HoloLens, l’ordinateur du futur ? | Le Net Expert Informatique

HoloLens, l’ordinateur du futur ?

Le projet « Windows Holographic », avec son masque HoloLens, permettra de manipuler des objets virtuels dans un environnement réel.Microsoft assure que ce dispositif ambitieux préfigure « l’ordinateur du futur ».

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d’entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.01net.com/editorial/642445/hololens-lordinateur-du-futur-video-du-jour/

L’immatriculation des drones bientôt obligatoire ? | Le

Net Expert Informatique

	L'immatriculation des #drones bientôt obligatoire ?

Les propriétaires de drones de loisir seront-ils bientôt obligés d'immatriculer leur appareil, de la même manière que lorsqu'ils achètent une voiture ou une moto ? C'est en tout cas l'une des idées intéressant actuellement le gouvernement, parmi bien d'autres.

Même si les drones ont un peu moins défrayé la chronique des faits divers ces derniers jours, les pouvoirs publics continuent d'examiner les solutions qui permettraient de mieux lutter contre les survols illicites (de centrales, de sites sensibles, d'espaces urbains…). Interrogé en décembre dernier par le député Patrice Verchère, le ministre de l'Intérieur vient de présenter plusieurs de ses pistes de réforme au travers d'une réponse écrite parue mardi au Journal officiel.

Vers un durcissement des sanctions

« La dissuasion des usages malveillants de drones civils peut être renforcée par un durcissement de la législation » expose d'entrée Bernard Cazeneuve. Comment ? « En rendant possible le prononcé d'une peine complémentaire de confiscation, soit par une augmentation du quantum des peines encourues dans le titre III du livre II de la VIème partie du code des transports, soit par l'insertion dans ce code d'un nouvel article le prévoyant. » En clair, les sanctions administratives et pénales prévues en cas de violation de la réglementation pourraient être relevées. Même si le nombre d'infractions possibles est actuellement assez vaste, on retient habituellement que l'article L6232-4 du Code des transports punit d'un an d'emprisonnement et de 75 000 euros d'amende le fait de ne pas respecter les règles de sécurité applicables aux drones (interdiction de voler de nuit, au-dessus de personnes, etc.).

Cazeneuve pose une option sur l'immatriculation obligatoire des drones

Le « premier flic de France » affirme ensuite qu'une immatriculation des drones « est également une option ». L'exécutif songe en effet à transposer l'obligation qui pèse actuellement sur tous les propriétaires d'aéronefs civils (ULM, planeurs…). Une formalité administrative qui coûte 91 euros. « Il convient d'en évaluer préalablement les conséquences, particulièrement en termes de gestion de fichier qui en découlerait » temporise néanmoins Bernard Cazeneuve.

Mieux détecter et neutraliser certains drones

« Au titre de la réponse capacitaire et juridique aux drones malveillants, l'identification électronique des drones en vol à l'aide de signaux émis, facilitant leur détection, est en outre un axe de travail susceptible de donner lieu à une mesure législative » ajoute le ministre de l'Intérieur. Avant de poursuivre : « Il en est de même de l'insertion dans les logiciels de vols des drones civils, fabriqués et utilisés en France, de zones interdites de survol. » Derrière ces mots, on comprend que l'exécutif envisage de doter les drones français de sortes de GPS qui permettraient d'une part de les repérer dès lors qu'ils approchent d'une zone sensible, voire carrément de les mettre en « panne volontaire » s'ils y pénètrent.

Enfin, dans un tout autre registre, le locataire de la Place Beauvau indique que la mise en place d'un « régime d'assurance obligatoire pour les usages de drones à des fins de loisirs » est actuellement « à l'étude ».

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.nextinpact.com/news/93584-limmatriculation-drones-bientot-obligatoire.htm

L’attaque des réfrigérateurs connectés a commencé ! | Le Net Expert Informatique

L’attaque des réfrigérateurs connectés a commencé !

D’apparence si inoffensive avec leurs façades remplies d’aimants, de cartes postales, de photos et de dessins d’enfants, les réfrigérateurs se sont pourtant dotés récemment d’une potentielle arme : un accès à Internet. Et c’est exactement ce qui est arrivé. Un réfrigérateur a été embrigadé dans un vaste botnet.

