloté à distance par un opérateur humain, mais peut alors avoir un degré plus ou moins important d'autonomie (par exemple pour éviter des collisions, gérer les conditions aérologiques, ou même atteindre la destination assignée par l'opérateur, qui n'est alors plus vraiment un pilote mais un superviseur). En réalité, un drone est avant tout une plateforme de capteurs mobile. En effet il emporte toujours une gamme de capteurs divers, au premier rang desquels une camera, mais également potentiellement des microphones, capteurs thermiques, capteurs infrarouges, détecteurs de composants chimiques... En fait, tous les types de capteurs utiles à la sécurité du vol ou à la mission du drone peuvent

composer la charge utile d'un drone. Certains capteurs peuvent même servir aux deux finalités : ainsi, la caméra du drone servira au pilotage « au-delà de l'horizon » par l'opérateur tout comme elle pourra servir pour une mission d'observation/surveillance. Si un drone peut peser plusieurs dizaines de tonnes et mesurer plusieurs mètres d'envergure ou bien ne peser que quelques centaines de grammes et tenir dans la main, il reste une machine à fusionner les données issues de capteurs. Les drones sont donc des engins d'observation, d'acquisition et de transmission de données géolocalisées.

C'est évidemment vrai pour les drones militaires qui – avant d'être les « chasseurs-tueurs » décrits par Grégoire Chamayou dans son ouvrage « *la Théorie du drone* » (édition La Fabrique, 2013) – sont des appareils de reconnaissance et de renseignement. Mais c'est également vrai à l'autre bout du spectre pour le monde des drones « brico-

lés » - les drones *do it yourself* (cf. focus en p. 4) - dont l'essor est fulgurant. La revue phare de la Silicon Valley, *Wired*, a ainsi dédié sa une à ces drones « maisons » en juillet 2012 en insistant sur ce point : certains capteurs autrefois lourds et coûteux, comme des accéléromètres, des boussoles ou mêmes des puces GPS, sont aujourd'hui présents dans des millions de smartphones : leur coût et leur taille ont donc dramatiquement décliné grâce à ce marché, ouvrant la voie à des drones de petite taille, à très faible coût (quelques centaines d'euros)¹ et à usage essentiellement ludique. L'entreprise française Parrot est d'ailleurs devenue le symbole de ce mouvement avec son *AR drone*.

D'un côté, une terrifiante machine de guerre, de l'autre un jouet du dimanche ? Mais ces deux figures antinomiques ne sont que les deux pôles opposés d'un spectre d'usages potentiels en réalité très vaste.

Demain des drones à tout faire ? Espionner, surveiller, protéger, transporter, amuser...



Technologie militaire à l'origine, les drones sont aujourd'hui à l'orée d'une toute nouvelle carrière civile. Assez naturellement, en glissant hors du militaire, les drones ont abordé le domaine civil par les mondes de la police et de la sécurité. Les premiers usages non militaires des drones sont donc des usages de sécurité globale, déclinaisons civiles de leur mission militaire d'observation et de renseignement. Les drones civils sont avant tout des engins de surveillance (aérienne) de nouvelle génération et les premiers utilisateurs de ces engins pour cette mission sont évidemment les pouvoirs publics : surveillance d'événements majeurs (sommets internationaux, grands événements publics,...), des frontières, voire de manifestations et rassemblements sur la voie publique, ou simples missions de sécurité et d'ordre public. La sécurité civile est également intéressée par les avantages du drone pour certaines missions de gestion de crise (surveillance des incendies de forêts ou accès à des zones de crise difficilement accessibles comme des zones inondées ou

touchées par des accidents industriels,...). De leur côté, des compagnies privées envisagent d'utiliser ou testent même déjà l'emploi de drones pour des missions similaires : surveillance de chantiers, de réseaux étendus (réseau électrique, réseau ferroviaire, etc.). Cette fonction d'observation peut d'ailleurs trouver de nombreuses autres déclinaisons : des scientifiques envisagent ainsi l'utilisation de drones, tout comme des organisations humanitaires ou écologistes, pour des missions de surveillance de l'impact écologique des activités humaines (par exemple pour des zones de pêches).

