Une formation réglementée du pilote de drone | Le Net Expert Informatique

	Une formation réglementée du pilote de drone

Les survols intempestifs de sites sensibles par des drones font peser une menace sur la future réglementation relative à la formation de télépilote. Alors que le nombre des écoles se rapproche de la centaine, le cadre pédagogique tarde à se mettre en place.

A elle seule, la Fédération professionnelle du drone civil (FPDC) compte, parmi ses 300 membres, une quarantaine d'organismes de formation au pilotage de drone. Au total, en France, ils seraient au moins deux fois plus nombreux. Beaucoup sont intégrés à des opérateurs. Quelques uns ont toutefois fait de la formation leur activité principale. Quoi qu'il en soit, tous ont mis au point leur propre programme, faute d'un cadre réglementaire.
Pour les aspirants télépilotes, le passage par une école n'est pas encore obligatoire. La seule obligation qui leur soit faite, est d'être titulaire d'un brevet théorique de pilote d'ULM ou d'avion (scénarios S1, S2 et S3). Pour les vols réalisés hors vue directe, au-delà d'un kilomètre (scénario 4), c'est-à-dire dans le cadre de missions complexes, le pilote de drone doit être titulaire d'une licence de pilote et avoir effectué 100 heures en tant que commandant de bord. Il s'agit d'un cas de figure très peu répandu et limité à la France.
La FPDC a proposé à la DGAC que la formation soit à la fois théorique et pratique. L'administration serait prête à suivre la proposition des professionnels. Si le dossier est bloqué depuis un an, c'est moins par désaccord, que du fait de la difficulté que rencontre l'administration à réunir les moyens matériels pour valider les cursus. D'où l'idée qui semble faire son chemin de sous-traiter les examens et de se réserver la supervision des organismes de formation. Avant fin 2015, la formation de pilote de drone devrait être officialisée. Il reste à espérer que la multiplication des infractions n'entraine pas une pression politique sur les travaux de la DGAC qui jusqu'à présent a eu le souci d'accompagner le développement de l'activité plutôt que de le contraindre.
Aux Etats-Unis, trois ans après la France, la Federal Aviation Association vient de dévoiler une série de recommandations visant à encadrer l'utilisation des drones civils commerciaux sur le territoire américain. Concernant la formation, la FAA souhaite que les télépilotes soient âgés au minimum de 17 ans et qu'ils passent un examen tous les deux ans pour obtenir une autorisation de faire voler des drones.
En Europe, l'EASA a rendu public la semaine dernière son projet d'encadrement réglementaire de cette nouvelle activité.L'Agence a travaillé à partir des règlements mis en place par les administrations nationales en pointe, à commencer par la DGAC française. Il existe de ce fait une cohérence entre l'approche communautaire et celle de la France. Rien ne s'oppose donc à ce que la DGAC boucle le dossier de la formation des télépilotes, d'autant que ce volet ne sera traiter par l'EASA que dans un deuxième temps.

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

Source : http://www.aerobuzz.fr/spip.php?article5749
Par Gil Roy

L’immatriculation des drones bientôt obligatoire ? | Le Net Expert Informatique

	L’immatriculation des drones bientôt obligatoire ? #drones

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 ».

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

56 % des Français s’inquiètent de la protection de leurs données | Le Net Expert Informatique

Alors que les pertes, vols, violations et surveillance des données privées continuent à être régulièrement dévoilés, les citoyens et consommateurs se montrent de plus en plus inquiets quant à leur protection. Le tout nouveau rapport de Symantec « State of Privacy », mené auprès de sept mille personnes, représentatives de la population de 7 pays européens dont la France, montre que 57 % des Européens s'inquiètent du fait que leurs données ne sont pas sécurisées et que 59 % ont fait l'expérience d'un problème lié à la protection de leurs données dans le passé.