Un botnet est un réseau de programmes connectés à Internet servant différents desseins. Souvent, ils sont mis en place et utilisés par des hackers pour mener de vastes opérations d’attaque et/ou de piratage. Selon le spécialiste de la sécurité informatique Proofpoint, pareille attaque a eu lieu entre le 23 Décembre et le 6 Janvier. Plus de 100 000 appareils ont été « réquisitionnés », dont des routeurs, des stations multimédias, des téléviseurs et au moins un réfrigérateur.
Cette attaque aura permis d’envoyer plus de 750 000 emails de spam, par vagues de 100 000, trois fois par jour. Une même adresse IP n’envoyait alors pas plus de 10 emails, rendant la chose très délicate à bloquer. C’est la première fois qu’une cyberattaque de ce genre – faisant participer des appareils si communs – est recensée.
Et comme il fallait s’en douter, si les pirates ont pu utiliser ces machines, ce n’est pas parce qu’ils ont utilisé des moyens sophistiqués mais davantage parce que les mots de passe n’avaient pas été changé ou parce qu’ils étaient branchés sur des réseaux publics.
Comme le rappelle David Knight de Proofpoint : « la plupart de ces appareils sont très peu protégés, au mieux, et les consommateurs n’ont virtuellement aucun moyen de détecter ni de réparer la moindre infection le cas échéant. » Et dire que ces objets connectés seront au nombre de 200 millions d’ici 2020… Le terrain de jeu des hackers s’agrandit sensiblement !

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d’entreprise.
Contactez-nous

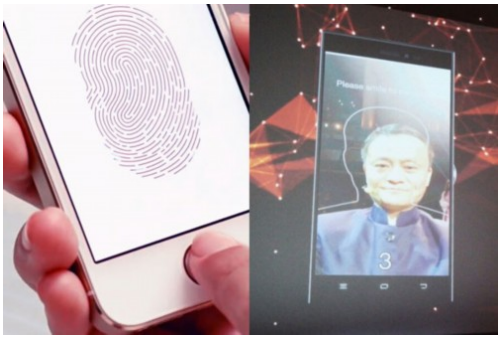
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.gizmodo.fr/2015/03/24/attaque-refrigerateurs-botnet.html

---

Alibaba va lancer un service

de paiement facial mobile plus sûr | Le Net Expert Informatique

	**Alibaba va lancer un service de paiement facial mobile plus sûr**

Selon une nouvelle publiée le 16 mars par la chaine d'informations financières américaine CNBC, le géant du commerce électronique chinois Alibaba développe actuellement une technologie de « paiement facial », qui permettra l'authentification de l'identité de l'utilisateur grâce à son smartphone qui scannera le visage de celui-ci, ce qui permettra d'assurer des paiements en ligne et des paiements mobiles plus sûrs.

Le système humain de scannage du visage, appelé « Smile and Pay », développé par une filiale d'Alibaba, Ant Financial Services Group, et qui servira pour les paiements en ligne et l'utilisation d'Alipay Wallet, est entré en phase de tests. Mais lors de la cérémonie d'ouverture du salon de l'électronique CeBIT de Hanovre, en Allemagne, le PDG d'Alibaba Jack Ma, a lors de son discours, fait une démonstration de la technologie de paiement facial. Après évoqué les divers problèmes que l'on peut rencontrer lors du paiement en ligne, comme l'oubli du mot de passe, il a utilisé cette technologie de paiement facial devant son auditoire pour acheter un timbre commémoratif du CeBIT de Hanovre.
Selon les données du cabinet de recherche Juniper Research Ltd, en 2019, le volume annuel des paiements en ligne et des paiements mobiles atteindra 4 700 milliards de Dollars US, ce qui fait que les autres entreprises tentent de développer ce service, ainsi d'Apple qui a lancé son service Apple Pay l'année dernière, et Samsung qui a présenté le mois dernier son service Samsung Pay.
Les développeurs de services de paiement mobiles s'efforcent tous de trouver des moyens de payer de façon plus sûre par le biais de technologies d'authentification d'identité. Les iPhone d'Apple utilisent déjà l'identification par empreintes digitales, et le mois dernier, lors du Mobile World Congress, certains fabricants ont présenté une technologie d'identification par scannage oculaire.
De son côté, Alibaba travaille également sur de nouvelles technologies d'identification, ce qui, selon un porte-parole, pourrait peut-être passer par le développement d'une technologie qui permettra aux clients de s'identifier en prononçant une expression particulière, ou même une autre approche appelée « Kung Fu », qui permettra d'identifier un animal domestique en scannant un tatouage.
En outre, le système « Smile to Pay » sera d'abord lancé en Chine, mais, a précisé le porte-parole, la date exacte reste encore incertaine ; il sera ensuite peut-être lancé dans d'autres pays.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://french.peopledaily.com.cn/n/2015/0323/c31357-8867317.html