Mais les usages des drones ne se limitent pas à des missions de surveillance, même si cette application est consubstantielle aux drones. Ces engins peuvent également transporter des charges, par exemple pour déplacer des médicaments en zone isolée et dans les pays en développement, pour améliorer la performance agricole en ciblant très précisément des épandages de produits, pour déplacer des objets sur des chantiers de construction, etc. Il est même envisagé d'utiliser des drones comme défibrillateur mobile que l'on pourrait envoyer auprès d'une victime d'un incident cardiaque...

Enfin des usages de service émergent. Les premiers à avoir saisi cette opportunité sont évidemment les photographes professionnels, déjà souvent utilisateurs de modèles réduits aériens téléguidés plus classiques. De nombreux professionnels proposent ainsi des prises de vue artistiques, de promotion/communication ou journalistiques par l'intermédiaire de

drones. Certains cas d'usages de drones par des paparazzis ont d'ailleurs déjà défrayé la chronique...

Enfin, les usages ludiques sont en pleine explosion. Le marché du drone de loisir est même en passe de devenir le plus vaste : des milliers de drones très basiques, pilotables à partir d'un smartphone, ont déjà été vendus, en particulier l'AR drone de la société française Parrot.

Tout cela pose les bases d'un marché loin d'être négligeable : l'association internationale « Association for Unmanned Vehicle Systems International » évalue, peut-être de manière un peu optimiste, l'impact économique de l'industrie commerciale des drones à près de 13,6 milliards de dollars aux États-Unis². Une étude du Teal Group de juin 2013 évalue quant à elle le marché mondial des drones tous secteurs confondus à 5,2 milliards de dollars pour l'année 2013 et prévoit que ce marché double dans les dix ans qui viennent³.

Selon le Washington Times, l'autorité fédérale chargée de l'aviation civile aux États-Unis prédit que 30 000 drones pourraient opérer sur le sol américain à l'horizon 2020⁴. Le français Parrot aurait quant à lui déjà vendu plus d'un demi-million de modèles de son AR drone dans le monde⁵.

¹ « Personal Drone's Secret Ingredient: iPhone » in *Wired*, juillet 2012.

² AUVSI. *The Economic impact of unmanned aircraft system integration in the United States*; mars 2013.

³ Source : Teal Group <http://tealgroup.com/index.php/about-teal-group-corporation/press-releases/94-2013-uav-press-release>.

⁴ Shaun WATERMAN. "Drones over U.S. get OK by Congress", *The Washington times*, 7 février 2012.

⁵ David CORNISH, "ESA launches drone app to crowdsource flight data", *Wired.co.uk*, 15 mars 2013.

3 questions à... Ryan Calo



Professeur de droit à l'Université de Washington et chercheur associé au « Center for Internet and Society » de Stanford.

■ Vous avez écrit en 2011 dans un article que « les drones [...] représentent l'incarnation technologique et froide de l'observation »^a. Quels sont pour vous les principaux enjeux de vie privée liés au développement des drones, et quelle est votre opinion sur l'état actuel de ce débat aux États-Unis ?

À mon avis, l'enjeu principal est que les drones rendent la surveillance plus facile et moins coûteuse. En conséquence, nous allons probablement en voir de plus en plus. Les lois américaines concernant la protection de la vie privée, cependant, ont besoin de rattraper l'avance prise par les moyens de surveillance. L'objet de la

phrase que vous citez était cependant différent : je voulais souligner que les risques liés à la surveillance par les drones, à l'inverse des autres formes de surveillance électronique, étaient faciles à appréhender, à visualiser par les citoyens.

■ Dans une hypothèse plus optimiste, vous avez appelé les drones un « catalyseur de vie privée » dans le titre de ce même article. Qu'entendiez-vous par là ?

