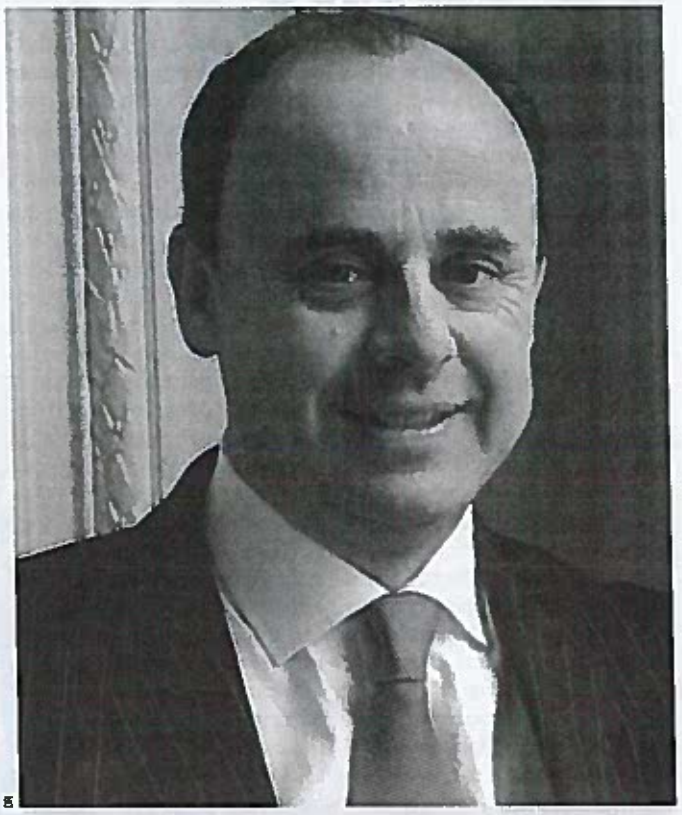
TRIBUNE LIBRE

Le concept de « Privacy by Design » à la rescousse des drones civils européens

par Laurent Archambault

AVOCAT À LA COUR, LAURENT ARCHAMBAULT EST UN DES ACTEURS IMPORTANTS DE LA FILIÈRE DRONES CIVILS. LE CABINET SELENE AVOCATS, EN EFFET, EST MEMBRE DU CONSEIL POUR LES DRONES CIVILS.



Les drones sont par essence des appareils permettant discrètement des prises de vues ou la captation de données. La grande majorité de ces aéronefs sont de petite taille. Ils peuvent voler près du sol, longer des édifices ou encore suivre une personne de jour comme de nuit. Comme l'a souligné Edouard Geffray, secrétaire général de la Cnil, la problématique du drone pour la vie privée et la protection des données réside d'ailleurs non pas tant dans l'emport de capteurs que dans la mobilité et la discrétion de l'appareil. A cet égard, le concept de « Privacy by Design » pourrait constituer un moyen de limiter, voire de supprimer tant les atteintes à la vie privée que la captation de données personnelles par les drones, ces dernières pouvant être grossièrement définies, comme des « données non anonymes ». Insistons sur le fait qu'à l'ère du numérique, ces deux domaines sont poreux entre eux.

Le concept de Privacy by Design (ou de protection de la vie privée dès la conception) impose aux entreprises de mettre en œuvre des mesures de protection dès la conception et lors de chaque utilisation de nouvelles technologies. Il concerne donc potentiellement aussi bien les centres de R&D, les fabricants, que les opérateurs de drones. Le concept a été développé dans les années 1990 au Canada, sous l'impulsion d'Ann Cavoukian, alors commissaire à l'information et à la protection de la vie privée de l'Ontario (Canada). Sa proposition visait à agir en amont du développement d'une technologie afin que celle-ci ne porte pas atteinte à la vie privée des individus. Il en découle sept principes : 1/ la proactivité (et non la simple réactivité), 2/ la protection de la vie privée par défaut (même en l'absence d'intention des particuliers visés), 3/ l'intégration de la protection de la vie privée dans la conception des systèmes, 4/ la conciliation des intérêts des utilisateurs avec ceux de la société (avec une collecte des données proportionnée à l'objectif poursuivi), 5/ la protection de bout en bout, pendant toute la période de conservation des données, 6/ la visibilité et la transparence sous la supervision d'un DPO (Data Protection Officer, successeur du conseiller Informatique et Libertés) dans l'entreprise, 7/ le respect de la vie privée des utilisateurs et la protection accrue des données personnelles.