Quelle réponse face aux survols illicites de drones ? | Le Net Expert Informatique

	Quelle réponse face aux survols illicites de drones ?

La multiplication de vols de drones inconnus et leur médiatisation inquiètent une filière française dont la croissance a été favorisée par l'existence d'une réglementation jusque-là assez libérale.

D'objet sympathique, le drone est presque devenu l'ennemi public numéro un depuis quelques semaines, face à la multiplication de vols aussi illicites que mystérieux. Une mini-psychose qui touche une partie de la population d'abord, certains imaginant déjà ces mini-appareils sans pilote se transformer en nouvelles armes aux mains de terroristes. Chez les policiers et les gendarmes ensuite, qui n'ont jusqu'à présent arrêté aucun responsable des soixante vols recensés. La médiatisation du phénomène inquiète enfin une filière en pleine croissance qui avait jusqu'alors bénéficié de la compréhension d'une administration plutôt bienveillante.

Depuis avril 2012, en effet, une réglementation assez libérale encadre l'utilisation des drones. Fruit d'une concertation entre la Direction générale de l'aviation civile et les professionnels, celle-ci comprend quatre scénarios d'utilisation. Tous imposent une altitude inférieure à 150 mètres mais autorisent, dans certains cas, le vol en dehors du champ de vision du pilote. Jusqu'à 1 kilomètre et même « hors vue » sur plusieurs dizaines de kilomètres dans certains cas. Dotée d'un cadre légal solide, la filière a connu un véritable boom avec une cinquantaine de constructeurs de drones et, surtout, 1.300 sociétés de services enregistrées auprès de la DGAC. Celle-ci imposant la constitution d'un dossier, inspiré de celui de l'aviation, détaillant le type de drone utilisé, la qualification des pilotes, les procédures mises en place… La Fédération professionnelle des drones civils (FPDC) revendique 300 membres et en espère 500 d'ici à la fin de l'année. Et estime à 3.000 le nombre d'emplois créés par la filière. C'est justement cette dynamique que les professionnels craignent de voir freinée par des pouvoirs publics susceptibles de réagir aux événements actuels en durcissant la réglementation. « Une hypothèse toutefois peu fondée puisque l'administration fait bien la différence entre une filière qui travaille dans le cadre réglementaire et les auteurs de ces actes irresponsables », relativise Emmanuel de Maistre, fondateur de la Fédération professionnelle des drones civils.

L'autre risque étant que l'opinion publique bascule et pousse les pouvoirs publics à plus de sévérité. Même si, en parallèle, le grand public semble avoir déjà adopté le drone. A lui seul, Parrot, l'un des principaux acteurs du marché du drone de loisirs, a déjà vendu près de 1 million d'appareils en quatre ans.

Les professionnels montent au créneau, en rappelant que ces dernières années des milliers de vols se sont déroulés sans incident. Il reste qu'un drone n'est pas un objet anodin et qu'il engendre des risques : blessure en cas de choc ou de chute, perturbation du trafic aérien, distraction des automobilistes… Une soixantaine d'enquêtes judiciaires ont d'ailleurs été menées depuis trois ans, dont six se sont soldées par une confiscation du matériel et deux par des peines de prison avec sursis. L'une pour un drone qui s'était écrasé sur la piste de l'aéroport de Montpellier et l'autre à l'occasion de l'échouage d'un paquebot sur une plage de Bayonne. Le propriétaire avait voulu filmer le navire, entravant du même coup les opérations de sauvetage. Et si en France la police n'a jamais enregistré d'accident, on l'a parfois frôlé. A l'image de ce qui s'est passé en Catalogne en 2013, lorsqu'un drone de plusieurs kilos qui filmait des festivités est tombé de 30 mètres de haut à quelques centimètres d'une petite fille.