Le rapport montre également la circonspection grandissante des consommateurs sur le sujet, leurs attentes en termes de protection et d'information, ainsi que, pour les entreprises comme pour les Etats, la valeur grandissante des données. Au vu des résultats, Symantec pense que la réticence des individus à partager leurs données va croître et va modifier leurs comportements en ligne.
Si seuls 20 % des Européens font confiance aux enseignes de distribution pour protéger leurs données, leurs actions et réactions ne reflètent pas nécessairement cette inquiétude. Le shopping en ligne continue sa croissancei ; seulement un consommateur sur quatre, voire un sur cinq en France, prend le temps de lire complètement les conditions d'utilisation d'un produit ou service, avant de partager ses données personnelles, et trois sur dix échangeraient leur adresse email pour des bénéfices ou avantages.
Symantec pense que ce n'est qu'une question de temps avant que les problèmes de sécurité ne causent un ralentissement de certaines activités en ligne. Des premiers éléments, montrés par l'étude de Symantec, sont révélateurs : 57 % évitent de poster des informations personnelles en ligne afin de protéger leur vie privée et une personne interrogée sur trois communique de fausses données pour que ses informations personnelles réelles restent privées.
A la lumière de ces résultats, Symantec suggère que nous sommes arrivés à un point critique et que les entreprises doivent utiliser la sécurité des données à leur avantage, en s'assurant que les politiques et procédures de gestion et de protection des données sont réellement solides, et que cette protection des données soit communiquée aux consommateurs comme un engagement vis-à-vis d'eux. La sécurité des données a évolué pour devenir une véritable priorité pour les consommateurs ; dès qu'elles le réaliseront pleinement, les entreprises pourront en tirer un avantage concurrentiel.
L'étude de Symantec suggère également que les consommateurs commencent à comprendre la valeur de leurs données, avec 24 % d'entre eux l'estimant à plus de 10 000 €. 88 % des consommateurs en ligne pensent que la sécurité de leurs données est un élément décisif dans l'acte d'achat, la plaçant devant la qualité du produit ou service, ou encore devant le service client.
Zoltan Precsenyi, Responsable des affaires gouvernementales de Symantec commente : « Les entreprises doivent être plus transparentes avec leurs clients sur la sécurisation de leurs données. La protection de celles-ci doit être intégrée dans la proposition de valeur des entreprises, et considérée en interne non comme un coût mais plutôt comme une exigence qui permet de gagner de nouveaux clients et de nouvelles parts de marché ».
« L'industrie informatique a l'opportunité d'aider les consommateurs à faire des choix raisonnés sur la protection des données » explique Laurent Heslault, Directeur des stratégies de sécurité de Symantec. « Le rapport « State of Privacy » montre que de nombreux consommateurs savent que leurs données ont une valeur. Les entreprises devraient donc envisager de prouver la sécurité des données qu'elles détiennent pour en faire un argument concurrentiel, qui leur permettra de développer leur activité. »

Udo Helmbrecht, Directeur exécutif de l'ENISA explique quant à lui que "les conditions d'utilisation des services en ligne sont souvent cachées, longues, difficiles à comprendre, voire même trompeuses. Nous recommandons aux sociétés et administrations de passer en revue leurs politiques de données privées et de créer des méthodes simples et plus efficaces de communication vers les consommateurs. Nous pensons que ces conditions d'utilisation doivent être plus concises, plus faciles à comprendre et que les entreprises doivent aider leurs clients à prendre le contrôle de leurs données ».

Maître Garance Mathias, Avocat à la Cour, intervenant essentiellement en droit des technologies avancées confirme : « Le rapport State of Privacy est particulièrement intéressant car il reflète le besoin d'information des consommateurs et de cadre juridique adapté à l'utilisation des données à caractère personnel en tant que moteur de l'activité économique. On voit en outre ici qu'il s'agit bien d'un enjeu européen. »

L'intégralité du rapport est disponible en téléchargement ici, et un résumé des résultats clés se trouve ci-dessous. Des commentaires supplémentaires de l'ENISA, de PwC et d'IDC sont intégrés au rapport.

