

## Maître Bensoussan répond à vos questions



*De nos jours, la vidéoprotection est l'un des moyens les plus demandés dans le domaine de la sécurité. Les caméras sont souvent à la une des médias, mais de plus en plus de robots mobiles pilotables à distance apparaissent sur le marché. M<sup>e</sup> Alain Bensoussan fait un point juridique sur le mariage "Vidéoprotection et robots".*

**Quels problèmes légaux peut soulever l'utilisation de robots mobiles pilotables ?**

**Existe-t-il une réglementation spécifique ?**

Le terme "robot mobile" n'est pas vraiment approprié bien que ce soit la terminologie couramment employée. Mieux vaut faire la distinction entre deux notions et la vidéoprotection me paraît relever davantage de la première que de la seconde. En effet, il convient de distinguer les automates équipés de capteurs intelligents des robots qui sont des machines avec capteurs sensoriels capables de prendre une décision en autonomie par rapport à leur environnement et aux processus qui ont été programmés.

A la différence des automates, les robots décideurs à capteurs sensoriels ne sont pas programmés pour accomplir des processus répétitifs ou réagir à une suite d'événements prédéfinis (machine avec une intelligence programmée). Ce n'est qu'au titre d'un processus, même réduit, que l'on peut parler "d'intelligence artificielle" et de "robot".

Si effectivement l'équipement obéit à des éléments préprogrammés, il vaut mieux utiliser le terme d'automate que celui de robot.

Il est intéressant de s'arrêter également sur le terme "mobile". La notion de mobilité s'évalue à deux niveaux : l'automate (la caméra) est capable d'avoir un champ d'action plus ou moins large à 360° par rapport à un point fixe et il peut se déplacer non pas sur son point fixe (caméra 360°) mais être piloté (le point fixe est déplacé). La différence est importante car si l'on veut structurer le Droit il faut d'abord structurer l'objet.

Le terme "pilotable" a également son importance. Si l'on prend le cas d'un robot domestique de téléassistance, on peut, par exemple, faire une "levée de doute vidéo" en déplaçant la caméra par un pilotage à distance pour savoir si une personne est réellement en danger (malaise, chute, etc.) – auquel cas une intervention directe sera déclenchée – ou si elle a simplement enlevé ou débranché son appareil de contrôle.

Bien qu'il n'y ait pas de cadre juridique spécifique pour ce type d'usage en France, ces robots mobiles pilotables à distance sont néanmoins soumis aux mêmes contraintes réglementaires que les systèmes de vidéoprotection (notamment le masquage des zones privées) car ils peuvent capter et diffuser des données personnelles.

En fait, il n'existe pas de réglementation particulière. Il s'agit d'un empilement de réglementations. Lorsqu'un drone, par exemple, va intégrer une caméra, on va appliquer le droit des drones qui est l'article D. 133-10 du Code de l'aviation civile relatif à la prise de vue aérienne et l'arrêté du 11 avril 2012 qui encadre les activités de télépilotage de drones à usage civil. Il n'y a donc pas de zone de non droit mais une zone d'empilement des droits.

**Comment protéger les citoyens à l'heure où les robots domestiques, médicaux ou de sécurité collectent et manipulent de nombreuses données personnelles ? Ce problème peut-il constituer selon vous un blocage majeur pour le développement de la robotique ?**

Il est effectivement temps de créer un droit des robots. Les robots sont aujourd'hui capables de mémoriser des éléments intimes de la vie des individus. Imaginez une personne âgée ou dépendante disposant d'un robot d'assistance médicalisée qui lui rappelle ses prises de médica-

ments. Ces données sont très intimes car elles recèlent des renseignements sur sa santé qui, s'ils étaient dévoilés, pourraient porter atteinte à sa dignité. Il faut donc protéger les utilisateurs des robots, mais également les robots en tant que tels car ils peuvent, à la différence des ordinateurs, déduire des données qui n'ont pas forcément été enregistrées par une précollecte.

Le droit ici est en retard. Les robots d'assistance médicalisée nécessitent une réglementation adaptée au traitement des données médicales, économiques et à l'interaction des robots avec l'être humain. Le rôle du droit est déterminant dans le développement d'une technologie : il peut être un frein ou un accélérateur.

Imaginons un robot équipé d'une caméra de vidéoprotection couplée à une technique biométrique de type reconnaissance faciale. Cette caméra pourrait être connectée à l'application Facebook de reconnaissance faciale qui permet de retrouver une personne et de l'identifier si elle a été taggée. Le détenteur d'une telle caméra – disponible dans le commerce dès l'âge de 13 ans – pourrait ainsi constituer un véritable fichier d'identité à l'instar de ceux tenus par les services de police...

**Les robots posent également la question de la protection des données sensibles contre le piratage ou la malveillance. Comment encadrer le développement de ces malveillances ?**

La loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite "Loi Godfrain", s'applique sans aucun doute à un robot qui n'est pas autre chose qu'un système de traitement automatisé de données au sens légal, comme le serait une caméra intelligente. Toute pratique d'accès, de maintien, de manipulation ou de détournement de données est aujourd'hui passible de peines de prison. Il n'y a aucun déficit juridique en ce domaine.

A titre d'exemple, si un système de vidéoprotection a été installé conformément au Code de la sécurité intérieure, en respectant les zones privatives notamment par masquage, une intervention illicite qui désactiverait ces zones de masquage nonobstant les règles touchant à la vie privée, serait passible de l'ensemble des sanctions pénales (prison et amende) applicables en matière de fraude informatique. Il s'agit des articles 323-1 à 323-7 du Code pénal.

**Les mini-drones ou robots aériens sans pilote équipés de caméra mobile, capteur sonore et dispositif de géolocalisation sont en concurrence directe avec la vidéosurveillance et plus généralement la télésurveillance à une différence majeure : ils se déplacent et effectuent parfois des actions qui peuvent poser des problèmes de responsabilité en cas d'accidents ou de blessures involontaires. Quelles règles peuvent alors s'appliquer ?**

Aujourd'hui, les drones civils avec multicaméras embarquées posent un vrai défi pour le respect de la vie privée sachant qu'elles ont un niveau de résolution capable de discerner à partir de 100 à 200 mètres d'altitude, des objets de quelques centimètres. La législation devra donc être renforcée. Les personnes qui utilisent des drones pour télésurveiller des zones privées sont responsables de la violation de la vie privée.

Par ailleurs, indépendamment des infractions liées à l'atteinte à la vie privée, la loi Informatique et libertés et Les droits de l'homme numérique trouvent leur légitimité à s'appliquer. Les personnes qui porteraient atteinte à la vie privée à l'aide de drones seraient considérées comme procédant à des collectes illicites et frauduleuses d'informations dès lors que la personne est identifiable. En revanche, la loi Informatique et libertés ne s'applique pas à des zones dans lesquelles aucune donnée à caractère personnel n'est collectée ou traitée.

Il est clair que la législation sur les drones apparaît pour l'instant beaucoup trop timide au regard des risques liberticides envisageables. Car, à partir du moment où toute personne peut acheter un drone avec caméra embarquée, les risques sont démultipliés. Il faudra nécessairement encadrer l'utilisation de ces produits afin de protéger l'intimité de la vie privée.