Les drones vont de toute façon voir le paysage changer. Impuissant depuis les premiers survols de sites sensibles, notamment des centrales nucléaires, l'Etat ne compte plus se laisser faire. Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) a été mandaté par le Premier ministre pour évaluer la menace et organiser la riposte « à moyen et long terme ». Les pistes sont d'abord réglementaires : immatriculation, enregistrement des drones, obligation de s'assurer.

Dans le domaine du drone de loisirs, pourquoi ne pas rendre obligatoire la note très bien faite de la DGAC recensant les 10 commandements pour l'usage d'un drone en France ? Les pistes sont aussi techniques avec la possibilité de les doter de puce d'identification ou de transpondeur, pour les rendre détectables. Même si ces dispositifs peuvent être contournés. « La grande mode étant désormais de fabriquer son drone en kit à partir de pièces achetées sur Internet », constate un spécialiste de la lutte contre les drones illicites. Dès lors, le SGDSN a aussi pour mission d'évaluer des dispositifs techniques, pour neutraliser les drones ou protéger les sites sensibles. Des technologies existent : brouillage du signal GPS, radars actifs ou passifs, voire laser ou canons à eau. « Aucune solution ne semble disponible immédiatement même si des industriels assurent en avoir », indique le SGDSN. Pour vérifier leurs dires, une série d'expérimentations sont déjà en cours avec l'appui technique du centre français de recherche aérospatiale (l'Onera). Le SGDSN a voulu aller plus loin en allouant 1 million d'euros à la recherche. Quelque 23 entreprises ont ainsi répondu à un appel à projets « Protection de zones sensibles vis-à-vis des drones aériens » lancé par l'Agence nationale de la recherche. Les candidats devraient être choisis ces jours-ci et se voir financer pour des projets sur dix-huit mois au maximum.

La réglementation va également évoluer à l'échelon européen. La Commission européenne s'en préoccupe et vient de réunir tous les acteurs la semaine dernière en Lettonie. L'objectif étant de réfléchir à une uniformisation des pratiques, très différentes d'un pays à l'autre. Avant cela la DGAC devrait encore faire évoluer la réglementation française. Avec pour l'instant des pouvoirs publics qui semblent prudents. « On ne veut pas faire abstraction de la filière et nuire à son développement », entend-on aussi bien au SGDSN qu'à la Gendarmerie des transports aériens (GTA).

Les points à retenir

Face à la multiplication des vols illégaux de drones, le Premier ministre a chargé le Secrétariat général de la défense et de la sécurité nationale d'évaluer la menace et d'organiser la riposte.

Les pistes sont d'abord réglementaires : immatriculation, enregistrement des drones, obligation de s'assurer.

Mais les réponses sont aussi techniques avec la possibilité de les doter de puce d'identification ou de transpondeur, pour les rendre détectables.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesechos.fr/idees-debats/editos-analyses/0204206144122-quelle-reponse-face-aux-vols-illicites-de-drones-1100859.php
Par Frank Niedercorn Journaliste au sein du service Prospective des « Echos »

Les experts de la sécurité se penchent sur la Watch d'Apple | Le Net Expert Informatique

Les experts de la sécurité se penchent sur la Watch d'Apple

La firme de Cupertino a donc lancé officiellement sa montre connectée, la Watch, le 9 mars 2015 hier soir. Tout a été dit sur ce gadget déclinable en plusieurs versions dont une luxueuse au prix stratosphérique de 11 000 euros. Mais cette annonce a aiguisé la curiosité des experts en sécurité qui se sont penchés sur les faiblesses de la tocante numérique.