Résultats clés européens et français du rapport State of Privacy de Symantec
– 56 % des Français s'inquiètent de la protection de leurs données, une inquiétude plus forte chez les 35-44 ans (61 %). Pourtant, moins d'1 Français sur 5 déclare lire complètement les conditions d'utilisation des services en ligne.
– 66 % des consommateurs européens veulent une meilleure protection de leurs données personnelles, mais ne savent pas comment faire ni vers qui se tourner. En France, ce ne sont pas moins de 72 % des individus qui partagent ces aspirations et doutes.
– 7 Européens sur 10 pensent que les institutions médicales sont les plus dignes de confiance pour la protection de leurs données. Les entreprises technologiques (moteurs de recherche ou OS informatique) (22 %), la distribution (19 %) et les réseaux sociaux inspirent le moins confiance. Les chiffres France sont identiques, avec seulement 8 % des Français qui font confiance aux réseaux sociaux pour la protection de leurs données.
– Les consommateurs sont divisés quant à savoir à qui revient la responsabilité de pourvoir à la protection des données : pour 36 % d'entre eux, c'est à l'Etat, pour 30 % aux entreprises et pour 33 % aux individus eux-mêmes de protéger au mieux leurs informations*. Pour les Français, c'est avant tout à l'Etat (37 %) et aux entreprises (36 %) et nettement moins aux individus (27 %) de prendre en charge ces mesures de protection.
– Pour 88 % des Français comme des Européens, la protection et la sécurité des données sont très importantes lors de l'achat d'un produit ou d'un service, devançant la qualité et le service client.
– Près d'un jeune sur deux (48 % des 18-24 ans) a déjà donné de fausses informations pour garder le caractère privé de ses données personnelles réelles lors d'un enregistrement quelconque.
– La majorité des personnes interrogées en France comme en Europe pensent qu'il n'est pas juste que des entreprises tirent profit de l'échange de données communiquées. Mais 3 utilisateurs sur 10 sont prêts à donner leur adresse email en échange de bénéfices ou d'avantages.

*les différences de pourcentage sont dues à l'arrondissement dans le calcul. Les données exactes sont disponibles sur demande.

A propos du rapport sur les données privées (State of Privacy) de Symantec Le rapport de Symantec sur les données privées « State of Privacy » intègre les détails d'une étude menée sur la perception et les attitudes du grand public sur la protection de ses données personnelles. Réalisée auprès de 7 000 personnes représentatives de l'Allemagne, du Danemark, de l'Espagne, de la France, de l'Italie, du Royaume-Uni, des Pays Bas, l'étude explore les comportements des consommateurs quant à la protection des données privées et lève le voile sur leur perception de la valeur de celles-ci. Le rapport identifie également des leviers spécifiques de confiance pour les entreprises et les Etats pour protéger les données personnelles. Un problème lié aux données privées se définit comme la violation des principes officiels du Data Protection Act, qui gouverne comment les informations personnelles sont utilisées par les entreprises publiques ou privées, les administrations et les Etats.

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

Source : http://www.globalsecuritymag.fr/Nouveau-rapport-Symantec-sur-les,20150316,51582.html

---

Un oeil sur vous – Citoyens

sous surveillance ! Replay jusqu’au 30/03/2015 | Denis JACOPINI

	Un oeil sur vous – Citoyens sous surveillance ! Replay jusqu’au 30/03/2015

Existe-t-il encore un espace dans nos vies citoyennes qui échappe à la surveillance ? Observer, contrôler et analyser les comportements n'ont jamais été aussi aisés qu'aujourd'hui. Depuis une dizaine d'années, les avancées technologiques se sont accélérées, jusqu'à favoriser une révolution sociétale : la surveillance ciblée s'est transformée progressivement en une surveillance de masse à l'échelle planétaire.

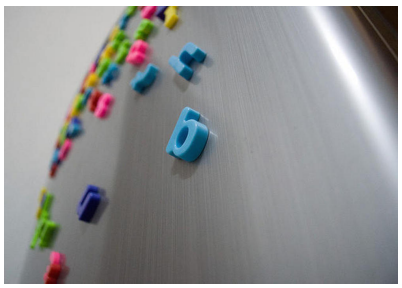
Jadis concentrée sur l'espace public, elle pénètre désormais notre vie privée. L'intimité est une notion de plus en plus floue, soumise à des attaques de moins en moins détectables. Plus sournois que les caméras de surveillance dont beaucoup aimeraient qu'elles couvrent chaque angle mort de l'espace public, le « regard invisible » joue les passe-muraille : jeux vidéo connectés, activité sur les réseaux sociaux, requêtes sur les moteurs de recherche ou géolocalisation via nos smartphones sont autant de constituants manipulables de notre seconde identité – l'alter ego numérique.
En fournissant, souvent sans y consentir ni en avoir conscience, un nombre important de données, le citoyen est devenu l'enjeu d'une bataille politico-économique sans précédent, entre les tenants du tout-sécuritaire, les multinationales du web ou les défenseurs des libertés individuelles.

Emission diffusée sur Arte le mardi 24/03/2015 à 20h50
Rediffusion le mar 07/04/2015 à 8h55
Regardez le replay de l'émission jusqu'au 30/03/2015

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

Source : http://www.arte.tv/guide/fr/049883-000/un-oeil-sur-vous-citoyens-sous-surveillance

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 !