Je prédisais alors que notre réaction viscérale (au sens propre) aux drones nous conduirait à réexaminer l'adéquation de nos lois concernant la vie privée à ces enjeux de surveillance. Cette évolution est engagée, quoique malheureusement elle se soit spécifiquement focalisée sur les drones à l'exclusion de toutes les autres technologies de surveillance. Cette focalisation prend fin progressivement, en particulier suite à une décision de la Cour Suprême des États-Unis concernant l'utilisation d'appareils GPS (US vs. Jones)^b, et bien sûr suite aux révélations concernant la surveillance de la National Security Agency (NSA).

■ Vous êtes un spécialiste non seulement des drones mais plus largement des questions liant la robotique et la vie privée. Comment voyez-vous l'évolution de ce sujet de l'éthique et

du droit de la robotique dans les prochaines années ?

Je crois qu'un défi intéressant est lié au fait que les robots, à l'opposé d'autres technologies, semblent avoir un sens sociétal. De nombreux objets ont un sens pour nous : par exemple une voiture sera synonyme de liberté, et un bijou de famille est plus important qu'un bijou acheté dans le commerce. Mais nous réagissons avec les robots comme s'il s'agissait d'objets sociaux. Ainsi, une étude récente de l'université de Washington, au sein de laquelle je travaille, suggère que l'attachement émotionnel des soldats pouvait influencer l'issue des combats. J'ai fait l'hypothèse que les robots pouvaient envahir notre solitude, notre isolement, par leur simple présence à la maison et au bureau même s'ils ne collectent et ne partagent pas d'informations. Prendre en compte la manière dont nous ressentons les robots sera un défi légal et éthique primordial dans les années à venir. Un second défi concerne le sujet des responsabilités juridiques (par exemple celles « du fait des choses »). J'explore cet enjeu en profondeur dans un article de la revue de droit Maryland Law Review intitulé « Open robotics » et qui est disponible au téléchargement ici : <http://ssrn.com/abstract=1706293>.

a. CALO, Ryan « The Drone as Privacy Catalyst », Stanford Law Review, 12 décembre 2011
b. Cour Suprême des États-Unis, 23 janvier 2012 « United States v. Jones (2012) »

Le drone comme froide incarnation de la surveillance robotique future ?

Pourquoi le drone soulève-t-il des interrogations aussi fortes concernant les droits et libertés des personnes⁸ ? Simplement car il s'agit d'une plateforme à nulle autre pareille, « incarnation froide et parfaite de la surveillance » selon la formule de Ryan Calo (cf. entretien), qui allie aux capteurs ses caractéristiques propres :

- la discrétion car on ne voit pas nécessairement le drone qui nous « capte » ;
 - « l'intrusivité » : un drone peut pénétrer et surveiller des espaces normalement inaccessibles (une fenêtre en étage élevé par exemple) ;
 - la captation de masse sans distinction : l'appareil peut enregistrer de manière indiscriminée des informations concernant un grand nombre de personnes, surtout si la zone de couverture est très large (le projet Gorgon Stare de l'armée américaine prévoit la surveillance d'un carré de 40 km²) ;
 - la permanence de l'observation, certains drones à longue endurance pouvant rester en position pendant de nombreuses heures ;
 - la mobilité de la surveillance, permettant ainsi de suivre des personnes ciblées, etc.
- Les drones, super caméras de vidéosurveil-

lance ailées, posent certes des questions similaires à celles que pose globalement la vidéosurveillance mais avec une magnitude et une complexité d'une toute autre ampleur : comment garantir l'anonymat dans l'espace public ? Comment ne pas aboutir à une surveillance potentielle permanente de l'ensemble de la population comme d'individus ciblés dans les espaces publics, voire dans les espaces privés ?

Au delà, comme le montre l'usage militaire, le drone offre des moyens d'action à distance et ne reste donc pas dans la durée qu'un capteur passif. Comme l'a souligné Éric Germain dans Le Monde, « il sera tentant de les équiper d'armes « à létalité réduite » mais, avant cela, ils auront probablement été utilisés dans des missions de coercition « douces » qui transformeront la vidéosurveillance en vidéociblage (pointeur laser) avec la détection automatisée de « comportements suspects » au sein de foules ou de manifestations »⁹.