Nos confrères de The Register ont interrogé plusieurs spécialistes de la sécurité sur ce sujet. Ainsi, Ken Westin, chercheur chez Tripwire a indiqué que « le fait que le dispositif soit à la fois WiFi et Bluetooth va faciliter le développement des fonctionnalités supplémentaires à la montre et de s'interopérer avec d'autres équipements. Mais cela va également augmenter la surface d'attaque de l'appareil ». Pour lui, il ne fait aucun doute que « les chercheurs et les hackers ont été émoustillés pour trouver de nouvelles vulnérabilités et s'appuyer sur des attaques existantes qui profitent des faiblesses du WiFi et du Bluetooth ».

Problème de confidentialité des données
Un autre aspect de sécurité selon l'expert réside dans la confidentialité des données. « Avec ces connectivités, il sera intéressant de voir comment les données peuvent être utilisées pour suivre les personnes dans espaces physiques. Cela peut avoir un impact pour un cyberattaquant, tout comme pour des campagnes publicitaires trop ciblés ». L'arrivée d'applications tierces n'est pas faite pour rassurer le spécialiste qui y voit un risque supplémentaire pour la sécurité et la vie privée.

La fraude au paiement
En disposant d'une capacité NFC, l'Apple Watch peut servir pour le paiement mobile. Les risques de fraudes existent donc. Une récente étude de Drop Labs montre que le niveau de fraude sur les paiements avec Apple Pay est de 6% contre 1% en moyenne pour les transactions par carte bancaire. Pour la défense d'Apple, le problème vient surtout d'un niveau d'authentification faible de la part des banques. Une affaire récente a démontré ce risque. Certains spécialistes s'interrogent sur la fiabilité de la technologie NFC avec la capacité de la contourner.

Une révision des politiques de BYOD ?
Phil Barnett, directeur général EMEA de Good Technology, préfère souligner les menaces que les montres connectées et plus généralement les « wearables technology » impliquent dans le monde du travail. Elles s'inscrivent dans les politiques de BYOD (Bring Your Own Device) qui selon lui doivent être révisées. « Le BYOD a déjà connu les smartphones et des tablettes, les accessoires connectés arrivent comme les prochains véhicules de la donnée. Ils représentent une immense opportunité pour la productivité, mais ils nécessitent avant leur arrivée en entreprise de les sécuriser. »
Cela passe pour lui par plusieurs axes : « Chiffrement des données transitant sur le Bluetooth et la conteneurisation des données de l'entreprise. Par ailleurs, un contrôle plus granulaire des politiques de sécurité devrait permettre de trouver un équilibre entre risques et productivité. » A condition qu'il n'y ait pas de défaut dans la cuirasse, comme le montre la faille Freak qui affaiblissait le chiffrement des navigateurs Apple et Android. La firme de Cupertino vient d'ailleurs de publier iOS 8.2 qui règle ce problème.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.silicon.fr/les-experts-de-la-securite-se-penchent-sur-la-watch-dapple-110567.html

« Aux mains d’une personne malveillante, l’utilisation d’un drone peut constituer un risque réel » | Le Net Expert Informatique

« Aux mains d’une personne malveillante, l’utilisation d’un drone peut constituer un risque réel »

Y a-t-il différentes bandes de fréquence utilisées en fonction du type ou de la taille du drone ?

Sur les drones civils, à ma connaissance, il n’y a qu’une seule bande de fréquence. Ce n’est pas le cas pour les drones militaires. Mais ceux qui ont survolé Paris à plusieurs reprises rentrent tous dans la catégorie des drones civils.

Y aurait-il par conséquent un risque d’interférences avec d’autres secteurs d’activité (aviation, GPS ou autres) ?
Il y a toujours des risques d’interférences possibles, comme le brouillage des antennes de télévisions. Il y a aussi un risque de perdre le contrôle du drone en cas de champ magnétique ou de fréquence assez forte.