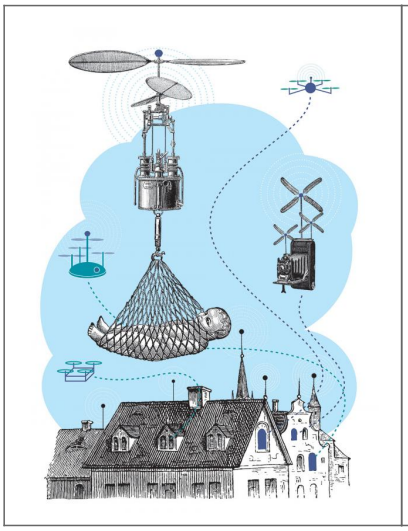
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

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

---

Les drones, outils de demain?

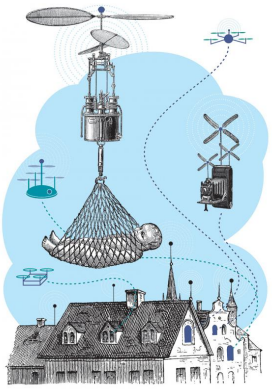
| Le Net Expert Informatique



Les drones, outils de demain?

Fin février, de mystérieux engins volants ont survolé Paris, pendant plusieurs nuits consécutives, semant l'émoi et soulevant des questions dans la capitale française. Même si la plupart des spécialistes s'accordent pour attribuer ces vols sauvages à des « dronistes » en mal de challenge et de provocation, l'effet anxiogène est là. Surtout en ces temps de menaces terroristes avérées.

Pas une semaine sans qu'une société ou un brillant concepteur ne propose un projet innovant porté par des drones. Certains tiennent de l'effet buzz, comme l'annonce par Amazon de la livraison des commandes, déposées le jour même sur le pas de la porte du petit pavillon de banlieue. D'autres, comme ce drone-ambulance imaginé par Alec Momont, un jeune Belge étudiant à l'Université de Delft, laissent entrevoir une facette du futur : équipé d'une trousse de secours, l'engin peut rejoindre une personne en attente d'une intervention médicale d'urgence à une vitesse qui peut grimper jusqu'à 100 km/h. D'autres projets existent comme celui de drones en stand-by tous les 20 kilomètres le long des autoroutes pour évaluer le type de secours attendus après un accident.



Mais si l'on se précipite à la fenêtre, le ciel est pourtant encore désespérément vide. Dépassée par la technologie, la société n'est pas prête, surtout d'un point de vue législatif. Mais déjà les drones ont conquis notre imaginaire. De deux manières. Côté lumière, à l'instar des voitures volantes dont on rêvait dans les années 50, ils concrétisent la promesse de confort et de services nouveaux. Côté sombre, ils apparaissent comme l'œil de Big Brother, le bras volant d'une surveillance généralisée. Des seins de Kate Middleton aux centrales nucléaires, plus rien ni personne ne semble être à l'abri de leurs objectifs et caméras ou de leurs bombes, s'ils deviennent outils des guerres à distance. Engins de guerre, ils permettent la mise à mort de combattants, réels ou présumés, repérés sur des écrans à plus de 10.000 kilomètres de distance.

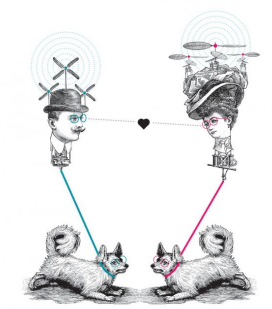
Un potentiel énorme

Sur la base ULM de Liernu, Renaud Fraiture propose des formations, indispensables, à tous ceux pour qui les drones deviennent un outil de travail, et ils sont de plus en plus nombreux. Espace Drone est la première école de ce type. On est actuellement en plein boom. Et ce n'est que le début. Les drones vont changer les habitudes et le confort de travail dans plein de secteurs. C'est un bouleversement comparable à ce qui s'est passé lorsque le GSM a supplanté le téléphone fixe, explique ce pilote d'hélicoptère et d'ULM, télécommande en main, lors d'une séance pratique de pilotage. On arrive très vite à faire décoller l'engin. Une fois qu'il est en l'air, on peut même lâcher quelques instants les commandes, il reste stationnaire. Mais évidemment ce n'est pas suffisant. La formation comprend, outre les trois jours de théorie, 15 heures de pratique. Le pilote, en effet, doit pouvoir faire face aux imprévus, que ce soit la rencontre d'un obstacle ou une bourrasque de vent. Ce jour-là, des employés de la société Elia venaient se familiariser au pilotage de drones destinés à inspecter les lignes à haute tension.