Pour autant, ne voir les drones que par le spectre de la surveillance généralisée serait une erreur qui pourrait conduire à tuer dans l'œuf à la fois les contre-pouvoirs que cette technologie porte en elle-même et les

innovations positives qu'elle promet. S'il est incontestable que cette nouvelle technologie est susceptible de constituer une véritable menace pour nos libertés, nous devons probablement accepter qu'elle continue à se déployer. La question à se poser est alors de savoir pour quels usages et avec quels contrôles ?

Foncièrement ambivalents, ces nouveaux outils demandent donc une régulation toute aussi innovante dans ses modalités d'applications. Avant toute chose, l'encadrement réglementaire des engins aériens doit s'adapter à ces outils (comme en France avec deux arrêtés d'avril 2012¹⁰ et en Europe avec la feuille de route en cours « Remotely Piloted Aircraft Systems »). Mais il s'agit moins d'élaborer de nouveaux textes que de penser à des modalités d'application adaptées aux spécificités de ces techniques.

Du point de vue de la protection des droits et libertés des personnes et en particulier de l'intimité de leur vie privée, le drone pose, au-delà des interrogations sociétales et éthiques, un problème d'applicabilité du droit tel qu'il existe aujourd'hui pour encadrer les technologies de surveillance. ►►

Il suffit ici, sans entrer dans les détails juridiques, d'évoquer certaines des garanties prévues par exemple dans le cadre de la vidéosurveillance : le « floutage » des images, à certains endroits prédéterminés du périmètre de la caméra, l'interdiction de pointer la caméra vers une habitation ou son entrée, etc. Ces obligations paraissent difficilement applicables aux drones. Prenons également la question de l'information des personnes : comment être averti du survol d'un drone et comment s'en prémunir ? Il importe très certainement en ce domaine de rechercher des solutions y compris sur le plan technique, permettant de garantir de façon effective, le respect des droits et libertés de chacun. L'innovation doit donc également être du côté de la régulation...

Ce débat n'est que la prémisse d'une réflexion beaucoup plus large sur les questions d'éthique de la robotique. En effet, un drone n'est rien d'autre qu'un robot inabouti : au bout des ondes, il y a encore généralement un opérateur qui prend les décisions de pilotage et d'action. Pourtant, pour des raisons d'efficacité, les drones intègrent progressivement plus d'automatismes et acquièrent donc de l'autonomie décisionnelle. Cette tendance nous permet d'anticiper le moment où ces engins prendront des décisions et agiront sans un humain « dans la boucle ». Les essaims de drones sont déjà conçus comme un moyen de faire accomplir des tâches programmées

sans intervention humaine à un ensemble de robots coopérants entre eux... et éventuellement apprenant les uns des autres. Il paraît indispensable de penser les drones dans ce cadre plus global de l'éthique de la robotique, qui n'en est aujourd'hui qu'à ses balbutiements. Car si la surveillance robotique peut d'une certaine façon nous protéger de la curiosité humaine, elle offre des possibilités insoupçonnées de détection de comportements jugés « anormaux ». À nous d'éviter un monde où les individus seraient surveillés par des robots autonomes pilotés par d'autres robots, logiques ceux-là, les algorithmes... La CNIL participe ainsi au groupe de travail constitué par le **Centre de recherche Saint-Cyr-Coëtquidan** sur les problématiques éthiques et juridiques soulevées par le développement de la robotique militaire et civile de surveillance. Enfin, au titre de sa participation à la **Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene**, elle suit les travaux engagés sur l'éthique de la recherche en robotique.

Geoffrey Delcroix ■

8. Par exemple dans ce document de l'Information and privacy commissioner, Ontario, Canada. *Privacy and drones : unmanned aerial vehicles*, août 2012.
 9. Éric Germain « La campagne pour l'interdiction des "robots tueurs" se trompe-t-elle de cible ? » *Le Monde*, 24 juin 2013.
 10. Arrêtés du 11 avril 2012 relatifs à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord et à la conception des aéronefs civils qui circulent sans aucune personne à bord, aux conditions de leur emploi et sur les capacités requises des personnes qui les utilisent. (JORF du 11 mai 2012)



En bref...