Est-il possible pour un service sécuritaire étatique de contrôler un drone et de le dévier de sa trajectoire, en plein vol, au cas où il constituerait un danger?
Pour l’instant, non. On pourrait leur interdire via un GPS de rentrer dans certaines zones, une sorte de « no fly zone ». Si la démarche pouvait être contournée par de bons ingénieurs en électronique ou en informatique, elle aurait au moins le mérite de limiter les risques. Aujourd’hui, on a plutôt à faire à des gens qui sont là pour provoquer, mais aux mains d’une personne malveillante, cela peut constituer un risque réel. Cela dit, les hélicoptères électriques qui peuvent supporter une charge plus lourde que les drones sont sur le marché depuis déjà 30 ans et n’ont jusqu’à présent jamais servi à commettre un attentat.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d’entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.lorientlejour.com/article/914452/-aux-mains-dune-personne-malveillante-lutilisation-dun-drone-peut-constituer-un-risque-reel-.html

Réglementation des drones et droit des robots | Le Net Expert Informatique

source : http://live.orange.com/drones-parrot-amazon-zephyr/

Réglementation des drones et #droit des robots

Le survol des drones au dessus des centrales nucléaires [1] ainsi que d'autres sites sensibles et parisiens [2] représente une menace face à laquelle les réponses, notamment réglementaires, semblent encore insuffisantes.

En effet, la détection par radar militaire mais également l'interception de ces engins volants se révèlent difficiles de par la furtivité des drones et l'incapacité actuelle des autorités à les tracer et à les écarter.

Au niveau réglementaire, l'utilisation des drones ou plus exactement d' « aéronefs qui circulent sans monde à bord » civils, à distinguer des drones militaires, est encadrée par deux arrêtés d'avril 2012 [3], un arrêté relatif aux conditions de navigabilité et de télépilotage et un autre relatif aux exigences liées à l'espace aérien.

Le principe est le suivant :
sauf autorisation particulière, les drones doivent survoler un espace bien précis délimité en volume et en temps, en dehors de toute zone peuplée. De plus, en fonction de deux catégories de critères (finalité d'utilisation et poids du drone), des règles particulières s'appliquent. Ainsi, les drones civils professionnels utilisés par exemple par les agriculteurs ou les photographes doivent notamment se faire connaître auprès des autorités.
Concernant l'utilisation de drone de loisirs qui est en vente libre, il faut également respecter des règles spécifiques qui sont rappelées dans une notice rédigée par la Direction Générale de l'Aviation Civile (DGAC) en décembre 2014 [4] et qui interdisent notamment le vol de nuit, le survol des sites sensibles ainsi que de l'espace public en agglomération.
Au final, la violation des conditions d'utilisation des drones est passible d'un an d'emprisonnement et de 75000 euros d'amende en vertu de l'article L.6232-4 du code des transports.
Autre point d'importance à souligner, même si la prise de vue aérienne est réglementée par l'article D. 133-10 du code de l'aviation civile, il n'en demeure pas moins que la captation et l'enregistrement d'images relatives aux personnes relèvent également de la loi « Informatique et Libertés »[5].
En effet, il est important de souligner également le risque de collecte de données à caractère personnel par les drones. Un facile parallèle peut être établi entre le survol des drones et le passage dans nos rues des « Google cars ». La CNIL avait constaté lors de contrôles effectués fin 2009 et début 2010 que la société Google, via le déploiement de véhicules enregistrant des vues panoramiques des lieux parcourus, récoltait, en plus de photographies, des données transitant par les réseaux sans fil Wi-Fi de particuliers, et ce à l'insu des personnes concernées. Cette collecte déloyale de très nombreux points d'accès Wi-Fi constitue un réel manquement à la loi « Informatique et Libertés ».
Concernant les drones, il faudra donc s'attacher à vérifier qu'ils ne récupèrent pas également des données à caractère personnelle de façon illégale. En effet, les drones sont des machines qui peuvent embarquer une quantité importante de capteurs divers et variés tels un appareil photo, une caméra ou un dispositif de géolocalisation permettant de collecter et diffuser des données à caractère personnel avec pour conséquence l'atteinte manifeste à la vie privée des individus.
Consciente de ces enjeux depuis 2012, la CNIL, en liaison avec le Groupe des 29 CNIL européennes (G29) réfléchit activement à l'amélioration de la réglementation à ce sujet.