L'engouement que suscite le secteur des drones depuis cinq ou six ans est lié à l'évolution de l'informatique qui a permis des contrôleurs de vol (le mini-ordinateur de bord), équipés de GPS garantissant la stabilité et des batteries plus puissantes et facilement rechargeables pour une meilleure autonomie. Pour du matériel professionnel, il faut compter 3000 € à 4000 € pour une machine de base et 10.000 € à 15.000 € quand on s'aventure dans le sur-mesure lié à une utilisation bien spécifique. Actuellement, 90 % des utilisations professionnelles sont liées à la prise de vue aérienne, mais cela ne représente que 20 % du potentiel des drones qui peuvent rendre d'immenses services dans la sécurité, le secteur industriel ou l'agriculture. On m'a parlé récemment d'un fermier qui confiait à des drones le soin de rentrer ses vaches le soir, confie Patrick Foubert, passionné d'informatique et d'aéromodélisme, qui s'est lancé dans une activité de conseil et d'expertise en matière de drones.

Responsabilisation du public

Outil de travail, le drone est aussi LE jouet à la mode qui s'écoule par camions entiers. Car on trouve désormais en grandes surfaces des drones d'entrée de gamme pour moins de 100 € et de belles petites machines pour 500 € à 600 €. De quoi donner des idées. L'apparente facilité du pilotage et les prix plus qu'abordables mettent ces engins entre toutes les mains avec les risques qu'on imagine. On achète un drone. Aussitôt sorti de la boîte, on le fait décoller de son jardin, on filme la maison et pourquoi pas le voisin, c'est rigolo non ? Beaucoup de gens ne comprennent pas que l'espace aérien au-dessus de leur maison ne leur appartient pas, précise Renaud Fraiteur. Il suffit pourtant de regarder et de déchiffrer la carte aérienne particulièrement dense de la Belgique. Aux no fly zones qui interdisent le survol, les villes, les zones militaires, d'intérêt stratégique… s'ajoutent les couloirs destinés à l'aviation civile. Aucun pilote d'aviation civile, et encore plus s'il est aux commandes d'un hélicoptère n'apprécierait de voir un drone, même de petite taille, croiser sa route. Les risques d'incident avec l'aviation civile sont très très faibles, assure Philippe Platteborze, pilote de long courrier, ce qui n'empêche pas qu'il faut prendre son temps pour établir une législation claire et réaliste qui tienne compte des différents types de drones. Que faire ? Les drones laissent peu de traces, ils sont difficilement repérables en vol. La seule chance, c'est de repérer et d'intercepter son pilote au sol. Certains proposent d'intégrer dans le logiciel des contrôleurs de vol des zones interdites. C'est peu fiable et peu praticable. Ou peut-être comme l'a suggéré un sénateur de l'Oklahoma de permettre au simple quidam d'abattre tout drone inconnu survolant sa propriété. L'interdiction de la vente est illusoire, la seule solution raisonnable, c'est la responsabilisation du public.



Tout le secteur est rivé au stylo de la ministre Jacqueline Galant, qui a promis de signer dans le courant de cette année l'arrêté royal réglementant le pilotage de drones dans le ciel belge. Tant qu'il n'est pas adopté, les vols de drones sont théoriquement interdits, sauf exceptions, pour les forces de l'ordre par exemple. Même si les modalités restent encore floues, il se calquera vraisemblablement sur les grandes lignes des législations en vigueur dans d'autres pays, à savoir le vol à vue avec une hauteur maximum, l'interdiction du survol des villes et du vol de nuit. Cela contentera-t-il tout le monde ? Rien n'est moins sûr.