> Près de 40 % de la population mondiale sera connectée à Internet fin 2013, soit 2,7 milliards de personnes, estime l'UIT. (*MIS Report*, 2013)

> 59 % des internautes américains pensent qu'il n'est pas possible d'être complètement anonyme en ligne. (*Étude Pew Internet* « Anonymity, Privacy, and Security Online », juillet 2013).

> Les e-mails non-solicités ont représenté 67,6 % du trafic mondial en août 2013. Les campagnes de phishing ont connu une forte hausse et représentent 5,6 % de l'ensemble du trafic d'e-mails. (*Étude de Kapersky Lab*, octobre 2013).

> Le marché mondial de l'Internet des objets devrait passer de 4 800 MD de dollars en 2012 à 8 900 MD en 2020. (*Étude du cabinet IDC*, octobre 2013).

Le « do it yourself » drone (DIY), nouvelle plateforme préférée des hackers ?

Lors des « DroneGames » organisés à San Francisco en décembre 2012, une équipe de développeurs de l'entreprise Groupon a "hacké" un AR drone afin qu'il prenne en photo le public, utilise un outil de reconnaissance faciale puis tweete la photo avec le nom de la personne lorsque celle-ci était identifiée. L'équipe gagnante, de l'université de Stanford, avait, quant à elle, utilisé son drone pour pirater et prendre le contrôle d'autres drones environnants... Comme le soulignèrent les organisateurs, l'éclosion d'événements de ce type prouve « que les développeurs n'ont plus besoin d'un doctorat et d'une habilitation de sécurité pour écrire des logiciels pour drones volants. Les fonctions que tout programmeur Web utilise pour développer des apps peuvent dorénavant faire naviguer un drone, lui faire prendre des photos, trouver des gens, voler au travers d'une fenêtre ou jouer à des jeux »⁶. Plusieurs experts pensent que le drone est le domaine qui concentrera

le plus de *disruption* et de bricolage dans les années à venir. À la manière du Homebrew Computer Club de San Francisco en 1975, où quelques bricoleurs inventèrent la micro-informatique moderne en se servant « de l'ordinateur comme d'une bicyclette pour l'esprit », selon la formule de Steve Jobs, les drones hackés « DIY » seraient une extension des sens comme l'ordinateur est une extension de l'esprit humain⁷. Dès lors il n'est pas étonnant de constater que des milliers de développeurs cherchent aujourd'hui à détourner des drones de leur usage initial et s'en servent pour faire des démonstrations de concept, comme ces équipes universitaires qui travaillent avec des drones de loisir sur des concepts d'essaims d'engins robotisés travaillant à l'accomplissement d'une tâche de manière autonome.

Geoffrey Delcroix ■

⁶<https://blog.groupon.com/cities/groupon-hosts-the-first-drone-games/>

⁷Trevor TIMM et Parker HIGGINS. « Nobody Knows a Drone », *The New Inquiry*, 2 juillet 2012

CNIL
Commission Nationale de l'Informatique et des Libertés

Commission Nationale de l'Informatique et des Libertés

Direction des Études, de l'Innovation et de la Prospective
8, rue Vivienne - CS 30223 - 75083 Paris CEDEX 02
Tél.: 01 53 73 22 22 - Fax: 01 53 73 22 00
deip@cnil.fr

Édition trimestrielle

Directeur de la publication : Édouard Geffray

Rédacteur en chef : Sophie Vulliet-Tavernier

Conception graphique : EFIL Communication

02 47 47 03 20 - www.efil.fr

Impression : Champagnac

Crédit photos : CNIL / Istock

ISSN : 2118-9102

Dépôt légal : à publication

©2013

Les points de vue exprimés dans cette publication ne reflètent pas nécessairement la position de la CNIL