L'idée d'une protection préventive a notamment été plébiscitée internationalement en 2010. Elle a également été consacrée à l'article 25 du Règlement général sur la protection des données personnelles, adopté le 27 avril 2016 (règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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 »).

PROTECTION DES DONNÉES.

A l'horizon 2018, le Règlement harmonisera les mesures concernant la protection des données entre tous les pays de l'Union européenne, obligeant les entreprises à revoir leur système d'information et leur usage d'Internet pour se mettre en conformité avec la nouvelle réglementation, sous peine de lourdes sanctions.

Dans un article du 18 octobre 2016, le journal « La Tribune » écrivait que « 96 % des entreprises des trois principales économies européennes (France, Allemagne, Royaume-Uni) ne comprennent pas encore clairement le Règlement général sur la protection des données (RGPD) (…) Selon une étude plus récente de la société de sécurité informatique Symantec, 92 % des dirigeants et décideurs français s'inquiètent de ne pas être en conformité au moment de l'entrée en vigueur de la RGPD » !

Ce règlement européen, qui entrera précisément en application le 24 mai 2018, prévoit l'obligation de mettre en œuvre des « mesures techniques et opérationnelles appropriées » afin de protéger les droits des personnes et de mettre en œuvre les principes relatifs à la protection des données. Cela signifie que les acteurs de la filière drone devront non seulement acheter ou

concevoir des drones qui prennent en compte cette question, planifier leurs missions dans cet état d'esprit, mais aussi adopter une organisation qui permette une protection maximisée des tiers et de leurs données.

Concrètement, la mise en œuvre du Privacy by Design dans le secteur des drones pourrait se faire via différentes mesures telles que la limitation du volume des données traitées, la restriction de la conservation puis de l'accès aux données enregistrées, le floutage ponctuel de visages ou de plaques d'immatriculation de véhicules sans lien avec la mission, l'adaptation des technologies embarquées sur les drones, ou encore par l'intégration de systèmes de cryptage des communications sol/air et de sécurisation des données. Les dronistes pourraient également se tourner vers l'Edge Computing, pratique consistant à traiter le plus de données possible directement sur l'appareil plutôt que de les transférer vers un support externe ou un serveur distant. Plus classiquement, des mesures d'anonymisation ou de pseudonymisation devront enfin être envisagées par les acteurs de la filière. Les opérateurs pourront également jouer sur l'orientation de la caméra ou la définition des points de passage lors d'une mission pour réduire le champ des données collectées.

Ces mesures devront être mises en œuvre en fonction « de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques, dont le degré de probabilité et de gravité varie ». Cette disposition devrait permettre de mettre en balance les intérêts de l'entreprise avec ceux des personnes, de manière à ce que l'innovation ne soit pas freinée.

QUESTIONS EN SUSPENS.

De nombreuses questions restent cependant en suspens : quelles sont les entreprises soumises à ce principe ? quelles sont plus précisément les technologies touchées ? comment concrètement mettre ce principe en œuvre ? quelle formation dispenser au sein des entreprises ?

Il semble néanmoins important pour la filière du drone de s'imprégner du principe de « Privacy by Design » afin de lever certains freins à l'acceptation sociale des drones, mais aussi de conquérir la confiance de ses (futurs) clients professionnels, qui souhaiteront voir leur exposition juridique limitée.

Rappelons ensuite que le règlement 2016 est d'application directe et s'imposera immédiatement aux Etats membres de l'Union européenne à compter du 25 mai 2018, sans qu'il soit besoin de le transposer dans les législations nationales (contrairement à une directive européenne).

Mai 2018, c'est demain. Il appartient donc aux fabricants de drones (et d'autres objets connectés), aux entreprises et administrations utilisatrices de drones de se préparer rapidement, d'autant que leurs obligations se sont considérablement renforcées, tout comme les sanctions prévues en cas de manquements. En effet, en cas de non-respect du dispositif, les entreprises s'exposeront à des amendes d'un montant allant de 2 à 4 % du chiffre d'affaires mondial et pouvant représenter jusqu'à 20 M€ pour les infractions les plus graves !

Parmi les « préparatifs » nécessaires, on peut songer à un état des lieux des traitements (inventaire, cartographie des flux de données…), des audits, et l'établissement des registres de ces traitements devra être réalisé, tout comme la mise en place de règles de conduite (chartes de conduite, procédures relatives à la vie privée et à la sécurité des données, programmes de formation ou de sensibilisation) ou la révision des clauses contractuelles portant sur l'information et le consentement préalables des personnes dont les données sont collectées. ■