Adrénaline

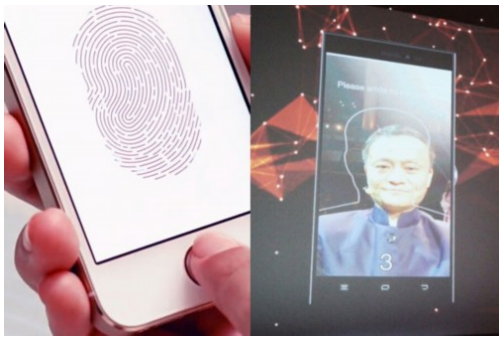
Rendez-vous est donné dans un parking sous terrain de Louvain-la-Neuve pour une séance de vol en immersion. La Team White Rabbits est l'un des premiers clubs en Belgique à pratiquer le low riding, une discipline apparue aux États-Unis qui consiste à se lancer dans des courses de drones pilotés en FPV ou First Person View. Grâce à des lunettes spéciales qui affichent les images prises par les minicaméras placées sur l'engin volant, le pilote sagement assis sur son petit siège pliant voit ce que voit son drone. C'est la montée d'adrénaline assurée. On fonce à ras du sol, les virages sont serrés. On essaie de ne pas perdre de vue les LED rouges qui brillent à l'arrière du drone du copain. On est dans l'appareil tout en restant assis… C'est éprouvant pour le cerveau. On dissocie le physique et le mental, on n'est plus que des doigts sur la télécommande, explique Sébastien. Les lapins blancs volent depuis décembre 2013. Venus du monde de l'aéromodélisme, ils y ajoutent de solides connaissances informatiques car ils assemblent leurs machines eux-mêmes pour qu'elles répondent au mieux à leurs besoins. Quand on vole en low riding, on privilégie les machines ultralégères qui seront plus puissantes, plus nerveuses . Et quand il y a chute ou crash, les éléments à remplacer ne coûtent pas trop cher. S'ils volent dans un parking désert, c'est d'abord parce qu'on est en hiver et qu'ils pensent à leurs petits doigts. Mais aussi pour rester discret. En belle saison, tout le matériel entre facilement dans un sac à dos. On part en balade et on cherche des endroits dégagés pour voler et s'amuser. Pilotes chevronnés, forts d'une longue pratique, Sébastien et Quentin regardent avec envie les législations françaises et canadiennes qui ont prévu quatre classes de drones en fonction de leur poids. On aimerait bien que notre discipline soit reconnue pour ce qu'elle est. Nous avons nos règles de bonne conduite et on sait ce qu'on fait, remarque Quentin.

À l'engouement et la démocratisation des drones se superposent les angoisses diffuses de ce début de siècle. Au delà de l'effet de mode, il faut veiller à ne pas tout mélanger : les outils professionnels, les objets de loisirs, les vols sauvages au-dessus des villes ou des centrales, les questions de vie privée et les dangers du terrorisme qui n'ont pas besoin des drones pour exister. Le 6 mars, les autorités européennes et la direction générale de l'aviation civile se sont accordés sur une déclaration qui plaide pour une harmonisation des règles d'utilisation des drones. Ils insistent aussi pour que les lois à venir soient proportionnelles aux risques encourus par chaque type d'utilisation sans oublier que derrière chaque vol à distance, il y a un opérateur. Les drones ne vont pas disparaître, ils attendent des balises.

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

Source : http://www.lesoir.be/831103/article/victoire/air-du-temps/2015-03-24/drones-outils-demain

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.

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

Les réserves de la CNIL sur le projet de loi renseignement | Le Net Expert Informatique

	Les réserves de la CNIL sur le projet de loi renseignement

Il n'y aura pas de surveillance généralisée du citoyen, assure-t-on à Matignon, alors que le projet de loi renseignement doit être présenté jeudi en Conseil des ministres. Cela n'a pas empêché la Commission nationale de l'informatique et des libertés (CNIL) d'émettre un certain nombre de réserves sur ce texte, dont le calendrier a été accéléré après les attentats contre Charlie Hebdo et le supermarché casher de la porte de Vincennes.

Le projet de loi va permettre « une surveillance beaucoup plus large et intrusive », estime un pré-rapport dont « Les Echos » ont pu prendre connaissance. Si les objectifs du gouvernement paraissent « justifiés », « les atteintes portées au respect de la vie privée doivent être limitées au strict nécessaire », écrit la CNIL.

Trois dispositifs nouveaux (collecte automatique d'informations sur les réseau, pose de sondes, sorte de mouchard permettant de collecter des informations en direct sur des personnes surveillées, et pose d'antennes à proximité de suspects) permettent de « collecter de manière indifférenciée un volume important de données » sur « des personnes relativement étrangères » aux suspects. « Ce changement a des conséquences particulièrement graves sur la protection de la vie privée et des données personnelles », avertit la CNIL.

« Aspiration massive de données »

Dans le détail, la détection « par un traitement automatique » des comportements suspects ressemble fort à de la surveillance généralisée. A Matignon, on se montre soucieux de faire de la « pédagogie » sur le sujet. L'objectif de la mesure, explique-t-on, est de détecter « les signaux faibles » permettant d'identifier des individus susceptibles de basculer dans le terrorisme. « Aujourd'hui, ceux qui partent n'ont pas été détectés avant leur départ [vers la Syrie, etc., ndlr]. Or, 89 sont morts, dont un garçon de 14 ans », rappelle-t-on à Matignon.