Au final, la réglementation relative aux drones qui, d'une part, a le mérite d'exister et, d'autre part, est relativement souple et adaptable en prévoyant plusieurs scénarii spécifiques, apparaît même novatrice au niveau international. Les Etats Unis par l'intermédiaire de la Federal Aviation Association (FAA) n'ont dévoilé que le 15 février 2015 et pour la première fois des recommandations pour encadrer l'utilisation des drones civils commerciaux sur le sol américain [6].
Toutefois, la DGAC a prévu quand même de réviser prochainement la réglementation des drones afin de mieux prendre en compte la massification de l'utilisation de drones civils. Cette révision devra si possible prendre en compte une future réglementation européenne à ce sujet.

Plus largement, ce focus juridique sur les drones peut élargir son horizon en s'intéressant à la problématique du droit des robots qui, au regard de la vitesse de création des inventions technologiques, constitue indéniablement un des enjeux majeurs juridiques mais également éthiques des années à venir.
Certes pour les objets connectés, les enjeux juridiques ont déjà été identifiés mais il semble qu'il faille pousser le cadre juridique plus loin pour les futures générations de robot doté d'une certaine forme d'intelligence artificielle.
La vente du robot, comme tout bien, entraine pour le vendeur une obligation de garantie et engage sa responsabilité délictuelle du fait d'un défaut de sécurité de l'un de ses produits ou services entraînant un dommage à une personne. Cependant, il est probable que l'autonomie des robots grandissante, il faille réfléchir à la responsabilité propre du robot. De prime abord, la responsabilité juridique repose sur la notion de discernement, actuellement les machines restent sous la responsabilité de son gardien soit de l'usager ou encore de son fabricant par le biais de la responsabilité des produits défectueux.
Il est possible que, dans un futur plus ou moins proche, le législateur décide de mettre en place une personnalité juridique spécifique du robot. Cette dernière, se distinguant du régime juridique lié aux animaux et des biens, devra être encadrée afin de prévoir la sécurité des utilisateurs mais également la sécurité du robot lui-même. Pour commencer, il pourrait même s'agir de la reprise des trois règles de la robotique édictée par Isaac Asimov [7]!

[1] Dix-sept centrales nucléaires sur les dix-neuf que compte le parc français ont été survolées par des drones depuis début octobre. Six l'ont été simultanément dans la nuit du 31 octobre.
[2] http://www.liberation.fr/societe/2015/02/24/paris-survole-par-des-ovnis_1209273
[3]Les arrêtés du 11 avril 2012 relatifs d'une part à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord et d'autre part 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 constituent le socle réglementaire d'utilisation des drones civils.
[4] Règles d'usage d'un drone de loisir : http://www.developpement-durable.gouv.fr/IMG/pdf/Drone-_Notice_securite-2.pdf
[5] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.
[6] « Drones civils – les Etats-Unis avancent sur leur législation : les différences avec le modèle français » par Emmanuel de Maistre, président de Redbird : http://www.infodsi.com/articles/154099/drones-civils-etats-unis-avancent-legislation-differences-modele-francais-emmanuel-maistre-president-redbird.html?key=a0a42d0bc78aa63d
[7] http://nte.mines-albi.fr/SystemiqueSudoku/co/v_regle_vie_Azimov.html

---

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://securitedessystemesjuridiques.blogspot.fr/2015/03/reglementation-des-drones-et-droit-des.html

---

Quasiment 100% des

responsables IT français inquiets de la sécurité des objets connectés | Le Net Expert Informatique

Quasiment 100% des responsables IT français inquiets de la sécurité des objets connectés

Une enquête menée par le cabinet Vanson Bourne montre que les responsables informatiques français sont nombreux à s'impliquer dans des projets liés aux objets connectés. Cela ne les empêche pas de se montrer particulièrement vigilants sur les risques qui en découlent en matière de sécurité.