Pour détecter ces inconnus, les agents veulent pouvoir analyser les flux de données, savoir qui communique avec qui, et quels sont les sites jihadistes visités. Pas d'autres moyens donc que de faire de la surveillance sur le réseau des opérateurs. « Nous voulons insérer dans les équipements des opérateurs des boîtes noires contenant des algorithmes identifiant des comportements marqueurs », précise Matignon. Si en théorie, la disposition pourrait s'appliquer aux géants du Net, les agents de l'Etat préfèrent d'abord aller traiter avec les opérateurs télécoms, considérant qu'ils sauront se montrer plus ouverts à leurs requêtes.

Inévitablement, une partie des flux échappera aux services, Google ayant depuis les révélations d'Edward Snowden chiffré l'ensemble des connexions de ses utilisateurs.

Quant à la captation en temps réel des données géolocalisées de personnes mises sous surveillance (3.000 personnes environ), elle est assimilée par la CNIL à un dispositif « d'aspiration massive et directe des données par l'intermédiaire de la pose de sondes ». Enfin, le système « IMSI Catcher » (pose d'antennes relais à proximité d'un suspect) permet aussi d'intercepter des informations sur des personnes n'ayant rien à voir avec les faits, regrette la CNIL.

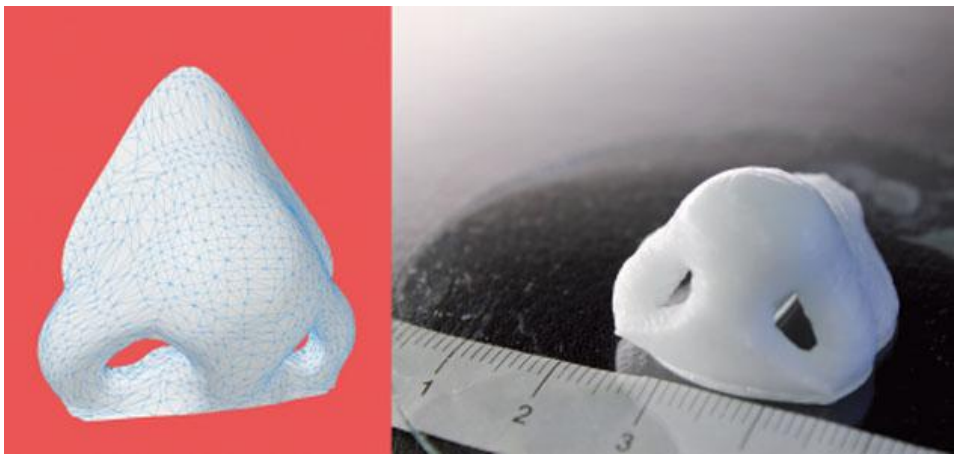
De leur côté, les interceptions de sécurité – les fameuses écoutes – ne sont plus « exceptionnelles », note la CNIL, même si le texte « renforce les modalités de contrôle ». Surtout, la loi donne la possibilité « par réaction en chaîne » d'écouter « des personnes qui n'auraient pas été en relation avec la personne surveillée ».

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

Source : http://www.lesechos.fr/tech-medias/hightech/0204235783787-les-reserves-de-la-cnil-sur-le-projet-de-loi-renseignement-1103298.php
Par Sandrine Cassini

Impression 3D : des

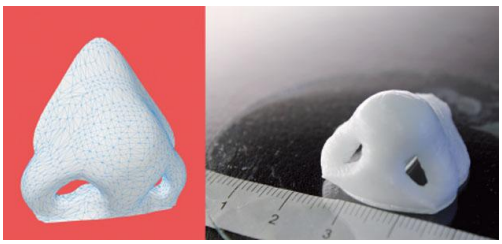
cartilages de nez imprimés en seulement 16 minutes | Le Net Expert Informatique



Impression 3D : des cartilages de nez imprimés en seulement 16 minutes

L'impression 3D continue son avancée dans le domaine médical. Des chercheurs d'un laboratoire de Zurich ont conçu un moyen d'imprimer une structure de nez humain qui, une fois greffée, peut s'intégrer à l'organisme.

Les chercheurs du laboratoire de recherche sur le développement et la régénération du cartilage, dépendant de l'École polytechnique fédérale de Zurich, en Suisse, viennent de dévoiler une avancée importante en matière d'impression 3D dans le domaine médical. A l'aide d'une imprimante 3D, ils sont parvenus à concevoir un cartilage de nez à l'aide de biopolymère et de vrai cartilage, le tout en seulement 16 minutes.
Le résultat obtenu peut ensuite être transplanté sur un être humain, et sa conception organique permet d'éviter au mieux le rejet puisque des cellules récupérées par biopsie sur le patient sont intégrées à la démarche d'impression. Au fil du temps, le cartilage imprimé en 3D est donc assimilé par l'organisme. Selon l'équipe de chercheurs, il devrait être impossible de différencier la greffe, des cartilages d'origine, au bout d'un certain temps.
Une découverte qui pourrait aider de nombreux patients dans le cadre, notamment, de la chirurgie reconstructrice. L'exemple du nez est intéressant, car à l'aide de la modélisation 3D, il serait possible de recréer un modèle totalement fidèle à la réalité, pour ne pas voir de différence avant et après un accident. Mais d'autres organes du corps pourraient bénéficier de ce type de technologie, comme une oreille ou un genou, par exemple.



Une technologie coûteuse
Mais reste, à l'heure actuelle, une limite importante, à savoir le coût de fabrication de ce genre de greffon. La « bio-impression » est très coûteuse, et encore inabordable pour la plupart des hôpitaux. Néanmoins, pour les chercheurs, développer ce genre de technique va s'avérer nécessaire par la suite. « Le potentiel de la bio-impression 3D va encore se développer à l'avenir, jusqu'à devenir la technologie ultime permettant aux patients de recouvrer la santé » estime Matti Kesti, responsable du projet. La route est encore longue, mais le futur est prometteur. Par contre, pour imprimer des humains, il faudra attendre un peu…

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.clubic.com/mag/sport/actualite-759491-impression-3d-cartilages-nez-imprimes-16-minutes.html?estat_svc=s%3D223023201608%26crmID%3D639453874_904240618

Recherche Web : Google a bien triché, et devait être sanctionné | Le Net Expert Informatique

	**Recherche Web : Google a bien triché, et devait être sanctionné**

En 2013, le régulateur US avait refermé le dossier antitrust sans sanctionner Google. Mais un rapport de la FTC, livré par erreur, atteste de la manipulation des résultats de recherche par Google, au profit de ses services et au détriment des concurrents et même des utilisateurs.

Suite à de longs mois d'enquête, le régulateur américain du commerce (FTC) avait finalement conclu un accord avec Google dans le cadre d'une plainte pour abus de position dominante. Aucune mesure contraignante n'avait été prise à l'encontre du géant de la recherche.Pour autant, cette décision ne signifie pas que les pratiques de Google dans la recherche en ligne aient été jugées par les enquêteurs de la FTC comme saines sur le plan concurrentiel.
Bien au contraire, et c'est d'ailleurs ce que démontre un rapport obtenu par le Wall Street Journal.

Google a altéré volontairement le ranking
Et ce rapport émane directement du régulateur qui, suite à une requête du WSJ demandant la communication d'un document public, a envoyé par erreur une version non expurgée et partielle du rapport d'enquête du personnel de la FTC.
Les conclusions y sont bien plus tranchées que les informations livrées à l'époque par la FTC pour justifier de faire mettre un terme à son litige avec Google. De nouveaux détails soulignent ainsi que Google a bien manipulé les résultats de recherche au profit de ses propres services, y compris lorsque ces résultats étaient d'une pertinence moindre pour l'utilisateur.
Le WSJ, grâce à cette erreur de l'administration, révèle ainsi plusieurs des pratiques constatées par le régulateur et qui n'avaient jamais été communiquées.

Dans le shopping par exemple, Google classait les résultats de son service avant ceux de ses concurrents, alors que celui-ci affichait un taux de clic inférieur.Le personnel de la FTC chargé de l'enquête estimait donc que Google plaçait volontairement ses services au-dessus de ceux de ses concurrents, comme Yelp, TripAdvisor ou Expedia, qui eux se voyaient dans le même temps rétrogradés par le moteur en termes de ranking, en dépit de leur pertinence pour l'utilisateur.

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

Source : http://www.zdnet.fr/actualites/recherche-web-google-a-bien-triche-et-devait-etre-sanctionne-39816656.htm