Alors que l'on pensait que les responsables informatiques français étaient plutôt frileux en matière d'objets connectés, les résultats d'une enquête menée par le cabinet Vanson Bourne pour le compte de Trend Micro montrent que cela n'est vraiment pas le cas. Parmi les 800 responsables informatiques dans le monde interrogés en novembre 2014, 86% des répondants français (100 au total) vont ainsi jusqu'à encourager l'utilisation des objets connectés dans leur organisation. Des organisations qui sont d'ailleurs de plus en plus nombreuses à s'engager (ou prévoir de le faire) dans des programmes impliquant des objets connectés. Ces programmes ont principalement pour vocation à augmenter le bien-être au travail (54%) ou encore à améliorer la productivité des collaborateurs (51%).
En revanche, la mise en oeuvre de projets informatiques faisant appel à objets connectés ne se fait pas au détriment de la sécurité des données. **Ainsi, la quasi-totalité (99%)** des responsables informatiques interrogés considèrent que l'utilisation des objets connectés présente des risques pour l'entreprise. « L'accès aux réseaux sociaux et aux boîtes mails personnelles, l'application la plus courante des objets connectés, est considéré par deux-tiers des répondants comme la plus risquée pour la sécurité des données de l'entreprise », indique Trend Micro. « En outre, près d'un quart des responsables informatiques interrogés admettent que leur entreprise a déjà été victime d'une faille de sécurité provenant d'un équipement mobile personnel, avec des conséquences alarmantes ».

Des politiques Byod élargies aux objets connectés
Par ailleurs, 77% des responsables informatiques interrogés indiquent être favorables à l'encadrement de l'utilisation des objets connectés sur le lieu de travail (77%), une grande majorité (92%) estimant d'ailleurs que les politiques mises en place pour encadrer le Byod vont être amenées à évoluer pour tenir compte de ces équipements.

Expert Informatique et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-99-des-responsables-it-francais-inquiets-de-la-securite-des-objets-connectes-60414.html
Par Dominique Filippone

Le premier kit électronique pour créer des objets connectés

Le premier kit électronique pour créer des objets connectés

Composé d'une carte équipée d'un microcontrôleur, d'une connexion Ethernet et de capteurs, le mbed IoT Starter Kit d'ARM accède aux outils de développement du PaaS BlueMix d'IBM pour élaborer des objets connectés. Les données recueillies par les capteurs sont également gérées dans le cloud d'IBM.

Avec le kit destiné à l'Internet des objets qu'ils ont annoncé hier, ARM et IBM proposent à un large public de réaliser des produits connectés à Internet. Le marché de ces objets, qui vont des capteurs météorologiques aux accessoires pour récupérer des informations de santé ou de bien-être, se développe rapidement. Le 1,2 milliard de dispositifs existant aujourd'hui pourrait être multiplié par 4,5 d'ici cinq ans, selon une récente étude de Verizon. Ce marché est actuellement fragmenté entre différents types de matériels, OS et standards de communication. Avec leur kit, ARM et IBM veulent simplifier le processus.
Les produits mis au point avec le « mBed IoT Starter Kit – Ethernet Edition » d'ARM recevront et transmettront des données qui pourront ensuite être analysées ou servir d'alertes. Cette solution de développement sera fournie avec le système d'exploitation mbed et se connectera au PaaS d'IBM, l'environnement cloud BlueMix, qui réunit des outils pour la conception d'applications et de services.

Bientôt mis en vente, sans doute pour moins de 200 $
Le kit s'adresse à des utilisateurs qui ne sont pas particulièrement familiarisés avec le développement web ou embarqué. A travers la conception de prototypes, ils seront guidés dans la réalisation des objets et la connexion à BlueMix. Le kit sera bientôt mis en vente. Il contient une carte équipée d'un microcontrôleur Freescale K64F Kinetis disposant d'un coeur de traitement Cortex-M4 fonctionnant à 120 MHz. Une connexion Ethernet relie la carte au service cloud BlueMix qui procure les explications sur sa mise en oeuvre.
Parmi les autres composants de la carte figure aussi un affichage LCD 128 x 32, 256 Ko de RAM, 1 Mo de stockage flash, un micro, un joystick cinq voies, un capteur de température, un accéléromètre et des potentiomètres. Sa fiche de présentation mentionne qu'il suffit de quelques minutes pour récupérer des données des capteurs embarqués et les charger dans le cloud d'IBM. La version Ethernet devrait être suivie de versions Wi-Fi et cellulaires.
ARM n'a pas encore communiqué le prix du kit, tout en indiquant qu'il devrait coûter moins de 200 dollars. Les premiers produits qu'il aura servi à concevoir devraient apparaître cette année. D'autres kits moins chers arriveront plus tard.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-arm-et-ibm-sortent-un-kit-pour-creer-des-objets-connectes-60340.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter