Revue du centre de recherche
de l'École des officiers
de la gendarmerie nationale

N° 132
Décembre 2016

## Le mot du rédacteur en chef

Ce dernier numéro de l'année 2016 est l'occasion de porter un regard rétrospectif sur douze mois pendant lesquels les forces de l'ordre ont été soumises à une pression ininterrompue.

Le terrorisme a imprimé sa marque sur l'activité de la gendarmerie mais aussi sur son organisation et ses modes d'action. La protection des lieux publics et les enquêtes tant administratives que judiciaires ont constitué une part importante de l'activité tandis que se mettaient en place tous les moyens spécifiques liés à la menace terroriste. Ont ainsi été créés les PSIG Sabre et de nouvelles antennes régionales du GIGN, lequel a assuré pour la première fois une présence continue sur le Tour de France. Les écoles de gendarmerie ont été amenées à réviser une partie de la formation initiale des militaires pour faire face à l'apparition des tueries de masse. L'EOGN a inclus elle-même des modules spécifiques dans son cycle de formation des officiers. Les premiers commandants de PSIG Sabre ont ainsi quitté l'école en août dernier.

Sur le plan plus général de l'ordre public, l'année s'est caractérisée par une longue période de manifestations qui ont mobilisé d'importants moyens. Les escadrons de gendarmerie mobile ont dû affronter à cette occasion des individus dont l'organisation et l'agressivité étaient inédites. Le pays a pu assister, médusé, à des déchaînements de violences dont le seul but était d'atteindre dans leur chair les membres des forces de l'ordre. Parallèlement, de l'autre coté de la planète, en Nouvelle-Calédonie, les gendarmes ont eu à faire face à des agresseurs armés qui n'ont pas hésité à ouvrir le feu à de nombreuses reprises sur eux. Cette violence touche également les unités territoriales dont les militaires sont de plus en plus souvent la cible d'individus utilisant leur véhicule comme une arme.

Dans leurs missions quotidiennes, les gendarmes ont payé cette année un tribut particulièrement lourd avec notamment la perte de quatre des leurs dans un accident d'hélicoptère au mois de mai et, il y a quelques jours, le décès de quatre militaires dans deux accidents de voiture, en métropole et en Guyane.

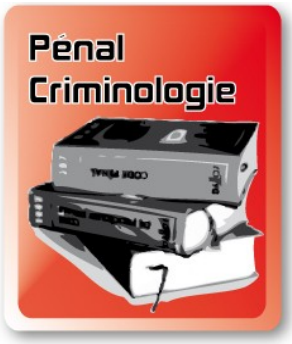
Les fêtes de Noël et du nouvel an sont traditionnellement des périodes de forte activité. Avec les mesures de vigilance accrue, la tension se rajoute à la charge du service. Nos camarades des armées, engagés quotidiennement dans le cadre de Sentinelle, prennent leur part dans l'organisation de la sécurité de nos concitoyens.

Puisqu'il est de saison de prononcer des vœux, ceux du CREOGN seront pour une année de lutte efficace contre les fléaux qui ont engendré en 2016 tant de drames. Pour vous, chers lecteurs, nous souhaitons paix, santé et réussite dans vos entreprises.

Bonne année 2017.


- Géolocalisation des véhicules
- Un espoir d'accord pour le transfert des données personnelles : « l'EU-US Privacy shield »
- Sujets de réflexion de la CNIL
- Avis de la CNCDH sur le portrait-robot génétique
- Des drones contre la prostitution ?
- Les technologies de cryptage, nouveau frein des enquêtes terroristes
- Blocages de sites web, bilan de la CNIL
- La CNIL se penche sur les objets connectés


- Inauguration du centre euro-méditerranéen de simulation des risques (CESIR)
- Un bouton « SOS » contre les terroristes
- Les drones, outils de la vidéoprotection des collectivités ?
- Drones civils : évolution de la réglementation




- Crime organisé sur Internet : état de la menace
- Nouvelle piste pour les investigations criminelles


- Le pneumatique italien intelligent sur les routes pour 2017
- La fin annoncée des rétroviseurs extérieurs ?
- Lunettes intelligentes anti-éblouissement
- L'ONU annonce la révision de la convention de vienne au profit des voitures autonomes
- Expérimentation de véhicules à délégation de conduite sur les voies publiques
- Parution d'une étude relative aux accidents de circulation liés aux « smombies »
- Étude européenne sur l'utilisation des plaques d'immatriculation RFID
- Conception smiling-car


- Webdrone chasse la contrefaçon et les autres formes de cybercriminalité sur le Net
- Risque cyber et gouvernance en entreprise


- Parution du règlement européen de protection des données à caractère personnel
- Europol élargit ses compétences en ligne

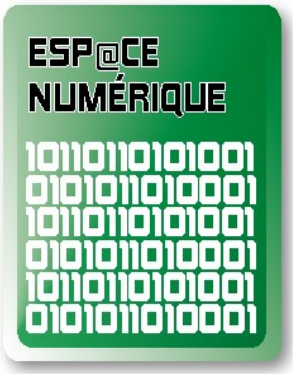

- Vraies vies, vrais crimes
- Un robot-avocat pour contester les contraventions
- La police britannique et l'enseignement supérieur vont travailler sur la cartographie des lieux à risques
- Rendre la justice à l'ère numérique
- Portraits anthropométriques en 3D pour la police de Tokyo
- Belgique : de jeunes « cyber-patrouilleurs » contre la haine en ligne


- Thales dévoile son nouveau drone naval hybride


- La cabine détachable : l’avenir de la sûreté aérienne ?


- La Californie veut strictement encadrer les voitures sans conducteur
- Sea Tags, bracelet maritime connecté
- « TRAD 112 » : application permettant une meilleure communication entre secouristes et personnes étrangères blessées ou malades
- La caméra CounterBomber, solution de sûreté vidéo à technologie radar
- Revolar : bouton d'alerte connecté
- Smartphone : détecteur de séismes
- SEAGULL : le bateau de déminage autonome
- Automist Smartscan : extincteur intelligent capable de viser le feu
- Dispositif de lutte contre les incendies autonome : création de robots-pompiers volants
- Auto-génération d'un robot
- Le robot Atlas, la révolution d'Alphabet
- Robotique : le serveur n'est pas humain
- An'Bot, CRS du futur
- Abandon du projet de « mule robotique » par l'armée américaine
- Dogo : un nouveau robot de combat télécommandé et armé
- Le Pentagone mise officiellement sur les « textiles intelligents »
- Les forces spéciales américaines bientôt équipées de tenues de combat intelligentes
- Une nouvelle couverture d'invisibilité pour les militaires
- Lancement d'un aéronef hybride « drone-avion-hélicoptère »
- Micro drone militaire
- Distribution de médicaments, vaccins et livraison de sang par drones
- Drones et aide humanitaire
- Un nouveau venu chez les drones : le drone-plongeur
- Le drone landais Helper spécialisé dans les interventions en mer primé au concours Lépine
- Premier drone connecté de transport autonome
- Commercialisation du premier drone solaire
- La police néerlandaise entraîne des rapaces à abattre des drones
- Drones et recherche environnementale
- Aux États-unis, les drones de loisirs devront être enregistrés auprès des services de l'État
- Droits et devoirs pour les robots ?
- Auschwitz : la réalité virtuelle au service de la justice
- L'authentification par empreinte digitale grand public
- Des capteurs d'empreintes de smartphones trompés avec une simple imprimante
- Identification biométrique par l'oreille
- Développement de la reconnaissance faciale
- Des lunettes pour déjouer la reconnaissance faciale ?
- Nouvelle vidéosurveillance intelligente

- « Iris VISÉO » testée à Pau
- Des ballons d'observations « municipaux » dans le ciel du Chili
- Transformation de portraits dessinés en photos
- L'intelligence artificielle lutte contre les commentaires violents en ligne
- Chine : lancement d'un satellite quantique pour bouleverser le monde du cryptage




- Rapport d'activité 2014-2015 de l'HADOPI
- Les règles de la neutralité du Net confirmées en appel aux États-Unis
- La CNIL réfléchit à la notion de partage dans le monde numérique
- Loi pour une République numérique
- Rapport 2015 de l'ARCEP
- Saisine de l'administration par les usagers à l'aide d'un téléservice
- Panorama mondial 2015 de la cybercriminalité
- Rapport 2016 de sécurité CISCO
- 2015 : une vingtaine de cyberattaques majeures contre la France
- L'étude d'Eurostat sur la perméabilité de l'internet européen face aux problèmes de sécurité
- Les inquiétantes perspectives de la cybercriminalité pour 2016
- Les dernières prévisions en cybercriminalité
- Cybercriminalité et paix en Afrique francophone
- L'aviation civile n'est pas à l'abri du cyber-terrorisme
- Internet des objets, sécurité et vigilance
- Le secteur énergétique exposé à la cybermenace en Europe
- Professionnalisation du cybercrime
- Complicité chez les opérateurs télécoms en matière de cybercriminalité
- Détection d'une vulnérabilité dans l'application Waze
- Danger des bornes de rechargement USB
- La croissance du nombre de malwares inquiète l'Italie
- L'authentification en deux étapes par SMS : une opération à risque
- Piratage du site du centre d'identification des matériels de la Défense
- Les hackers s'en prennent toujours plus aux hôpitaux
- Nouveau  ransomware « Petya »
- Très populaire aux États-Unis, l'application canadienne KIK offre l'anonymat pour les adolescents et leurs prédateurs…
- Abus sexuels d'enfants en direct sur Internet en hausse selon Interpol
- Revenge porn, un phénomène mieux connu
- L'application Gossip dans le viseur de la CNIL
- Une application antisémite supprimée par Google Play
- Protection de la vie privée et cryptage des données

- Le FBI pirate le dark web pour débusquer des pédophiles
- L'Internet des objets, outil au service des gouvernements
- Sous les pavés numériques, la plage, vraiment ?…
- L’arme fatale contre la fraude
- Lentilles de contact caméras
- « Maison connectée » : un nouveau dispositif de protection de son habitat à distance
- Invention d’une coque iPhone anti-espionnage
- Réseau social citoyen
- Les fournisseurs d’infrastructures cloud se dotent d’un code de bonne conduite européen
- Partenariat sur l'éthique par les géants du Web
- Réalité virtuelle : serons-nous heureux dans la matrice ?


- Sécurité des données en entreprise – rapport 2016 de GEMALTO


- Apparition d’une application visant à prévenir les suicides
- Création de tissus humains avec une imprimante 3D laser
- Facebook utilisé pour le commerce illégal d'espèces menacées
- Facebook et braconniers
- Drone contre frelon asiatique
- Opération Pangea IX : lutte contre la vente illicite de médicaments sur Internet
- La réalité virtuelle s’invite dans le domaine de la paraplégie
- Partage des données de santé entre patients et acteurs médicaux
- La technologie « gene drive »
- Victeams, logiciel de simulation médical


- Le développement inquiétant des maladies dites de « connexion »


- Au Royaume-Uni un guide pour lutter contre le *sexting* dans les écoles

## *ÉDITORIAL DU DIRECTEUR*


Au moment où je rédige cet éditorial, l'Allemagne est en deuil. Les terroristes ont à nouveau frappé de manière aveugle en ciblant un marché de Noël et donc nos traditions. Chrétiens ou non, nous attachons du prix à cette fête qui nous rassemble en famille. Le principal auteur a été abattu lors d'un contrôle, mais combien de fous circulent encore ? Les commentaires vont bon train et sont le plus souvent empreints d'ignorance ou de mauvaise foi. Quels que soient les voies et moyens employés pour lutter contre le terrorisme, nous ne le vaincrons qu'en proposant un modèle de société qui suscite l'adhésion, en s'appuyant sur le respect de l'être humain. La bataille est d'abord celle du sens. À nous de le retrouver, de le reformuler.

Au moment où je rédige, la gendarmerie est en deuil. Quatre de nos camarades ont trouvé la mort dans des accidents de la circulation, dans l'Oise et en Guyane. Pour leurs familles, pour leurs unités, c'est un drame qui survient alors que nous sommes dans la joie des fêtes de Noël. La mort d'un camarade est ce que j'ai le plus redouté pendant toute ma carrière.
Je me suis donc doublement interrogé sur la pertinence de mon éditorial, considérant qu'il serait totalement décalé par rapport à la dureté du moment. Mais la vie continue. Notre réflexion, même modeste, contribue à la construction du monde à venir. Celui-ci sera plus que jamais conditionné par les nouvelles technologies que l'on dit souvent « disruptives », car elles bouleversent nos modes de vie. Ce numéro de la Revue du centre est publié quelques jours avant le FIC (24 et 25 janvier à Lille, www. Forum-fic.com). « Nouvelles technologies, nouveaux usages, en toute sécurité », un thème qui sera également développé par la Revue de la gendarmerie nationale, numéro spécial FIC. De bonnes lectures en perspective !

Toute l'équipe du CREOGN qui a contribué à ces publications vous souhaite une bonne et heureuse année 2017.

***Par le Général d'armée (2S) Marc WATIN-AUGOUARD***

RETOUR

# *AGENDA DU DIRECTEUR*

**3 janvier 2017** :

- réunion sur les études du CREOGN présidée par le Major général
- rencontre avec Master 2 droit de la défense et de la sécurité Paris2

**4 janvier 2017** : écoles de Coëtquidan, jury de soutenances de mémoires

**5 janvier 2017** : réunion sur les blackmarkets (FIC)

**6 janvier 2017** :

- réunion à la préfecture de Lille (FIC)
- réunion à la DGGN sur la formation des brigades de contact

**9 janvier 2017** : réunion du comité des études au ministère de l'Intérieur

**10-13 janvier 2017** : préparation FIC

**14 janvier 2017** : cours à la CPI

**17 janvier 2017** : conférence sur les politiques de sécurité à Paris V

**18 janvier 2017** : réunion IEJ Paris 2

**19 janvier 2017** : réunion du cercle K2, cercle Saint-Augustin

**21-22 janvier 2017** : Lille, préparation du FIC

**23 janvier 2017** : conférence sur la réponse aux incidents et les investigations numériques (CoRIIN) à Euratechnologies (Lille)

**24 et 25 janvier 2017** : FIC à Lille

**26 janvier 2017** : « post-FIC », conférence à Lille 2 sur les enjeux de la transformation numérique

**28 janvier 2017** : cours à la CPI


### *132-16-LP-01* GÉOLOCALISATION DES VÉHICULES (JANVIER)

La CNIL a mis en ligne le 28 décembre 2015 une fiche destinée à détailler les règles régissant, pour les entreprises, la géolocalisation des véhicules des salariés. La fiche s'appuie sur l'article 16 d'une recommandation du Conseil de l'Europe en date du 1er avril 2015.
La CNIL précise la finalité des dispositifs de géolocalisation : ils servent à justifier la facturation de prestation, à renforcer la sécurité des employés et des marchandises et véhicules, à gérer au mieux l'utilisation de la flotte, accessoirement à suivre le temps de travail, éventuellement à répondre à une obligation légale ou réglementaire liée à la nature des marchandises transportées et enfin à contrôler le respect des règles d'utilisation des véhicules. Ils ne peuvent pas servir à contrôler le respect des limitations de vitesse ou à contrôler en permanence un employé, ou encore à calculer le temps de travail de l'employé alors qu'un autre dispositif existe par ailleurs.
Les employés sont informés de l'installation des dispositifs de géolocalisation. Ils doivent avoir accès aux informations enregistrées par ces dispositifs les concernant. Enfin, ils doivent pouvoir désactiver le dispositif pendant les horaires non ouvrés.
Les données sont conservées en principe au plus deux mois. Pour autant, ce délai est porté à un an lorsqu'elles servent à optimiser les tournées ou à servir de preuve pour les interventions (en l'absence d'autre moyen). Il est porté à 5 ans lorsque le dispositif sert à suivre le temps de travail des employés.

http://www.cnil.fr/fileadmin/documents/approfondir/dossier/travail/FICHETRAVAIL_GEOLOCALISATION.pdf

### *132-16-LP-02* UN ESPOIR D'ACCORD POUR LE TRANSFERT DES DONNÉES PERSONNELLES : « L'EU-US PRIVACY SHIELD » (MARS)

Début février 2016, l'Union européenne et les États-Unis se sont entendus sur la définition d'un nouvel accord-cadre relatif au transfert des données personnelles.
Ce sujet fait l'objet de bien des débats depuis quelques années. Après l'invalidation de l'accord « Safe Harbor » par la Cour de Justice de l'Union Européenne en octobre 2015, la nouvelle entente vise à poser les principes d'une meilleure protection des données.
Il s'agit d'un bouclier pour la protection de la vie privée, « l'EU-US Privacy Shield ». Pour autant, ce n'est jusque-là qu'un accord politique acté par la Commission européenne.
Il tend à instaurer des obligations de protection renforcées, à destination des sociétés américaines de traitement des données en provenance de l'Europe.
C'est ici la première fois que le gouvernement américain s'engage de manière écrite à ce que l'accès aux données par les autorités publiques, ou en charge de la sécurité nationale, soit limité et soumis à des mesures de contrôle. Ainsi, les États-Unis tentent d'atténuer

l'image de surveillance de masse des données qui leur est attribuée. La présence d'autorités de contrôle est elle aussi prévue.
De plus, l'accord envisage plusieurs moyens de recours en vue d'une meilleure protection des citoyens. Il leur sera possible d'adresser directement une plainte aux sociétés adhérentes au nouvel accord.
À côté de cela, les plaintes recueillies par les autorités de contrôle européennes pourront être transmises au Département du Commerce américain ainsi qu'à la Federal Trade Commission. Un système de résolution des conflits gratuit est aussi prévu et un médiateur des questions d'accès aux données par les agences de renseignement doit être créé.
Actuellement, l'Union européenne et les États-Unis se trouvent dans une phase de transition fragile, celle de la régularisation des transferts effectués sur la base du Safe Harbor.
En attendant et d'ici le mois d'avril, les autorités nationales de protection des données personnelles et les États membres de l'Union doivent encore examiner le texte.

http://www.lemonde.fr/idees/article/2016/02/29/accord-sur-les-transferts-de-donnees-personnelles-vers-les-etats-unis-les-bases-d-une-meilleure-protection-sont-posees_4873957_3232.html

### *132-16-LP-03* SUJETS DE RÉFLEXION DE LA CNIL (AVRIL)

La CNIL a mis en ligne son rapport annuel d'activité pour l'année 2015. Ce document de 100 pages revient sur l'activité globale de la commission mais propose aussi des analyses sur la lutte contre le terrorisme à l'aune des libertés publiques, sur les caméras-piéton des forces de l'ordre, la protection des données personnelles dans le cyberespace et l'invalidation du Safe Harbor. Il détaille également les sujets de réflexion pour l'année 2016. Au nombre de trois, ils portent sur les véhicules connectés, les objets connectés et les *data brokers* (les courtiers en données).
Les véhicules connectés sont abordés sous l'angle d'un pack de conformité qui viendrait s'imposer aux futurs véhicules connectés. La sécurité des données liées à la voiture connectée est considérée comme centrale dans la mesure où la sécurité physique des personnes pourrait être en jeu en cas de compromission des éléments de pilotage. La voiture elle-même est vue comme une plate-forme d'échange d'un très grand nombre de données touchant au conducteur, aux passagers, au véhicule et aux infrastructures. Comme cette plate-forme est susceptible de se déplacer sur tout le territoire européen, il semblerait judicieux que le pack de conformité fasse l'objet d'une réflexion européenne.
S'agissant des objets connectés, la CNIL souhaite porter son regard sur les robots dont le rôle et la présence sont de moins en moins anecdotiques dans nos sociétés. Les drones, par exemple, s'apparentent de plus en plus à des robots puisqu'ils peuvent, de façon automatique, effectuer certains mouvements (revenir au point de départ en cas de perte de signal, suivre une personne, éviter des obstacles…). Les voitures connectées elles-mêmes entrent progressivement dans cette catégorie. Selon la CNIL, des enjeux éthiques émergent. Ils portent sur l'augmentation et la réparation de l'humain, la création de robots socialement interactifs et l'autonomie décisionnelle laissée aux machines.
Enfin, les courtiers en données tendent à devenir des acteurs incontournables de

l'économie. S'appuyant sur le « pétrole » que constituent les données, ils entraînent un questionnement sur la propriété de celles-ci. Le droit à « l'autodétermination informationnelle » (la faculté de décider et de contrôler l'usage fait de ses propres données personnelles) apparaît une notion essentielle en la matière. Pour autant, la CNIL pointe l'ensemble du business généré par le courtage des données, partiellement pris en compte par des règles juridiques stables.
En page 18, l'article sur les caméras-piéton dotant les forces de l'ordre fait un point précis sur les enjeux de vie privée, l'encadrement à prévoir pour ces caméras et leur avenir prévisible.

https://www.cnil.fr/sites/default/files/atoms/files/cnil-36e_rapport_annuel_2015.pdf

### *132-16-LP-04* AVIS DE LA CNCDH SUR LE PORTRAIT-ROBOT GÉNÉTIQUE (AVRIL)

Dans la Revue du CREOGN N°113 de janvier 2015 (article 113-15-PC-02), nous évoquions le portrait-robot génétique et les questions éthiques qu'il pouvait soulever. Ce nouveau moyen d'investigation, la recherche ADN des caractères morphologiques apparents, a été autorisé par un arrêt de la Cour de cassation du 25 juin 2014, contre l'avis de l'avocat général. Jusqu'alors, le séquençage de gènes n'était réalisé, conformément à la loi bioéthique de 1994, que dans un but scientifique ou médical et devait impérativement être précédé du consentement explicite de la personne concernée et, dans certains cas, de l'avis d'un comité de protection des personnes.
La Commission Nationale Consultative des Droits de l'Homme a publié à ce sujet un avis le 17 mars 2016, sur demande de la garde des Sceaux. Si elle reconnaît la légitimité d'une telle recherche dans le cadre d'une enquête criminelle et l'allègement du dispositif ainsi rendu possible (« en évitant le recueil de masse de parties d'ADN non codantes »), elle estime cependant que la législation actuelle n'offre pas de garanties suffisantes quant au respect du droit à la vie privée, « protégé par l'article 8 de la Convention européenne des droits de l'Homme ». Selon la Commission, l'article 81 du Code de procédure pénale, sur lequel se fonde l'autorisation du recours au portrait-robot génétique, ne propose pas actuellement un cadre suffisant à l'expertise génétique codante. Elle rappelle ainsi opportunément qu' « aucun texte ne prévoit explicitement la faculté d'ordonner une expertise aux fins de révéler les caractères morphologiques apparents d'une personne à partir de son ADN dans le cadre d'une procédure judiciaire ». De plus, elle met en garde contre une surestimation de la fiabilité de ce procédé, considéré comme une « technique prédictive ».
Des précisions seraient donc nécessaires sur la nature et le nombre de caractéristiques morphologiques apparentes pouvant être légalement déterminées, sexe, couleur de la peau, des yeux, des cheveux, taille, trisomie 21, albinisme, appartenance à telle ou telle ethnie... Cette pratique ne devrait en aucun cas être utilisée pour déceler des anomalies génétiques, ce qui pourrait conduire à des dérives comme la mise en relation entre un type de criminel et une caractéristique génétique et devrait se limiter strictement à la recherche de l'identification de l'auteur d'un crime, sur décision du seul juge d'instruction, magistrat indépendant. La CNCDH, devant le caractère très sensible des données qui peuvent être

révélées par cette nouvelle technique, recommande leur traitement par des personnes habilitées, « dans des conditions de sécurité élevées » et une conservation limitée dans le temps.

*NDR : Avis à rapprocher de la note N°18 du CREOGN relative à la « numérisation du visage : opportunités et limites de la reconnaissance faciale ».*

http://www.cncdh.fr/fr/publications/avis-sur-le-portrait-robot-genetique-0
http://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Numerisation-du-visage-opportunites-et-limites-de-la-reconnaissance-faciale

### *132-16-LP-05* DES DRONES CONTRE LA PROSTITUTION ? (AVRIL)

Le site smartdrones.fr rapporte le 29 mars 2016 le cas d'un usage pour le moins étonnant d'un drone de loisir. L'affaire, qui se déroule aux États-Unis, met en scène un simple citoyen de la ville d'Oklahoma-City engagé depuis des années dans la lutte contre la prostitution. Il filme les prostituées et leurs souteneurs et diffuse les vidéos sur son site. Il a eu l'idée, il y a un an, d'utiliser son drone pour filmer les ébats d'une prostituée avec son client dans une voiture stationnée dans son quartier. Un jugement vient d'être rendu contre cette prostituée, le film ayant été remis par cet activiste à la police. Elle a été condamnée à un an de prison, son avocat étant resté impuissant devant l'évidence des images. Le procès du client interviendra, quant à lui, ultérieurement.
L'intéressé se défend de porter atteinte à la vie privée des personnes puisqu'il filme la voie publique. Il s'inquiète par ailleurs de l'utilisation de ce genre d'engins par des individus insuffisamment expérimentés, par exemple pour dénoncer des trafics de drogue ou la prostitution dans une rue. Pour autant, cet usage des caméras aériennes portées par les drones illustre parfaitement les risques de dérive et d'atteintes à l'intimité des personnes.

http://www.smartdrones.fr/les-drones-se-mettent-a-chasser-les-prostituees/005075
http://motherboard.vice.com/read/drone-vigilante-brian-bates-johntv-oklahoma-spies-on-sex-workers
http://www.bbc.com/news/technology-35926009

### *132-16-LP-06* LES TECHNOLOGIES DE CRYPTAGE, NOUVEAU FREIN DES ENQUÊTES TERRORISTES (JANVIER)

Les dernières attaques terroristes font ressortir le rôle central des téléphones portables dans l'organisation de ces tragiques événements. Leur exploitation permet souvent de remonter le processus des attaques. Mais certains cas bloquent à l'inverse les investigations.
En effet, les technologies de cryptologie actuellement disponibles rendent parfois l'exploitation de ces objets très difficile. Par exemple, le téléphone d'un des assaillants des attaques parisiennes de novembre 2015 reste toujours impossible à débloquer et c'est loin d'être un cas isolé. Les politiques actuelles de chiffrement des grands développeurs

téléphoniques s'orientent vers une meilleure garantie de la confidentialité des données des utilisateurs. La totalité des données devient inaccessible à quiconque ne possède pas le code de déblocage des téléphones. Pour certains, les nouveaux smartphones « rendent la justice aveugle ».
Or, cette tendance montre parfois ses limites, comme c'est le cas ici. Il n'existe aucune solution permettant aux services techniques de déchiffrer de manière systématique les données.
Une des solutions est alors pour les enquêteurs de faire appel à la Direction Générale de la Sécurité Intérieure (DGSI) mais sans garantie absolue de résultat.
Le regard tend à se porter de plus en plus sur les fabricants afin de développer des solutions adaptées à ces cas extrêmes. De même, une meilleure coopération internationale en la matière est encouragée dans le but d'accélérer le cours des enquêtes.

http://www.la-croix.com/Actualite/France/L-analyse-des-telephones-portables-au-caeur-de-l-enquete-sur-les-attentats-de-Paris-2015-12-20-1395303
http://www.lemonde.fr/attaques-a-paris/article/2016/01/08/antiterrorisme-la-difficulte-de-faire-parler-les-telephones-cryptes_4843888_4809495.html
http://www.lapresse.ca/international/201512/17/01-4932130-des-cellulaires-au-service-des-djihadistes.php

### *132-16-LP-07* BLOCAGES DE SITES WEB, BILAN DE LA CNIL (MAI)

Depuis plus d'un an, les autorités peuvent ordonner le blocage administratif, sans passer par un juge judiciaire, de sites Internet aux contenus pédopornographiques ou ceux incitant à des actes de terrorisme et en faisant l'apologie, et/ou à leur déréférencement dans les moteurs de recherche. L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), déjà en charge de Pharos, la plate-forme de signalement du ministère de l'Intérieur, liste les demandes de retrait de contenus et les sites à bloquer via les fournisseurs d'accès à Internet (FAI). La liste est ensuite soumise à l'Unité de Coordination de la Lutte Anti-Terroriste (UCLAT). Le contrôle du bien-fondé des demandes de retrait, de blocage et de déréférencement est confié à la « personnalité qualifiée » désignée par la Commission Nationale de l'Informatique et des Libertés (CNIL), qui a rendu public, le 15 avril 2016, son premier rapport d'activité. Ainsi, entre le 11 mars 2015 et le 29 février 2016, 25 séances de vérifications ont été tenues par la « personnalité qualifiée », dont 9 depuis les attentats du 13 novembre 2015. 1 439 demandes de retrait de contenus (textes, photos, vidéos…) émises par l'OCLCTIC ont été examinées (1 286 ayant trait à l'apologie du terrorisme et 153 à caractère pédopornographique). 1 080 de ces demandes de retrait à caractère terroriste et 99 à caractère pédopornographique ont été suivies d'effet. Concernant les blocages administratifs, le rapport s'inverse : 244 sites à caractère pédopornographique contre 68 à caractère terroriste. Quant au déréférencement dans les moteurs de recherche, 855 pages web étaient visées : 386 pour apologie du terrorisme et 469 pour pédopornographie. Les réseaux sociaux ou des plates-formes d'hébergement des contenus étant le plus souvent concernés par des demandes de retrait, le choix se porte alors plus sur le déréférencement, jugé moins intrusif et plus simple, que sur le blocage. Sur l'efficacité du dispositif, le

représentant de la CNIL reste prudent. « À la suite du blocage de sites pédopornographiques, de nouveaux sites identiques apparaissaient, avec une adresse légèrement modifiée ». Le rapport révèle que « quelque 35 000 connexions vers des sites censurés sont redirigées chaque semaine sur une page d'avertissement du ministère de l'Intérieur ». Les sites bloqués pour pédopornographie représentent 98,6% des cas.

http://www.liberation.fr/futurs/2016/04/15/blocages-de-sites-web-le-bilan-de-la-cnil_1446488
https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_blocage_sites_internet_2016_0.pdf

### *132-16-LP-08* LA CNIL SE PENCHE SUR LES OBJETS CONNECTÉS (MAI)

Le 12 avril 2016, la CNIL a annoncé qu'elle mènerait avec 29 autres autorités dans le monde une opération conjointe d'audit en ligne afin de mieux cerner l'impact des objets connectés sur la vie privée. Conduit pendant le mois de mai 2016, cet audit porte sur les objets domotiques, les objets de santé (balances, tensiomètres et glucomètres connectés) et les objets de bien-être comme les montres et autres bracelets d'activités. La CNIL s'intéresse en particulier à la qualité de l'information, à la sécurisation des flux de données et au degré de contrôle exercé par l'utilisateur sur la manière dont ses données sont exploitées. Les résultats seront publiés à l'automne 2016 mais la CNIL annonce d'ores et déjà qu'elle mènera des contrôles plus formels si elle détecte des anomalies importantes s'agissant du respect de la loi de 1978. L'audit étant international, il sera possible d'avoir une perception globale du phénomène des objets connectés « grand public » et de la manière dont les exploitants de ces objets utilisent les masses de données qu'ils collectent.

https://www.cnil.fr/fr/internet-sweep-day-2016-comment-les-objets-connectes-du-quotidien-impactent-la-vie-privee

RETOUR

# *POLITIQUE DE SÉCURITÉ*


***132-16-PS-01*** **INAUGURATION DU CENTRE EURO-MÉDITERRANÉEN DE SIMULATION DES RISQUES (CESIR) (FÉVRIER)**

Le ministre de l'Intérieur a inauguré, le 29 janvier 2016, le Centre Euro-méditerranéen de Simulation des Risques (CESIR) à Valabre (Bouches-du-Rhône). Le CESIR est la suite d'une démarche novatrice initiée en 2001 pour la formation des sapeurs-pompiers et des acteurs de sécurité civile sur simulateur. Les améliorations apportées aux scénarii futurs de situations de crise permettent désormais de traiter le feu de forêts, l'inondation, les tremblements de terre, les accidents chimiques… La réalité virtuelle de très haute définition devrait plonger les stagiaires dans une dimension très proche de la réalité. Centre unique dans son concept, il dispose de 800 $m^2$ d'espace high-tech de simulation, de 2 postes complets de pilotage hélico et avion et d'un poste de commande bateau. Disposant d'une salle de conférence de plus de 200 places avec cabines de traduction permettant de suivre l'exercice de simulation en cours, 24 à 32 acteurs peuvent intervenir en simultané dans un environnement 3D virtuel. En fonction de sa demande, chaque participant pourra ainsi acquérir, approfondir, tester, vérifier ou découvrir son domaine de compétence et/ou d'activité. Après avoir défini un besoin, l'équipe élabore un scénario opérationnel qui est ensuite traduit techniquement. Il est, par exemple, possible de scénariser un exercice de lutte contre les pollutions en mer, un accident mettant en cause un transport de substances dangereuses dans une commune ou un exercice de gestion de crise suite à un accident d'aéronef sur une plateforme aéroportuaire... Le programme de la formation alterne exercices pratiques et conférences. Il accueille jusqu'à 5 000 stagiaires par an.

http://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Inauguration-du-Centre-Euro-mediterraneen-de-Simulation-des-Risques
http://www.entente-valabre.com/blog/215/48/inauguration-du-cesir-par-monsieur-bernard-cazeneuve-ministre-de-l-rsquo-interieur-et-monsieur-christos-stylianides-commissaire-europeen

***132-16-PS-02*** **UN BOUTON « SOS » CONTRE LES TERRORISTES**

La ville de Nice (Alpes-Maritimes) vient de doter six salles de spectacle d'un dispositif d'alarme constitué d'un boîtier en plastique avec un bouton rouge sur lequel est marqué « SOS ». Si un responsable du site ou un agent de sécurité appuie sur le bouton, une alerte est déclenchée au Centre de supervision urbain (qui traite 24 heures sur 24 les images des 1 260 caméras de vidéoprotection de la commune). Le directeur de la police municipale explique qu' « en 4 secondes, les opérateurs localisent précisément d'où vient le problème. Ils voient alors les images à l'extérieur pour une levée de doute, puis celles du propre

réseau de caméras à l'intérieur de la salle ». Les agents composent un numéro de téléphone GSM et ont ainsi la possibilité d'entendre le son d'ambiance capté par le micro du boîtier afin de mieux cerner le danger. Le système, déjà expérimenté dans plusieurs commerces niçois, présente, selon le maire de Nice, l'avantage d'être « préventif et de donner la possibilité de vérifier qu'il ne s'agit pas d'une fausse alerte ». Il ajoute que « si la menace est avérée, le dispositif permet de juger la situation en direct, de guider les gestes et la prise de décision des policiers, pompiers, urgentistes ».

http://www.leparisien.fr/espace-premium/actu/contre-les-terroristes-un-bouton-sos-04-05-2016-5765263.php

### *132-16-PS-03* LES DRONES, OUTILS DE LA VIDÉOPROTECTION DES COLLECTIVITÉS ? (SEPTEMBRE)

La technologie des drones est suffisamment développée pour être en mesure d'offrir un nouvel usage. Ainsi, le maire d'Asnières-sur-Seine (92) envisage son utilisation sur l'espace public pour prolonger l'action de la vidéoprotection fixe. Cette idée semble faire d'ailleurs l'unanimité au sein de la municipalité. Le but affiché du développement de ce moyen mobile est de lutter contre la délinquance. La vidéoprotection fixe ne permet pas, en effet, de tout contrôler.
L'édile considère que les libertés publiques et individuelles ne seraient pas mises en danger, la technologie étant, selon lui, aboutie pour que l'outil soit en capacité de flouter les parties privatives.
Pour autant, d'un point de vue opérationnel, les forces de sécurité intérieure ne l'utilisent que dans des cadres particuliers, notamment à l'occasion de grands rassemblements. Il ne s'agit pas alors de lutter contre la délinquance mais bien de disposer d'une vue d'ensemble du terrain pour mieux répartir policiers et gendarmes.

*NDR : L'idée de l'emploi des drones dans la vidéoprotection d'une collectivité territoriale est toute récente et pour l'heure isolée. Si des solutions technologiques existent probablement, il n'en demeure pas moins que les conditions pratiques d'utilisation restent à définir au même titre que l'usage, le stockage, la transmission des images captées et la sécurité de l'appareil utilisé. La gendarmerie a posé, quant à elle, une réflexion approfondie sur l'usage et les capacités du drone en matière de sécurité, notamment dans la préparation et l'aide aux opérations.*

http://www.lefigaro.fr/actualite-france/2016/08/31/01016-20160831ARTFIG00176-les-drones-la-solution-securitaire-pronee-par-le-maire-d-asnieres-sur-seine.php
http://fr.calameo.com/read/002719292ef245da9a83b?page=53

### *132-16-PS-04* DRONES CIVILS : ÉVOLUTION DE LA RÉGLEMENTATION (NOVEMBRE)

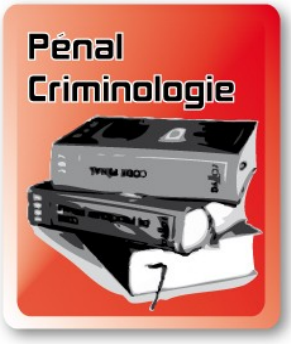
La loi 2016-1428 du 24/10/2016 vient modifier le Code des transports s'agissant des

drones. Un enregistrement des drones devient obligatoire pour tous les modèles dont la masse est supérieure à 800 grammes (un arrêté fixera la limite qui ne peut pas être supérieure à 800 grammes). Une formation du pilote est obligatoire si la masse de l'engin dépasse un seuil fixé par arrêté et qui ne peut être supérieur à 800 grammes. Ces mêmes engins doivent disposer d'un dispositif de signalement lumineux et électronique ou numérique ainsi que d'un système de limitation de leurs capacités. En cas de perte de contrôle par le pilote, un dispositif sonore doit se déclencher.
L'article L.6232-12 crée une infraction de survol par maladresse ou négligence de zone interdite (telle que définie par l'art. L.6211-4) passible d'une peine de 6 mois d'emprisonnement et de 15 000€ d'amende. En cas de volonté avérée de survol malgré l'interdiction, les peines sont portées à un an d'emprisonnement et 45 000€ d'amende. Le drone peut par ailleurs être confisqué.
Ce texte durcit considérablement les sanctions et donne aux forces de l'ordre des outils mieux adaptés pour lutter contre les pilotes qui, par ignorance ou de façon délibérée, contreviennent aux restrictions de survol imposées pour des raisons d'ordre militaire ou de sécurité publique.

https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000033293745

RETOUR

# *PÉNAL-CRIMINOLOGIE*




## *132-16-PC-01* CRIME ORGANISÉ SUR INTERNET : ÉTAT DE LA MENACE (NOVEMBRE)

Europol a mis en ligne son estimation annuelle de la menace représentée par le crime organisé sur Internet. Ce rapport 2016 pointe la nécessité de disposer d'outils juridiques et de réponses judiciaires adaptées, c'est-à-dire rapides et capables de faire face aux évolutions permanentes de la menace. La réalité des conséquences matérielles de la criminalité sur Internet (souvent ressentie comme indolore et virtuelle) devrait notamment être mieux perçue, d'où la nécessité d'une action préventive très forte.
La menace la plus commune s'agissant des logiciels malveillants concerne les « cryptowares », ces logiciels qui encryptent les disques durs et soumettent ensuite leur accès au paiement d'une rançon. Les abus sexuels sur les enfants constituent un secteur en développement, notamment sur le Dark Net, les procédés de chiffrement de bout en bout permettant désormais aux criminels de proposer des vidéos de ce type en direct (et à la demande) depuis des pays pauvres qui n'assurent qu'une faible protection des mineurs. Par ailleurs, les mineurs sont de plus en plus ciblés par des criminels qui, après avoir gagné leur confiance, parviennent à obtenir une image ou une vidéo à caractère sexuel puis en obtiennent davantage par chantage (menace de publier les images par exemple). Les réseaux sociaux, les forums de jeu et les jeux en ligne constituent les terrains de chasse de ces prédateurs sexuels.
S'agissant de fraude à la carte bancaire, 66 % des sommes en jeu concernent des escroqueries en l'absence de la carte physique (c'est-à-dire avec les seules données de la carte). Les achats frauduleux concernent des biens physiques mais aussi les billets d'avion, les séjours en hôtel ou les locations de véhicules. L'industrie du transport aérien estime ses pertes à plus d'un milliard de dollars par an. L'achat frauduleux de billets d'avion est d'autre part souvent en lien avec le crime organisé ou le terrorisme. Il convient enfin de noter que la technologie sans contact (puces NFC) commence à être l'objet de fraudes, notamment pour le paiement sans contact avec les téléphones.
Ce rapport, extrêmement complet, brosse un panorama très large de la criminalité sur Internet, chaque thématique étant traitée sous l'angle des tendances lourdes de l'année, des évolutions majeures et des réponses à apporter.

https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

## *132-16-PC-02* NOUVELLE PISTE POUR LES INVESTIGATIONS CRIMINELLES (NOVEMBRE)

Sur tous les appareils tactiles, nous laissons de nombreuses traces, molécules, produits

chimiques, bactéries, même après nous être lavé les mains ou avoir essuyé la surface de l'écran. Une équipe universitaire de Californie a procédé à l'analyse de 500 prélèvements sur 39 téléphones portables et sur une main de chacun de leurs propriétaires, grâce à une technique de spectrométrie de masse. Elle a permis de déterminer le sexe de l'utilisateur, son type d'alimentation, une prise éventuelle de médicaments, l'utilisation d'insecticides… Ainsi, cette méthode pourrait permettre de repérer des individus parmi des profils recherchés dans le cadre d'enquêtes criminelles. Elle n'est pas aussi fiable pour le moment que des empreintes digitales mais est considérée comme relativement « précise » et sera améliorée. Pour cela, il est nécessaire de constituer une base de données de molécules très fournie qui contiendrait celles « de nourritures communes, de matériaux utilisés dans les vêtements et les tapis, de peinture murale et de tout ce qui peut être en contact avec les personnes ».

http://www.courrierinternational.com/article/microbiologie-montre-moi-les-traces-sur-ton-telephone-et-je-te-dirai-qui-tu-es
http://passeurdesciences.blog.lemonde.fr/2016/11/16/ce-que-votre-portable-dit-de-vous-chimiquement/

## *SÉCURITÉ ROUTIÈRE*


### *132-16-SR-01* LE PNEUMATIQUE ITALIEN INTELLIGENT SUR LES ROUTES POUR 2017 (JANVIER)

L'Italie prend place sur le marché de la voiture connectée. La start-up Wriggle Solutions, fruit d'ambitions toscanes, a développé le projet Smart tyre. Elle a breveté un système permettant de relever le taux d'usure des pneumatiques et d'évaluer leurs dommages éventuels afin de les transmettre directement au conducteur. Le système tend à s'insérer à l'avenir dans les technologies des ordinateurs de bord par le biais d'algorithmes complexes. Il suggère au conducteur le moment opportun pour changer ses pneumatiques.
Les mérites de cette technologie sont vantés de toutes parts. Elle permettrait de prévenir les accidents, qui dans près d'un cas sur deux en Italie, sont dus à un défaut d'entretien des pneumatiques. Elle permettrait aussi de réduire la consommation d'énergie du véhicule.
Encore en phase d'expérimentation, la mise sur le marché du système est prévue pour 2017. La start-up ambitionne ainsi d'accroître le marché de l'autoconnectée, tout en gardant à l'esprit la volonté de contribuer à améliorer la sécurité routière.
Selon des statistiques américaines, les technologies du pneumatique intelligent représenteront un chiffre d'affaire de 5,6 milliards de dollars à l'horizon 2019. Un tel développement impactera à l'avenir les politiques assurantielles.
De son côté, le géant Michelin travaille depuis plusieurs années sur ce type d'innovation et tend à lancer les pneus connectés pour poids lourds. Le projet « Michelin Time Care » vise à proposer aux entreprises de transport routier et aux opérateurs d'autobus urbains la gestion et le diagnostic de leurs pneumatiques à l'aide de technologies numériques. Il permettrait à ces entreprises de réaliser des économies non négligeables.
En attendant, le pneu connecté est déjà à l'œuvre dans plusieurs compétitions automobiles.

http://corriereinnovazione.corriere.it/2016/01/04/pneumatico-intelligente-dimezzare-incidenti-b628cf1c-b2d7-11e5-8f58-73f8cf689159.shtml
http://www.lepoint.fr/automobile/actualites/pneus-connectes-michelin-lance-une-solution-pour-poids-lourds-en-europe-05-10-2015-1970912_683.php

### *132-16-SR-02* LA FIN ANNONCÉE DES RÉTROVISEURS EXTÉRIEURS ? (FÉVRIER)

Aux États-Unis, l'équipementier de voitures Continental propose les rétroviseurs numériques en lieu et place des traditionnels rétroviseurs extérieurs. Le principe est assez simple, des caméras captent les vues sur l'arrière et les côtés du véhicule. Ces vues sont ensuite diffusées sur un ou des écrans dans l'habitacle dans le champ de vision du conducteur.
Les expérimentations ont débuté en Asie et aux États-Unis. L'Europe devrait tester cette technologie dès 2016.

Les arguments pour passer à cette nouvelle technologie sont assez nombreux. Outre le fait d'améliorer sensiblement le design de la voiture, la suppression des rétroviseurs extérieurs améliorerait le confort de conduite par la réduction du bruit qu'ils provoquent habituellement. De plus, leur retrait permettrait une économie de consommation de carburant, les protubérances extérieures générant une résistance à l'air. Deux autres arguments sont à considérer. Le premier touche à la sécurité. En effet la qualité des capteurs permet aujourd'hui de résoudre la problématique des angles morts. Dans cet ordre d'idées, certaines technologies complémentaires au rétroviseur numérique permettraient de détecter et d'alerter le conducteur de la présence d'obstacles mobiles à prendre en compte. Le second argument est économique. Aujourd'hui, remplacer un rétroviseur endommagé représente un coût de près de 900$ si l'on prend en compte le clignotant, le système de dégivrage, le réglage électrique ou encore le design.
Le rétroviseur numérique apparaît donc comme une solution bénéfique pour le confort, la sécurité et le porte monnaie du conducteur.
Pour autant, les essais réalisés montrent que la bonne utilisation de ce nouveau dispositif nécessite une certain entraînement pour les conducteurs.

www.nytimes.com/2016/02/05/automobiles/end-of-the-road-may-be-near-for-side-mirrors.html

### *132-16-SR-03* LUNETTES INTELLIGENTES ANTI-ÉBLOUISSEMENT (FÉVRIER)

L'équipementier français VALEO a présenté au CES de Las Vegas 2016 des lunettes intelligentes anti-éblouissement afin d'améliorer la visibilité du conducteur. Cet objet connecté s'assombrit lorsqu'un capteur mesure une forte luminosité. De jour, ces lunettes s'adaptent ainsi automatiquement à la luminosité variable (conditions climatiques, tunnel...). De nuit, elles évitent au conducteur de se faire éblouir par les phares des voitures venant en sens inverse. À ce stade, les lunettes « by Valeo » ne sont qu'une démonstration technologique, aucune date de commercialisation n'est communiquée.

http://www.clubic.com/mag/transports/actualite-792042-les-lunettes-by-valeo-conduite-de-nuit.html

### *132-16-SR-04* L'ONU ANNONCE LA RÉVISION DE LA CONVENTION DE VIENNE AU PROFIT DES VOITURES AUTONOMES (AVRIL)

Depuis 1968, la circulation routière est régulée par la Convention de Vienne. Mais le 23 mars 2016, sa révision a été annoncée par la Commission économique des Nations Unies pour l'Europe (UNECE). Celle-ci vise à autoriser officiellement les systèmes de conduite automatisés sur les routes dès lors qu'ils se révèlent conformes *« aux règlements des Nations Unies sur les véhicules ou qu'ils puissent être contrôlés voir désactivés par le conducteur ».* Elle tient ainsi en échec l'article 8 de la Convention prévoyant que *« tout conducteur doit constamment avoir le contrôle de son véhicule ».*
Par la suite, il est prévu qu'une liste des véhicules autorisés soit établie.

Dans tous les cas, le conducteur devra pouvoir conserver un contrôle permanent sur le véhicule afin de parer à une défaillance éventuelle de trajectoire ou de vitesse.
Si les choses avancent correctement, la nouvelle réglementation devrait être en place aux alentours de 2017.
Mi-mars 2016, les États-Unis s'étaient déjà accordés sur l'adoption d'un freinage automatique d'urgence d'ici 2022. La future révision viendra donc compléter cette mesure.
Pour le moment, certains pays européens comme l'Allemagne, la France, le Royaume-Uni ou la Suède autorisent les essais sur routes ou autoroutes dans des conditions bien spécifiques.
La question des véhicules autonomes doit également être abordée mi-avril à l'occasion d'un sommet informel des ministres des transports à Amsterdam.
Le principal obstacle que représentait la Convention de Vienne à la mise en circulation des véhicules autonomes est désormais tombé. Dès lors, la transition vers l'autonomisation des véhicules semble plus que jamais se dessiner et tend à réduire l'accidentologie routière.

http://www.latribune.fr/entreprises-finance/industrie/automobile/voiture-autonome-l-onu-leve-le-verrou-reglementaire-559443.html
http://www.lemonde.fr/economie/article/2016/03/24/la-reglementation-internationale-autorise-desormais-la-voiture-autonome_4889485_3234.html

### *132-16-SR-05* EXPÉRIMENTATION DE VÉHICULES À DÉLÉGATION DE CONDUITE SUR LES VOIES PUBLIQUES (SEPTEMBRE)

Publiés au Journal officiel du 5 août 2016, un rapport et une ordonnance encadrent les conditions de l'expérimentation de véhicules à délégation de conduite sur les voies publiques. Cette ordonnance fait suite à l'application du chapitre IX de l'article 37 de la loi 2015-992 du 17 août 2015 relative à la transition énergétique pour la croissance verte.
L'ordonnance habilite le gouvernement à prendre « toute mesure relevant du domaine de la loi afin de permettre la circulation sur la voie publique de véhicules à délégation partielle ou totale de conduite, qu'il s'agisse de voitures particulières, de véhicules de transport de marchandises ou de véhicules de transport de personnes, à des fins expérimentales, dans des conditions assurant la sécurité de tous les usagers et en prévoyant, le cas échéant, un régime de responsabilité approprié ». L'expérimentation du « véhicule autonome » sur les voies publiques présente plusieurs objectifs : valider le niveau de sécurité, observer l'acceptabilité sociale, étudier sa capacité d'intégration dans le système de transport existant et évaluer ses performances. La terminologie retenue « Véhicule à Délégation Partielle ou Totale de Conduite » (VDPTC) vise, d'une part, à faire référence aux technologies d'automatisation avancées de ce type de véhicule et d'autre part, à mettre en exergue le changement fondamental de nature de l'acte de conduire. Un décret en Conseil d'État précisera prochainement les conditions de délivrance de l'autorisation et les modalités de mise en œuvre du VDPTC.

*NDR : L'Observatoire Central des Systèmes de Transport Intelligents (OCSTI) représente la gendarmerie nationale dans le groupe interadministrations en charge de mener les réflexions sur l'évolution du cadre réglementaire et normatif, respectivement dans le champ*

*de l'expérimentation et la mise en œuvre sur le marché.*

https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000032966690
https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000032966695

### *132-16-SR-06* PARUTION D'UNE ÉTUDE RELATIVE AUX ACCIDENTS DE CIRCULATION LIÉS AUX « SMOMBIES » (MAI)

En Europe, 22% des accidents mortels sur route concernent des piétons, accidents survenant majoritairement en ville. La dernière enquête menée par le département de recherche en accidentologie du groupe Dekra révèle un nouveau fléau, celui des accidents de la circulation liés au piétons connectés. Publié en avril 2016, le rapport de Dekra souligne le lien de causalité entre « smombies » (contraction de smartphone et zombie) et accident de circulation. Après une première étude menée à Stuttgart, un sondage élargi a été effectué dans six capitales européennes (Amsterdam, Berlin, Bruxelles, Paris, Rome et Stockholm) où 14 000 piétons ont été interrogés. Les lieux ont été choisis en tenant compte du niveau de densité des piétons : gares, arrêts de bus et stations de métro. Premier constat, 17% de ces piétons « sont régulièrement distraits par leur smartphone lorsqu'ils traversent des voies de circulation », selon le rapport. Dans le détail, environ 8% des piétons ont été aperçus en train d'envoyer un SMS pendant qu'ils traversaient la route tandis que 2,6% téléphonaient et que 1,4% faisaient les deux en même temps. Près de 5% des sondés portaient des écouteurs diffusant de la musique. C'est la tranche d'âge 25-35 ans qui utilise le plus son smartphone et représente 22% de plus par rapport aux autres tranches d'âge. Parmi cette tranche d'âge, la distinction est faite entre les femmes qui ont une préférence pour les SMS (11,44% des Parisiennes) et les hommes qui optent pour la musique (8,28% des Parisiens). Amsterdam a le taux d'usage du smartphone par le piéton le plus faible avec 8,2%, suivi par Rome avec 10,6% et Bruxelles à 14,12%. Paris et Berlin sont au coude à coude avec respectivement 14,53% et 14,9%. Le taux d'usage du smartphone par piéton le plus élevé est de 23,55 % et concerne la ville de Stockholm.
Des solutions sont mises en place dans certains pays comme l'Allemagne : la ville d'Augsburg, en Bavière, a décidé de mettre en place des feux de circulation au sol, seul moyen pour que ces derniers entrent dans le champ de vision des « zombies du smartphone ». Quand les LED clignotent au rouge, les piétons sont invités à s'arrêter. À l'inverse, une lumière verte annonce que la voie est libre. Pour le moment, seuls deux arrêts de tramway particulièrement fréquentés par les étudiants en sont équipés mais la municipalité annonce d'ores et déjà une future généralisation du système. Par ailleurs, la ville d'Anvers a créé dans son centre-ville une voie exclusivement destinée aux accros du smartphone, « la voie pour texto ».

http://www.lesnumeriques.com/volant/dekra-17-pourcent-pietons-distraits-par-smartphone-n52123.html
http://www.dekra-vision-zero.com/downloads/road_safety_report_2015.pdf
http://www.tomsguide.fr/actualite/feux-signalisation-sol,51222.html#xtor=RSS-20
http://www.liberation.fr/france/2016/05/11/le-nez-sur-le-smartphone-les-pietons-se-mettent-en-danger_1451940

## *132-16-SR-07* ÉTUDE EUROPÉENNE SUR L'UTILISATION DES PLAQUES D'IMMATRICULATION RFID (OCTOBRE)

Le principe des plaques d'immatriculation RFID consiste en l'intégration d'une puce RFID (Radio Frequency IDentification) unique à la plaque minéralogique. Une expérimentation réalisée par NXP Semiconductors a commencé fin 2015 sur une base militaire aux Pays-Bas avec des voitures et des camions équipés de IDePLATEs (plaques RFID) et IDeSTIXs (étiquettes de pare-brise) avec des puces RFID passives intégrées.
Cette étude a été conduite sur une durée d'un an sur plus de 100 véhicules militaires et a confirmé l'utilisation sûre et fiable de la RFID pour l'identification du véhicule, dans diverses conditions météorologiques et à des vitesses de près de 100 miles par heure. La RFID dans des plaques d'immatriculation peut conduire à d'autres applications telles que la collecte de la taxe automatisée dans les garages de stationnement, si les propriétaires de voitures en acceptent les termes au préalable.
Concrètement, ces plaques d'immatriculation peuvent être identifiées jusqu'à 12 m par les portiques prévus à cet effet. Les dernières technologies de déchiffrage sont utilisées pour garantir l'inviolabilité de la puce. Quant à la détection, elle peut se faire à des vitesses jusqu'à 150 km/h. Une telle technologie permettrait d'automatiser de nombreuses opérations payantes sur les routes, comme le franchissement d'un péage ou l'utilisation d'un parking. Actuellement, le LAPI, ou Lecteur Automatique de Plaques d'Immatriculation, est en mesure d'offrir de telles facilités, par contre son degré de fiabilité est inférieur.

http://www.filrfid.org/2016/07/une-etude-europeenne-ouvre-la-voie-a-des-plaques-d-immatriculation-rfid.html

## *132-16-SR-08* CONCEPTION SMILING-CAR (NOVEMBRE)

Une société suédoise Semcon et un institut de recherches suédois, Viktoria Swedish ICT , travaillent sur un concept de voiture autonome capable d'afficher un sourire électronique à l'égard d'un piéton pour lui signaler qu'il peut traverser la chaussée. Un écran électronique placé au niveau de la calandre affiche un large sourire indiquant aux usagers de la route qu'elle les a pris en considération et qu'elle va s'arrêter. La voiture souriante de Semcon est dans ses premières phases de développement et l'entreprise espère ajouter des capteurs capables de détecter précisément les mouvements du regard ou de la tête d'un usager de la chaussée. Ce dispositif a été conçu dans le but de rassurer les piétons hésitant à traverser la chaussée car, selon Semcon, 8 piétons sur 10 recherchent le regard des conducteurs avant de traverser la route. Le responsable de l'expérience chez Semcon insiste sur la nécessité de réfléchir à une vraie interaction entre les véhicules autonomes et les usagers de la route les plus fragiles.
http://www.nouvellestechnologies.net/cette-voiture-sourit-aux-pietons-pour-qu-ils-traversent.php

RETOUR

## *SÉCURITÉ PRIVÉE*


### *132-16-SP-01* WEBDRONE CHASSE LA CONTREFAÇON ET LES AUTRES FORMES DE CYBERCRIMINALITÉ SUR LE NET (JUIN)

Au sein d'une entreprise basée à Dijon, un ancien enquêteur de la gendarmerie spécialisé dans la cybersécurité et la cyberdéfense et son associé, spécialiste de l'intelligence économique, ont développé un système accessible en mode SaaS (Software as a Service : location à la demande sur Internet) pour traquer et démanteler des trafics de contrefaçon, baptisé Webdrone.
Depuis 2013, des drones virtuels opèrent sur Internet pour détecter les cybercriminels s'attaquant aux clients de l'entreprise, entre autres des industriels du luxe et des grandes marques. Une vingtaine de personnes, réparties en deux pôles, composent cette entreprise. Le premier, dédié à la veille et à l'expertise, est constitué d'anciens gendarmes spécialisés dans l'investigation numérique. Le second, le pôle développement, est chargé de faire évoluer la plateforme.
Disponible aujourd'hui dans une version 2.0, Webdrone utilise des « drones » programmés pour repérer les cyberdélinquants, établir les liens qu'ils ont entre eux et rapporter ainsi des informations aux clients. Ces « robots d'enquête » sont capables de couvrir rapidement le Web visible mais aussi le Deep Web (regroupant des contenus non indexés par des moteurs de recherche) et le Dark Web (dont les contenus sont cryptés, la règle étant l'anonymat et les activités majoritairement illicites).
Grâce à Webdrone, de nombreuses affaires ont été résolues, la plus significative portant sur « *le démantèlement en moins de 6 mois d'un réseau d'une centaine de milliers de personnes participant à un trafic portant sur plusieurs millions d'objets contrefaits, pour un préjudice de plus de 70 millions d'euros* ». Suivant la complexité des recherches demandées, le prix de l'abonnement peut varier de quelques milliers à quelques dizaines de milliers d'euros. Un nouveau module vient compléter l'offre, permettant de faire des enquêtes sur des personnes morales ou privées, de quoi intéresser les entreprises voulant « en savoir plus sur un futur partenaire, un nouveau collaborateur ou un client ».
L'entreprise a prévu d'ouvrir en octobre 2016 un bureau à Paris, un autre dans l'avenir à Singapour.

http://www.infoprotection.fr/CYBERSECURITE/

### *132-16-SP-02* RISQUE CYBER ET GOUVERNANCE EN ENTREPRISE (OCTOBRE)

Le CIGREF, réseau des grandes entreprises, a diffusé le 7 octobre 2016, sur son site Internet, un rapport portant sur le risque cyber en entreprise et sur la façon, pour les organes dirigeants de l'entreprise, de l'appréhender. Partant du constat que, si le risque cyber est désormais une réalité qui touche l'ensemble des entreprises, il est néanmoins difficile d'obtenir des budgets pour permettre à l'entreprise d'y faire face, les auteurs

appellent à concentrer les efforts dans trois domaines : l'implication de l'équipe de direction et le développement de compétences, l'appréciation réelle du niveau de prise en compte du risque cyber dans le fonctionnement habituel de l'entreprise et la définition du niveau de risque auquel le dispositif de gestion des risques de l'entreprise doit pouvoir faire face. L'identification du patrimoine essentiel de l'entreprise (celui dont la perte ou la divulgation met en péril l'entreprise) doit notamment être faite de façon particulièrement soignée. Pour les auteurs, l'engagement du comité exécutif de l'entreprise dans ces questions doit être à la hauteur des enjeux et garantit que les bonnes réponses seront apportées. Le rapport évoque la façon d'introduire ces questions auprès des dirigeants et du comex ainsi que la nature des réponses possibles face à une menace polymorphe. La mise en place d'indicateurs pertinents est ainsi suggérée. La question de l'assurance est aussi évoquée.
Ce document de 21 pages est avant tout destiné à sensibiliser les entreprises au risque cyber. Il souligne l'intérêt capital que représente l'implication directe des dirigeants en termes de certitude de réelle prise en compte de ces questions vitales pour la survie des entreprises.

http://www.cigref.fr/rapport-cigref-cyber-risque-dans-la-gouvernance-de-l-entreprise

RETOUR

## *EUROPE*


### *132-16-EU-01* PARUTION DU RÈGLEMENT EUROPÉEN DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL (MAI)

Règlement très attendu par l'ensemble des opérateurs publics et privés relevant de l'espace européen, le texte final a été publié au Journal Officiel de l'Union européenne le 4 mai 2016. Le règlement 2016/679 porte sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Dans les considérants qui précèdent la rédaction des articles, leur rédacteur émet toute une série de déclarations d'intention sur la portée qu'il entend donner à ses dispositions. Tout en rappelant que la protection des données à caractère personnel constitue un droit fondamental, le règlement ne va pas jusqu'à lui consacrer un statut de droit absolu. Ce droit fondamental doit être mis en balance avec les autres droits fondamentaux, conformément au principe de proportionnalité. Le règlement reconnaît aussi que toute personne physique devrait avoir le contrôle de ses données personnelles. Sur la notion de données à caractère personnel, le règlement a élaboré une définition qui fera autorité auprès des différentes instances de jugement des États de l'Union européenne. Les données à caractère personnel sont : « toute information se rapportant à une personne physique identifiée ou identifiable. Une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. »

*NDR : Le règlement entre en vigueur le 24 mai 2016 pour une application à partir du 25 mai 2018. En vue de le rendre le plus accessible possible, les acteurs investis de fonctions de régulation de chacun des États membres sont encouragés à élaborer des codes de conduite. Ces codes s'avéreront indispensables en raison de « la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises ».*

http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&rid=1

### *132-16-EU-02* EUROPOL ÉLARGIT SES COMPÉTENCES EN LIGNE (MAI)

Le Parlement européen a adopté le 11 mai 2016 de nouvelles règles de gouvernance afin de renforcer les actions d'Europol dans la lutte contre le terrorisme, la cybercriminalité et d'autres infractions pénales. L'agence Europol pourra obliger les sites à retirer la propagande terroriste. Depuis juillet 2015, une unité chargée du signalement des contenus sur Internet parcourt déjà les sites accessibles au public pour trouver des contenus de nature terroriste.

Les députés favorables à ces nouvelles règles rappellent que l'incitation à la haine et à la violence en ligne favorise le passage à l'acte. Par ailleurs, les entreprises pourront plus difficilement s'opposer à une demande de suppression émanant d'une autorité communautaire, ce qui représente une nouvelle étape en termes de coopération. D'autres députés, par contre, craignent des dérives dans la gestion et la définition des données à détruire.
Le règlement entrera en vigueur 20 jours après sa publication au Journal Officiel de l'UE et sera d'application à partir du 1er mai 2017.

http://www.euractiv.fr/section/innovation-entreprises/news/activists-wary-of-data-super-authority-europol-as-reform-looms/?nl_ref=12855843
http://www.europarl.europa.eu/news/fr/news-room/20160504IPR25747/europol-de-nouveaux-pouvoirs-afin-de-renforcer-la-lutte-contre-le-terrorisme
http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com%282013%290173_/com_com%282013%290173_fr.pdf

## *INTERNATIONAL*


### *132-16-IN-01* VRAIES VIES, VRAIS CRIMES (JANVIER)

Le HMIC (Her Majesty's Inspectorate of Constabularies) a mis en ligne une étude intitulée « *real lives, real crimes - a study of digital crime and policing* » et portant sur la criminalité numérique et la répression de cette dernière. Ainsi que le précise dans son introduction un inspecteur, « le public a le droit de demander de chaque policier ou membre de la police avec qui il entre en contact (que ce soit son interlocuteur de base ou un enquêteur spécialisé) une action rapide et des conseils de bonne qualité quant à la meilleure manière de traiter ceux qui commettent des crimes numériques ». Le rapport se penche sur les effets des technologies digitales sur la délinquance et l'action policière. Il rappelle en préambule que 36 millions de Britanniques adultes ont eu accès à Internet en 2013 et que 53 % de la population utilise son téléphone pour accéder à Internet, les jeunes connaissant la progression la plus foudroyante. Il souligne ainsi l'intérêt pour la police de traiter cette délinquance avec sérieux.
La rapport s'appuie sur des cas concrets tirés de la vie courante. Il se place du côté de la victime pour comprendre ses attentes et analyse les réponses données par la police. Il porte également un regard sur la formation des policiers (qui repose notamment, pour les non spécialistes, sur des cours en ligne comprenant quatre modules). S'agissant des spécialistes, une formation spécifique est en place, comprenant 5 jours de formation en ligne et 5 journées de cours en classe. Le budget permettra de former 800 policiers en 2015-2016. Le rapport précise que la matière étant très technique, il est nécessaire de recourir au secteur privé pour fournir certaines formations très spécifiques.
D'une manière générale, les rédacteurs passent en revue l'ensemble des moyens mis à disposition des services de police dans le domaine de la lutte contre la cybercriminalité. En conclusion générale de l'étude, ils notent que ces services doivent pouvoir évaluer l'ampleur des phénomènes criminels et leur impact, s'agissant de cyberdélinquance, tant au niveau local que national. Ils soulignent qu'il est également nécessaire d'avoir une gouvernance et une stratégie impliquant tant les services publics que le secteur privé. La question de la formation est jugée essentielle, de même que celle de la prise en compte effective des besoins des victimes par les services de police. Chaque chef de police devrait notamment s'assurer qu'il dispose bien des personnels qualifiés pour traiter avec rapidité et efficacité les éléments électroniques susceptibles de contenir des éléments de preuve. Le rôle des instances nationales est enfin souligné, de même que la nécessité de porter rapidement à leur connaissance les affaires dont les policiers sont saisis.

http://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

### *132-16-IN-02* UN ROBOT-AVOCAT POUR CONTESTER LES CONTRAVENTIONS

**(MARS)**

Un étudiant de Stanford a créé, fin 2015, un programme informatique « DoNotPay » (« Ne payez-pas » ) qui établit un argumentaire juridique pour porter réclamation d'une contravention. Certains le surnomment déjà le « robot-avocat » même s'il est incapable pour le moment d'assurer une réelle plaidoirie. Il est gratuit et accessible à tous. Il fonctionne sous forme de questions-réponses pour, à la fin, établir une lettre de contestation qu'il suffit d'envoyer au tribunal.
Encore au stade d'essai, ce robot connaît un taux de réussite de 47% soit la suppression de 95 000 contraventions et une économie de 3 millions de dollars d'amende.
Son succès est tel que son concepteur a d'ores et déjà élargi la compétence de son robot-avocat aux retards de trains et d'avions et envisage de développer son produit à New-York, au Canada et à Mexico.

http://etudiant.lefigaro.fr/les-news/actu/detail/article/un-etudiant-cree-un-robot-avocat-qui-annule-les-contraventions-19229/
http://tempsreel.nouvelobs.com/l-histoire-du-soir/20160223.OBS5205/un-etudiant-invente-un-robot-juriste-capable-de-faire-sauter-les-contraventions.html

### *132-16-IN-03* LA POLICE BRITANNIQUE ET L'ENSEIGNEMENT SUPÉRIEUR VONT TRAVAILLER SUR LA CARTOGRAPHIE DES LIEUX À RISQUES (MARS)

Au Royaume-Uni, afin de mieux gérer les ressources, les forces de police sont invitées à développer un outil prédictif sur les lieux et types de faits susceptibles de s'y commettre. Il s'agit donc d'anticiper et de préparer le déploiement des effectifs par une analyse des faits cartographiés.
Le travail d'élaboration de cet outil à caractère prédictif se fera en liaison avec la London school of economics. L'analyse portera sur des milliers de caractéristiques qui permettront de dégager un cadre espace temps pour un type de risque.
Il est évident que tout ne peut être prédit et que des événements imprévus seront à prioriser dans leur traitement.
Cette annonce est critiquée au motif que l'outil viendrait compenser les coupes budgétaires des forces de police d'Angleterre et du Pays de Galle.

*NDR : Le principe de cet outil à caractère prédictif qui vise les points à risque de troubles et de faits de délinquance est déjà en œuvre dans d'autres pays.*

http://www.theguardian.com/uk-news/2016/feb/24/police-developing-new-system-to-identify-hotspots

### *132-16-IN-04* RENDRE LA JUSTICE À L'ÈRE NUMÉRIQUE (MAI)

Le HMIC (*Her Majesty's Inspectorate of Constabulary*) a mis en ligne le 13 avril 2016 un rapport d'inspection intitulé « *Delivering justice in a digital age* », établi conjointement par le

HMIC et le HMCPSI (*Her Majesty's Crown Prosecution Service Inspectorate*). Ce rapport fait le point sur l'adaptation des différentes forces de police et la justice au numérique, tant sur le plan de la digitalisation des procédures que sur celui de la gestion des éléments de preuve numériques. Tout en reconnaissant les progrès réalisés, les rapporteurs constatent que les institutions avancent à des vitesses qui leur sont propres et que de sérieux problèmes de compatibilité entre systèmes continuent à se poser.
S'agissant des avancées constatées, le rapport souligne que la digitalisation a permis de faciliter le travail des policiers et des magistrats. La numérisation donne par ailleurs une flexibilité dans le travail qui n'existait pas précédemment, permettant notamment d'actualiser les procédures en temps réel. Enfin, le déploiement de la vidéo portable individuelle est salué dans le sens où elle permet aux policiers de recueillir des éléments de preuve.
Les tribunaux se sont équipés en ordinateurs individuels et disposent de WiFi ainsi que d'un système simple permettant de projeter sur grand écran des documents. Les différentes forces de police, en revanche, ne sont pas parvenues à se doter de matériels toujours compatibles. De nouvelles règles communes devraient résorber ce problème.
Le rapport propose 8 recommandations et 4 bonnes pratiques.
Certaines recommandations concernent police, magistrats et procureurs, d'autres uniquement un ou plusieurs services. D'une manière générale, les inspecteurs souhaitent une plus grande compatibilité entre les moyens techniques déployés au sein des différents services, y compris entre justice et police. Les initiatives permettant de réduire les déplacements et les courriers physiques, la présentation d'éléments de preuve électroniques et la bonne exploitation des médias saisis dans le cadre des affaires judiciaires constituent également une priorité affichée.
Le dispositif britannique d'inspections conjointes effectuées par des organismes émanant de ministères différents mais relatifs à une mission commune montre ici toute sa pertinence, le spectre complet d'une affaire judiciaire (enquête, instruction, jugement) étant passé en revue de manière globale afin d'identifier les espaces de progrès.

http://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/delivering-justice-in-a-digital-age.pdf

### *132-16-IN-05* PORTRAITS ANTHROPOMÉTRIQUES EN 3D POUR LA POLICE DE TOKYO (AVRIL)

La police de la capitale japonaise peut désormais réaliser les photos d'identité judiciaire en 3D permettant de connaître la forme et le volume exacts d'un visage humain. Afin d'améliorer la reconnaissance faciale des caméras de surveillance et ainsi d'endiguer la criminalité, les 102 commissariats de Tokyo sont équipés depuis avril 2016 d'une caméra 3D photographiant les suspects arrêtés sous trois angles différents, dont on peut faire varier l'éclairage. La section d'identification de la police japonaise est chargée de gérer tous les clichés produits par le nouveau système. L'initiative est partie d'un constat : les photos prises lors d'un acte de délinquance par les caméras de surveillance montrent la plupart du temps des suspects vus d'en haut, les visages orientés vers le bas ou pris de côté. Il était ainsi difficile de les comparer aux classiques photos anthropométriques en deux dimensions de face et de côté. Un travail grandement facilité par ces nouveaux portraits en 3D, comme

l'explique un gradé du département de police : « Vu que nous pouvons identifier et arrêter les suspects plus rapidement et avec une meilleure précision, nous ne pouvons que nous attendre à voir notre taux d'arrestation devenir meilleur ».

https://8e-etage.fr/2016/01/26/la-police-de-tokyo-va-prendre-des-photos-en-3d-de-tous-ses-suspects/
https://www.brief.me/a/20160126/357/1737/flyhNrzuPZ5E/

***132-16-IN-06*** **BELGIQUE : DE JEUNES « CYBER-PATROUILLEURS » CONTRE LA HAINE EN LIGNE (NOVEMBRE)**

Dans le cadre de la campagne « Non à la haine », 31 jeunes Belges, âgés entre 18 et 35 ans, ont été formés pour devenir des « cyber-patrouilleurs » afin de lutter contre l'intimidation et le harcèlement en ligne, rejoignant ainsi les rangs du programme du Conseil de l'Europe de lutte contre les discriminations et la radicalisation. La ministre belge de la Promotion sociale, de la Jeunesse, du Droit des femmes et de l'Égalité des chances, initiatrice du programme, déplore que « les jeunes sont de plus en plus en contact sur Internet avec des propos haineux, pas seulement racistes mais aussi sexistes, des propos discriminatoires ». Que ce soit face à un anonyme mettant un post sur Facebook ou des posts de personnes connues, leur travail est de « calmer le jeu et essayer de ramener la vérité » en vérifiant ce qu'affirment les persécuteurs en ligne. Selon l'UNIA, organisme indépendant de lutte contre la discrimination basé à Bruxelles, 92 % des 365 cas d'incitation à la haine enregistrés en 2015 en Belgique venaient d'Internet, 126 venant plus précisément de Facebook et Twitter. Assurant ne pas vouloir créer une police de l'Internet, la ministre belge souhaite « renforcer la citoyenneté chez les jeunes », qu'ils puissent être critiques par rapport aux images et aux discours afin d'agir ensuite, en ayant suffisamment de connaissances pour convaincre d'autres jeunes. Le gouvernement belge voudrait élargir le programme aux mineurs, qui seraient assujettis à la présence d'un adulte pour ne pas affronter, seuls, des discours menaçants.

http://www.france24.com/fr/20161117-jeunes-cyber-patrouilleurs-belges-contre-haine-ligne

RETOUR

## *ESPACE MARITIME*


***132-16-EM-01*** **THALES DÉVOILE SON NOUVEAU DRONE NAVAL HYBRIDE (NOVEMBRE)**

À l'occasion du salon Euronaval qui s'est déroulé à Paris-Le-Bourget du 17 au 21 octobre 2016, le groupe Thales a dévoilé son nouvel AUSS (Autonomous Underwater & Surface System), un drone naval hybride, d'un diamètre de 53 centimètres, conçu pour opérer aussi bien sous la mer qu'en surface. Développé durant trois ans en étroite collaboration avec 19 PME françaises, l'AUSS est capable d'effectuer des missions civiles comme la surveillance des plateformes pétrolières et militaires, à l'instar de la collecte de renseignements ou encore de la lutte contre le terrorisme maritime. Si sa manœuvrabilité et son agilité à 360 degrés lui permettent de se déplacer dans toutes les directions et d'éviter une menace ou un obstacle en moins de dix mètres, ses capteurs performants assurent la qualité des données recueillies lors des missions. Les cinq essais menés par Thales ont également attesté de son endurance supérieure sur plusieurs semaines et sur de longues distances, répondant ainsi à un besoin de surveillance constant. Pour Thales, ce projet « amorce la création d'une véritable filière drones dans l'industrie navale en France ».

http://www.opex360.com/2016/10/17/thales-presente-drone-hybride-pouvant-operer-la-mer-en-surface/
http://www.leparisien.fr/high-tech/thales-presente-un-drone-naval-hybride-pour-des-missions-civiles-et-militaires-17-10-2016-6218529.php

RETOUR

## *TERRITOIRES ET FLUX*


***132-16-TF-01*** **LA CABINE DÉTACHABLE : L'AVENIR DE LA SÛRETÉ AÉRIENNE ? (FÉVRIER)**

Un ingénieur russe semble avoir trouvé une solution pour que les crashs aériens ne se traduisent pas en drames humains. Pendant plusieurs années, il a réfléchi à l'idée d'une cabine détachable en cas de risque avéré. Il s'agirait d'une capsule éjectable en cas de chute ou d'atterrissage d'urgence. La capsule serait alors séparée du reste de l'avion pour se poser en douceur sur terre ou sur l'eau grâce à deux parachutes s'ouvrant au moment de la chute.
Les passagers seraient épargnés tout comme leurs bagages. Malgré tout, le sort des pilotes se révèle incertain.
Plusieurs spécialistes trouvent cette idée irréaliste. En effet, la probabilité que la cabine se pose en zone urbaine est très élevée. De même, le coût du système est lui aussi pointé du doigt. L'investissement serait conséquent comparé au risque à prévenir.
Pour autant, l'ingénieur a mené sa propre enquête et selon lui 95% des individus interrogés seraient prêts à payer leur billet plus cher si leur avion disposait d'un tel système. Si les chances de voir le projet aboutir sont faibles, il suscite quand même certains espoirs. A cela s'ajoute l'important manque à gagner pour l'industrie aéronautique causé par la peur de l'avion.
Le projet de cabine détachable n'est également pas le premier du genre, Airbus ayant déjà envisagé une telle hypothèse en 2013 afin d'accélérer l'embarquement en transit des voyageurs.

http://www.huffingtonpost.fr/2016/01/16/avion-cabine-detachable-invention-futur-video_n_8998800.html
http://www.lesoir.be/1097813/article/victoire/voyages/2016-01-19/crash-aerien-une-cabine-detachable-pour-sauver-passagers-video

RETOUR


### *132-16-ST-01* LA CALIFORNIE VEUT STRICTEMENT ENCADRER LES VOITURES SANS CONDUCTEUR (JANVIER)

Le Department of Motor Vehicule (DMV) de l'État de Californie a présenté les futures règles susceptibles d'encadrer la mise en circulation des véhicules autonomes sur son territoire. La présence d'un opérateur (autrement dit un conducteur) capable de reprendre immédiatement le contrôle en cas de défaillances technologiques ou d'autres urgences sera obligatoire. Pour le DMV, un permis de conduire spécifique sera de surcroît nécessaire en raison des risques associés au déploiement de cette nouvelle technologie.
Les conducteurs demeureront responsables en cas d'infraction au code de la route ou d'accidents quand le véhicule sera placé sous contrôle automatique. Chaque véhicule devra être titulaire d'une autorisation de mise en circulation valable 3 années. Dans un premier temps, les autorités californiennes exigeront que ce type de véhicule reste la propriété exclusive des constructeurs. Les voitures autonomes ne pourront faire l'objet d'une vente au particulier ou à une entreprise. La finalité de cette dernière disposition est de contraindre juridiquement les constructeurs à fournir des rapports mensuels sur l'utilisation et les performances de leurs voitures avec une obligation de signaler tous les accidents. De ce fait, les données collectées permettront d'évaluer la sécurité et les performances en conditions réelles des véhicules autonomes. Malgré les assurances données par les autorités californiennes sur le caractère provisoire de ces mesures, les concepteurs de cette technologie innovante se montrent visiblement inquiets des annonces faites et n'excluent pas l'hypothèse de délocaliser leur centre de recherche vers un autre État beaucoup plus libéral en la matière.

*NDR : Il s'agit a priori de la première tentative de régulation menée par une autorité publique. Jusque-là, les États fédérés ont favorisé largement les initiatives des industriels en édictant des règles de droit très souples dans les conditions de mise en circulation des voitures autonomes (exemple : loi de l'État du Nevada). Le fait que des industriels soient sur le point de réussir à sortir un prototype pouvant être exploité à grande échelle incite des États comme la Californie à adopter une démarche pro-active dans la gouvernance des données pour ne pas dépendre par la suite de leur bon vouloir.*

http://siliconvalley.blog.lemonde.fr/2015/12/19/la-californie-veut-severement-encadrer-les-voitures-sans-chauffeur/

### *132-16-ST-02* SEA TAGS, BRACELET MARITIME CONNECTÉ (JANVIER)

Produit développé par l'entreprise Marine Assistance International, Sea Tags est un système d'alerte qui se déclenche automatiquement ou manuellement en cas de chute en mer. L'application Sea Tags affiche sur une carte la position de la personne tombée en mer, la

position en temps réel du bateau et elle actualise en permanence le cap et la distance à suivre pour récupérer l'équipier. Composé d'un bracelet émetteur se portant au poignet comme une montre, elle se connecte à n'importe quel smartphone équipé de la technologie bluetooth et de l'application Sea Tags. Si une personne tombe à l'eau, le bracelet émet en continu un signal qui est capté par un ou plusieurs téléphones équipés de l'application. En cas d'immersion ou d'éloignement d'un bracelet, le signal est coupé et en réponse, le ou les téléphones déclenchent une alarme et enregistrent la position GPS au moment de l'incident. Il est possible de paramétrer l'application afin qu'un SMS soit envoyé à un ou plusieurs numéros de téléphone prédéfinis (amis...). Ainsi, une personne seule tombe à l'eau, le téléphone resté à bord enverra un message avec la position du bateau au moment de la chute. La personne à terre qui reçoit le SMS pourra contacter les secours et fournir la position GPS de la personne tombée en mer. L'application permet aussi de déclencher une alerte manuellement et de contacter le Centre Régional Opérationnel de Surveillance et de Sauvetage (CROSS).
L'entreprise Marine Assistance International est spécialisée dans l'assistance maritime, la vente et le développement de produits et de services en lien avec la sécurité des plaisanciers. Depuis plusieurs années, elle propose et développe des solutions de sécurité et d'aide à la navigation, constatant que de plus en plus de plaisanciers sont équipés de smartphones dont les fonctionnalités complètent les instruments de bord classiques.

http://atoutnautic.fr/info_detail.php?article=1109
http://sea-tags.com/content/7-comment-ca-marche-

### *132-16-ST-03* « TRAD 112 » : APPLICATION PERMETTANT UNE MEILLEURE COMMUNICATION ENTRE SECOURISTES ET PERSONNES ÉTRANGÈRES BLESSÉES OU MALADES (SEPTEMBRE)

Dans un aéroport, la communication peut rapidement devenir compliquée lorsqu'un voyageur malade ou blessé ne maîtrise ni le français, ni l'anglais. Afin que les secouristes se fassent mieux comprendre des touristes étrangers nécessitant des soins, un sapeur-pompier de l'aéroport Charles-de-Gaulle a donc imaginé et créé « TRAD 112 », une application d'aide au bilan de santé pour smartphones et tablettes qui permet de récolter des informations importantes auprès de la personne prise de malaise ou blessée. Sous forme de questions médicales simples traduites en différentes langues, le professionnel de santé n'a qu'à choisir sa question qui est immédiatement traduite dans la langue souhaitée auprès du patient, de façon écrite mais aussi vocale. Le patient répond simplement par oui ou par non ou choisit via le smartphone la réponse la plus appropriée. La personne peut lire elle-même ou une voix de synthèse s'en charge, parmi 17 langues plus la langue des signes. Il suffit ensuite de répondre en appuyant sur « oui » ou sur « non ». TRAD 112, disponible sous les systèmes d'exploitation Androïd et IOS, pour 5,99 euros, fonctionne également hors connexion. Les professionnels de santé peuvent donc poser les questions nécessaires aux patients en souffrance même en avion, en mer, sous terre ou à la montagne. L'application est déjà téléchargée dans 46 pays. Des versions personnalisées peuvent être créées à la demande.

http://francais-express.com/actualite/france/-13204-lappli-qui-permet-aux-secouristes-de-mieux-communiquer-avec-les-voyageurs-malades/

### *132-16-ST-04* LA CAMÉRA COUNTERBOMBER, SOLUTION DE SÛRETÉ VIDÉO À TECHNOLOGIE RADAR (FÉVRIER)

En matière de détection pour la lutte contre le terrorisme et les attentats, la société Hi Tech Detection Systems (HTDS) propose la caméra CounterBomber, dotée d'un système permettant de repérer automatiquement les menaces dissimulées sur les piétons à distance, en toute sécurité, en utilisant la technologie radar dirigée par la vidéo. Véritable scanner corporel et comportemental, elle est conçue pour protéger les zones critiques contre des kamikazes potentiels. Idéale pour la sécurisation des bâtiments gouvernementaux, bases militaires, stades, aéroports, gares, hôpitaux, écoles ou postes de contrôle, la caméra, entièrement mobile, permet une inspection automatique des sujets en marche dès leur entrée dans une zone critique. Grâce à son système de suivi vidéo, les responsables de la sécurité civile et militaire peuvent prendre rapidement des décisions précises sur les personnes suspectes. La CounterBomber peut être utilisée manuellement pour le dépistage dans les lieux publics, moins structurés en matière de sécurité, ou de façon autonome (mains libres) pour le dépistage dans les zones hautement contrôlées. Sans danger pour l'opérateur et les personnes inspectées, la caméra bénéficie d'une capacité élevée de détection et d'un très faible taux de fausses alarmes.

http://www.controles-essais-mesures.fr/actualite-2692-terrorisme-une-solution-de-surete-video-a-technologie-radar-scanner-corporel-et-comportemental
http://www.htds.fr/fr/surete/inspection-personnes/camera-counterbomber/

### *132-16-ST-05* REVOLAR : BOUTON D'ALERTE CONNECTÉ (FÉVRIER)

Revolar est un nouvel objet connecté qui avertit les proches en cas de danger ou de menace. Plus petit qu'une pièce de 2€, il se fixe à un vêtement ou à un porte-clés. Ce boîtier discret est connecté à un smartphone via Bluetooth et fonctionne avec une application dédiée permettant l'envoi d'un message d'alerte à une liste de contacts en cas d'urgence. Ainsi, l'appui sur ce bouton permet d'appeler de l'aide et de prévenir les proches qui recevront sur leur terminal la position GPS de l'utilisateur. En cas de fausse alerte, l'utilisateur peut la supprimer en saisissant un code de sécurité et un message de rectification sera envoyé aux proches. À l'état de prototype, ce gadget connecté peut s'avérer pratique notamment pour les personnes âgées et les enfants. Le produit fini est attendu sur le marché en 2016.

http://www.iphon.fr/post/revolar-bouton-wearable-alerte-urgence-prevention-securite-connectee-840903

### *132-16-ST-06* SMARTPHONE : DÉTECTEUR DE SÉISMES (MARS)

En partenariat avec l'opérateur allemand Deutsche Telekom, le directeur du laboratoire de sismologie de l'université de Berkeley en Californie (États-Unis) a créé avec son équipe une application mobile destinée à détecter les séismes. Cette application pour smartphones permet de détecter automatiquement des tremblements de terre. Si un smartphone et plusieurs autres se trouvent à proximité et enregistrent un même déplacement au même instant, et dans une direction identique, le centre d'analyse conclut qu'il s'agit bien d'un tremblement de terre et donne l'alerte à tous les mobiles de la région. Plus le nombre de participants sera élevé, plus la précision sera importante. Ce programme « MyShake » fonctionne uniquement avec des appareils équipés du système d'exploitation Android. Afin de ne pas dégrader les performances ou l'autonomie des batteries sur les smartphones, ce dispositif a été créé de manière à utiliser le minimum d'énergie lorsque le programme est activé. Il s'emploie en position horizontale. Grâce au capteur de mouvements et à son système de positionnement par satellite GPS, l'appareil envoie en permanence un ensemble de données aux centres d'analyses antisismiques. L'application MyShake est capable de distinguer un mouvement normal d'une secousse sismique. Elle peut détecter un séisme d'une magnitude supérieure à 5 dans un rayon de 10 kilomètres.

http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/smartphone-smartphone-devenu-sismographe-pourrait-sauver-vies-61654/

### *132-16-ST-07* SEAGULL : LE BATEAU DE DÉMINAGE AUTONOME (MARS)

La société israélienne ELBIT a mis au point un bateau de déminage autonome, le SEAGULL (le « goéland » en anglais).
À l'heure actuelle, quand des éléments tendent à suspecter la présence de mines dans une zone, des démineurs doivent s'en approcher pour pouvoir les désarmer. A cet égard, le SEAGULL pourrait préserver des vies. En effet, ce bateau est conçu avec un système de navigation autonome lui permettant d'éviter les obstacles et de se conformer aux règles de navigation internationale.
Une fois sur zone, le SEAGULL est doté des équipements nécessaires pour la recherche, la détection, la classification, l'identification, la neutralisation ainsi que la vérification de mines marines, qu'elles soient émergées ou immergées. Toutes ces opérations sont téléguidées à distance depuis un autre vaisseau voire même depuis le rivage.
Pour le moment, ELBIT n'a pas donné le nom d'éventuels clients mais à n'en pas douter, certaines forces navales pourraient rapidement être intéressées.

http://www.clubic.com/mag/transports/actualite-796182-elbit-seagull-bateau-deminage-autonome-teleguide.html
http://www.tomsguide.fr/actualite/seagull-eolienne-geante,50239.html

### *132-16-ST-08* AUTOMIST SMARTSCAN : EXTINCTEUR INTELLIGENT CAPABLE DE VISER LE FEU (FÉVRIER)

Après avoir évoqué l'extincteur aux infrasons dans un article de notre revue du mois de septembre 2015 (Revue CREOGN n°119-15-ST-05), ce mois-ci sera consacré aux extincteurs automatiques à eau (ou *sprinklers*). Les extincteurs automatiques arrosent généralement toute la pièce lors d'incendie et peuvent détruire du matériel de valeur. Pour lutter contre ce problème, une société anglaise *Plumis* a développé l'Automist Smartscan, un extincteur capable de viser directement le feu. Ce système intelligent d'extincteur automatique permet de cibler la source de chaleur et agit directement sur le feu. Lorsque le détecteur infrarouge situé au plafond d'une pièce capte de la chaleur, il active le *sprinkler* situé sur l'un des murs. Celui-ci arrose ensuite la zone avec sa tête pivotante tant que la source de chaleur est détectée comme étant dangereuse. L'avantage de ce système est qu'il n'a pas besoin de tuyauterie ou de réservoir indépendant puisqu'il utilise l'arrivée d'eau déjà présente dans les foyers. De plus, comme il est directionnel, il n'arrose pas toute la pièce, ce qui permet de protéger le reste des objets qu'elle contient.

http://www.futura-sciences.com/videos/d/automist-smartscan-extincteur-automatique-intelligent-vise-feu-3336/

### *132-16-ST-09* DISPOSITIF DE LUTTE CONTRE LES INCENDIES AUTONOME : CRÉATION DE ROBOTS-POMPIERS VOLANTS (JANVIER)

Dans notre article n°114-15-ST-07 paru dans la revue du CREOGN du mois de février 2015, nous évoquions « Saffir » le robot marin pompier capable de se déplacer, d'ouvrir les portes, de voir à travers la fumée et de tenir une lance haute pression pour éteindre un incendie à bord d'un navire. Saffir est désormais assisté d'un drone capable de se déplacer dans un bâtiment pour cartographier les lieux et cibler les sources de l'incendie.
Toujours dans cette optique de lutter contre les incendies, une entreprise américaine spécialisée dans les équipements militaires et de sécurité, Lockheed Martin, a développé un dispositif similaire dans les airs. Ce concept nécessite un drone, le Stalker XE, et un hélicoptère bombardier d'eau sans pilote, le K-Max. Le drone guide l'hélicoptère grâce à une tourelle à capteur de rayons infrarouges permettant au K-Max de cibler l'incendie avec une grande précision. La démonstration a été effectuée par le drone qui a localisé le foyer d'incendie et transmis les données à l'hélicoptère qui a ensuite effectué des largages d'eau pour éteindre l'incendie.
Mécanisme déjà présenté l'an passé, la nouveauté réelle réside dans le fait que cette mission est transmise en temps réel au contrôle du trafic aérien, Air Traffic Control et sous la surveillance du service d'aviation des États-Unis, le National Airspace System (NAS - système de gestion du trafic aérien des Etats-Unis), condition indispensable pour que ce dispositif soit habilité à évoluer dans l'espace aérien. Le vol de démonstration a donc permis de confirmer la capacité de Lockheed Martin à intégrer ce type d'opération dans le NAS par le biais de son propre système de gestion de trafic de drones (UTM, *UAS Traffic Management*). Le système UTM a assuré le suivi des deux engins ainsi que la communication avec les contrôleurs aériens en temps réel. Cette innovation offre la possibilité de voler de jour comme de nuit ainsi que par tous temps permettant le triplement de la durée du support aérien pour les équipes au sol.

L'entreprise défend son projet en évoquant une complémentarité avec les pilotes de tracker, qui eux, luttent contre les incendies uniquement le jour.

http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/robotique-bientot-robots-pompiers-volants-60738/

### *132-16-ST-10* AUTO-GÉNÉRATION D'UN ROBOT (FÉVRIER)

Le site atelier.net met en ligne, le 10 février 2016, un article présentant un projet de l'université d'Oslo visant à doter un robot de capacités d'auto-génération. Il s'agit en fait de l'association en un seul engin d'un robot, d'un logiciel d'apprentissage et d'une imprimante 3D. L'objectif poursuivi par l'équipe universitaire est de produire un engin destiné à l'exploration lointaine ou à l'intervention dans un contexte de catastrophe naturelle. La structure de base de l'engin doit analyser son environnement, déterminer la forme globale du corps ainsi que le nombre des membres (et de leurs articulations) nécessaires pour intervenir de façon optimale puis créer les morceaux nécessaires grâce à l'imprimante 3D. Si le projet est encore loin d'avoir abouti, les scientifiques estiment que le robot, au fur et à mesure des défis qu'il devra relever, améliorera constamment la qualité des solutions trouvées et de leur réalisation. Ce projet est une illustration des capacités futures offertes aux appareils autonomes par l'intelligence artificielle d'une part et la technologie de l'impression 3D d'autre part.

http://www.atelier.net/trends/articles/netexplo-un-robot-auto-corrige-grace-imprimante-3d-integree_440058?utm_content=bufferb7b41&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

### *132-16-ST-11* LE ROBOT ATLAS, LA RÉVOLUTION D'ALPHABET (MARS)

L'entreprise Boston Dynamics n'a de cesse de multiplier les innovations. Fin février 2016, la filiale d'Alphabet, entreprise mère de Google, a présenté son dernier né en matière de robotique.
Par le biais d'une vidéo mise en ligne, l'entreprise a dévoilé la nouvelle version de son humanoïde Atlas. Ce dernier a été pensé afin de pouvoir évoluer à l'extérieur et au sein de bâtiments. Dans la vidéo publiée, on voit clairement le robot d'1,75m et de 82kg être à même de marcher dans la neige, d'ouvrir des portes, de soulever des charges et d'éviter les chutes même en cas de déséquilibre.
En cas de chute, le robot ne subit que peu de dommages et est capable de se relever.
De fait, ce nouveau type d'humanoïde fait preuve de bonnes capacités d'adaptation. L'ensemble de ces tâches, simples pour un humain, sont globalement peu aisées à réaliser pour un robot et font l'objet d'un travail depuis plusieurs années. Les observateurs notent une nette avancée en matière de robustesse. Néanmoins, le bruit encore trop important du robot et sa forte consommation en énergie le rendent encore peu attractif.
En dehors des informations décelables à travers la vidéo, l'entreprise n'a que faiblement

communiqué sur le sujet. On sait malgré tout qu'Atlas fonctionne grâce à des moteurs hydrauliques et qu'il suscite une certaine empathie de la part de bien des personnes ayant visionné la démarche du robot.
En effet, les réactions relevées sur les réseaux sociaux témoignent de la pitié exprimée face à un robot malmené par son créateur. Celles-ci amènent à s'interroger sur l'individu lui-même, aujourd'hui placé à côté de l'humanoïde.

http://www.lemonde.fr/pixels/article/2016/02/24/un-nouveau-robot-humanoide-tres-performant-devoile-par-une-entreprise-d-alphabet_4870864_4408996.html

### *132-16-ST-12* ROBOTIQUE : LE SERVEUR N'EST PAS HUMAIN (MAI)

Dans un article mis en ligne le 12 mai 2016, une journaliste du site *the daily beast* rapporte le mouvement actuel de diffusion des robots de service dans les restaurants. Lancé dans des pays asiatiques (Chine, Japon, Corée du Sud, Hong Kong et Thaïlande), le concept s'exporte progressivement. Dès 2013, un restaurant londonien avait provoqué la curiosité en proposant un service par des drones aériens. Désormais présentes en Californie, des chaînes ouvrent des restaurants où les plats sont amenés par des robots, voire préparés par leurs soins. Une société américaine a mis au point un engin capable de retourner un steak et de découper la garniture nécessaire pour un hamburger en quelques secondes. Les débits de boisson ne sont pas en reste : le barman électronique existe déjà, confectionnant les cocktails à la demande mais sans discuter avec le client… Le secteur hôtelier est également de la partie, le premier hôtel proposant réceptionniste, chasseur et porteur de bagage robotisés étant désormais ouvert au Japon. Un chercheur britannique prévoit que, d'ici 2018, 35 millions de robots de service auront été mis en circulation dans le monde. En conclusion, la journaliste se demande quelle est la finalité de ces innovations qui font disparaître de l'emploi sans que l'on puisse discerner, a priori, de véritables progrès pour la population humaine.

http://www.thedailybeast.com/articles/2016/05/12/bartending-robots-are-coming-for-your-cocktail.html

### *132-16-ST-13* AN'BOT, CRS DU FUTUR (MAI)

Loin de l'image de RoboCop, ce robot ressemble plus à un œuf géant équipé de patins à roulettes et à première vue, il ne fait pas très peur. Mais ce « robot CRS », dévoilé mi-avril 2016 à la foire de la high-tech de Chongping et conçu par l'armée chinoise, dispose de compétences impressionnantes en matière de renseignement et de maintien de l'ordre. Répondant au petit nom d'An'Bot, il est le premier prototype de robot policier intelligent qui aura pour mission de « lutter contre le terrorisme » et pourra servir à réprimer des émeutes. Machine de 1m50 pour 80 kg, selon l'armée chinoise, il peut se déplacer à 18 km/h (même si sa vitesse de patrouille tourne plutôt autour de 1 km/h…), avec une autonomie de 8 heures. Il est équipé d'un pistolet à impulsion électrique (comparable à un taser). Il possède des capteurs imitant le cerveau, les yeux et les oreilles d'un humain. Avant toute

intervention, il pourra même vous notifier votre garde à vue. Il dispose également d'un bouton « SOS » qui permettra à toute personne en détresse d'appeler la police. À l'heure actuelle, il n'existe aucune démonstration vidéo d'An'Bot en action.

http://www.metronews.fr/high-tech/l-armee-chinoise-devoile-le-tout-premier-robot-crs-intelligent/mpdC!Uc5ghNluVPwmU/

### *132-16-ST-14* ABANDON DU PROJET DE « MULE ROBOTIQUE » PAR L'ARMÉE AMÉRICAINE (JANVIER)

Conçue pour transporter des charges sur le terrain, la mule robotique LS3 (*Legged Squad Support System*) vient de subir un revers dans son développement.
En effet, fin décembre 2015, l'armée américaine s'est prononcée en faveur de son abandon. L'innovation, capable d'être pilotée à la voix et d'avancer sur des terrains accidentés afin d'accompagner les soldats au cours d'un assaut, était porteuse d'espoirs. Pour autant, des difficultés inhérentes à son exploitation ont freiné sa course. En cause, un manque de durabilité et un bruit excessif auxquels les concepteurs ne sont pas parvenus à répondre. Le prototype de LS3, testé sur le terrain, a rapidement montré ses failles.
Malgré les efforts d'adaptation des développeurs, le niveau de bruit lors des déplacements est tel qu'il rend incompatible l'utilisation de la « mule » avec le bon déroulement d'une mission. De même, la complexité de sa construction permet difficilement d'imaginer une réparation sur le terrain.
L'armée en a conclu que l'outil ne pouvait être utilisé en conditions réelles. Cependant, les technologies nées de ce projet serviront au développement d'innovations futures, plus performantes et réalistes.

http://fr.sputniknews.com/defense/20151229/1020654186/US-refuse-mule-robotique.html
http://www.opex360.com/2016/01/03/lus-marine-corps-met-en-veilleuse-le-projet-de-robot-mule/

### *132-16-ST-15* DOGO : UN NOUVEAU ROBOT DE COMBAT TÉLÉCOMMANDÉ ET ARMÉ (MAI)

L'évolution des robots de combat commandés à distance est loin d'être terminée. Il faut remonter à la Seconde Guerre mondiale pour trouver le premier robot militaire du genre. Monté sur chenille et contenant des explosifs, le « Goliath » était actionné à distance pour détruire un char. Avec le temps ont été développés des robots démineurs ainsi que des robots de combat plus performants. Le robot SWORDS (*Special Weapons Observation Reconnaissance Detection Systems* ) en est un exemple. Utilisé par l'armée américaine depuis 2004, il est équipé notamment d'une mitrailleuse, d'un lance-grenade et d'une caméra.
Qu'y a-t-il donc de révolutionnaire dans le robot de combat surnommé « Dogo » (en référence au dogue argentin) et développé par l'entreprise israélienne General Robotics Ltd ? D'une part, il convient de souligner sa légèreté avec un poids de 12 kg (le SWORDS

fait plus de 45kg). Il monte ainsi aisément des escaliers, avance sans contrainte sur un terrain escarpé voire sous terre. Dogo est également doté de huit caméras assurant une vision à 360°, d'un pistolet Glock 9 mm et d'un désignateur laser. Il ne s'agit en aucun cas d'un robot autonome tueur puisqu'il doit avoir reçu l'ordre de l'opérateur qui le manœuvre grâce à une console. Toutefois, pour de simples opérations de police, il peut également être équipé d'armes non létales telles que du spray au poivre.
Dogo peut s'avérer utile dans de nombreuses situations. De la simple reconnaissance à la négociation avec des preneurs d'otage (grâce à son émetteur/récepteur), en passant par la guerre souterraine, ce robot se veut plus fiable que ne l'est le SWORDS présentant de fréquentes pertes de contrôle.
La société General Robotics Ltd a annoncé qu'elle dévoilera officiellement sa technologie lors de l'Exposition Eurosatory à Paris (salon international de défense et de sécurité) du mois de juin 2016.

http://www.opex360.com/2016/05/09/lentreprise-israelienne-general-robotics-ltd-propose-robot-arme-pour-les-operations-speciales/
http://www.defensenews.com/story/defense/international/mideast

### *132-16-ST-16* LE PENTAGONE MISE OFFICIELLEMENT SUR LES « TEXTILES INTELLIGENTS » (AVRIL)

Le 1er avril 2016, le Pentagone a lancé un programme de recherche sur les textiles dits « intelligents ». Évalué à près de 317 millions de dollars, le programme associe plusieurs universités, conduites par le Massachusetts Institute of Technology (MIT), à des entreprises industrielles (Bose, Intel, New Balance…). La recherche a pour but d'identifier des fibres conductrices à même de recevoir des composants électroniques stockant ou diffusant des informations. Il s'agit là de l'étape première du programme à vocation militaire.
Une fois le textile élaboré, il sera en mesure de contenir des circuits intégrés, des lumières LED ou bien encore des cellules solaires. Les applications seront alors d'une grande diversité. Le ministère américain de la Défense prévoit par exemple que des micro-capteurs soient intégrés dans le nylon des parachutes afin d'anticiper tout risque de rupture. De même, l'idée d'une tente ou d'un « treillis intelligent » a été avancée. Ce dernier prendrait en compte les données biologiques du soldat et s'adapterait à son environnement (changement de couleur, détection de menace chimique…).
Ce programme industriel, associant sphères publique et privée, est le 8ème conduit sous l'ère de l'actuel Président américain et le 6ème confié au Pentagone. La Maison Blanche ambitionne ainsi d'établir un réseau national pour l'innovation au sein de tout le pays. A cette fin, l'administration fédérale a, à ce jour, investi aux alentours de 600 millions de dollars, auxquels viennent s'ajouter une part moindre issue du secteur privé.

http://www.opex360.com/2016/04/02/le-pentagone-lance-programme-de-recherche-sur-les-textiles-intelligents/
http://www.zonebourse.com/INTEL-CORPORATION-4829/actualite/Le-Pentagone-investit-dans-les-textiles-intelligents-22108338/

## *132-16-ST-17* LES FORCES SPÉCIALES AMÉRICAINES BIENTÔT ÉQUIPÉES DE TENUES DE COMBAT INTELLIGENTES (JUIN)

Un premier prototype de tenue de combat tactique surnommé TALOS (Tactical Assault Light Operator Suit) devrait être livré en août 2018 aux forces spéciales américaines. Cette tenue comprendra une protection balistique, une localisation spatiale GPS ainsi que des indications sur l'état de santé du combattant, c'est-à-dire une batterie de capteurs qui mesurent la fréquence cardiaque, la température, la position du corps et le niveau d'hydratation (dont le type et la gravité d'éventuelles blessures). Une étude complémentaire vise à intégrer un exosquelette, des composants capables de stocker et de restituer de l'énergie, ainsi que des capteurs biométriques et de C4I (Command Control, Communications, Computer and Intelligence).

*NDR : L'Internet des objets (IoT en anglais : Internet of the Things) est en passe de faire son entrée chez les combattants américains. Afin d'éviter le hacking, reste à savoir si la sécurité des systèmes d'information a été intégrée dès la conception.*

http://www.janes.com/article/60916/ussocom-continues-to-advance-talos-development
http://www.techtimes.com/articles/92478/20151007/u-s-military-to-deliver-its-first-bulletproof-weaponized-iron-man-suit-in-2018.htm

## *132-16-ST-18* UNE NOUVELLE COUVERTURE D'INVISIBILITÉ POUR LES MILITAIRES (AVRIL)

Initialement développée par POLARIS SOLUTIONS en Israël et aujourd'hui fabriquée et commercialisée par READYONE INDUSTRIES, une couverture d'invisibilité a été testée par l'armée britannique.
Cette nouvelle couverture de camouflage, nommée VATEC, a pour particularité de dissimuler le personnel militaire ainsi que le matériel des appareils thermiques et optiques. Grâce à sa structure et à son interaction avec la lumière et la chaleur, le tissu permet, en effet, de les déguiser en tas de cailloux. VATEC pourrait bien à terme remplacer les éléments de camouflage traditionnels des snipers.
Il est vrai que cette « cape d'invisibilité » n'est pas la première du genre. Toutefois, ces dernières années, l'invisibilité des objets demeurait limitée puisqu'il fallait soit se situer dans un angle de vision précis soit être à une température fixée.
Cette technologie de camouflage ne sera sans doute pas la dernière. Des scientifiques misent désormais sur le camouflage dynamique en tentant de reproduire la façon dont les pieuvres ou les poulpes changent de couleurs pour se fondre dans leur environnement.

http://www.defensereview.com/vatec-concealment-solutions-vcs-multispectral-3d-combat-camouflage-system-texturized-individual-and-vehicle-camouflage-by-polaris-solutions-israel-and-readyone-industries-conceals-your-visible-li/
http://www.telegraph.co.uk/news/uknews/defence/12199541/British-troops-test-invisibility-cloak-to-hide-on-battlefield.html

-africa/2016/05/08/introducing-israeli-12-kilo-killer-robot/83970684/
http://www.glrobotics.com/#!dogo-members/cp4r

### *132-16-ST-19* LANCEMENT D'UN AÉRONEF HYBRIDE « DRONE-AVION-HÉLICOPTÈRE » (JUIN)

Dans le cadre du projet baptisé VTOL X-Plane (Vertical Takeoff and Landing Experimental Plane), l'agence américaine de défense développe le « lightningStrike », un drone alliant la souplesse d'utilisation et la manœuvrabilité d'un hélicoptère avec la vitesse et le large rayon d'action d'un avion. La DARPA, l'agence américaine chargée des projets de recherche avancés en matière de défense, a confié la réalisation de ce prototype à un consortium de trois sociétés, Aurora pour la partie électronique et « dronisation », Rolls-Royce pour la motorisation et Honeywell International pour les batteries. Leur mission consiste à faire voler le « LightningStrike », un drone à motorisation hybride, d'ici 2018.
L'engin sans pilote décolle et atterrit grâce à ses ailes qui pivotent pour orienter la poussée des 24 moteurs. Le cahier des charges exige que l'appareil soit capable d'atteindre une vitesse de 300 à 400 nœuds (550 à 740 km/h) et de transporter des charges pesant 40% de son poids, soit environ 2 tonnes de cargaison.
Par ailleurs, le point perfectible se situe au niveau de la consommation de carburant lors des phases d'atterrissage et de décollage. En effet, la consommation excessive de carburant réduit considérablement l'autonomie durant les missions.
Et enfin, bien que les recherches ciblent davantage le domaine militaire, ce drone hybride pourrait également intéresser d'autres secteurs professionnels tels que la surveillance, le secours en mer, le ravitaillement, le transport, l'agriculture, etc.

http://www.smartdrones.fr/la-darpa-veut-lancer-un-aeronef-hybride-drone-avion-helicoptere/005086

### *132-16-ST-20* MICRO DRONE MILITAIRE (OCTOBRE)

Le site smartdrones.fr se fait l'écho de la mise au point par la société Prox Dynamics d'un micro drone destiné à une utilisation militaire. Cet appareil, non armé, est conçu pour mener des opérations de reconnaissance à l'échelon du groupe de combat, y compris sous la pluie et de nuit. Donné pour 25 minutes d'autonomie et une portée de 1600 mètres, le micro drone pèse moins de 20 grammes et emporte trois caméras dont une thermique. Emporté prêt au vol dans un boîtier spécifique, l'engin se pilote à une main avec une manette identique à celles des consoles de jeu vidéo. Sa petite taille et sa vitesse relativement réduite doivent l'aider à passer inaperçu dans une ambiance de combat. L'armée des États-Unis le teste sur le terrain et pourrait s'en doter à l'avenir.
Ce type de drone tactique doit donner aux groupes de combat une capacité de reconnaissance à très courte portée.

http://www.smartdrones.fr/black-hornet-les-mini-drones-qui-interessent-larmee/0013987

### *132-16-ST-21* DISTRIBUTION DE MÉDICAMENTS, VACCINS ET LIVRAISON DE SANG PAR DRONES (MAI)

La Fondation UPS a annoncé un partenariat avec Zipline et l'Alliance mondiale pour les vaccins et la vaccination afin d'expérimenter l'utilisation de drones pour distribuer des produits tels que des médicaments, du sang et des vaccins. L'entreprise postale américaine UPS a déclaré que la livraison rapide par drone permettrait de sauver des milliers de vies et 800 000 dollars ont été versés pour soutenir ce projet. Le drone appelé « Zip » a l'aspect d'un petit avion avec une envergure de près de 2,4 mètres et pèse moins de 10 kg. Equipé de deux moteurs électriques, il est capable de transporter une charge utile avoisinant 1,6 kg. Le Zip peut voyager à une vitesse pouvant aller jusqu'à 100 km/h pour un aller-retour de 120 km. Son plan de vol est stocké dans une carte SIM. Une fois sur zone, le drone largue à basse altitude sa cargaison vitale par parachute. Dès son retour, la batterie du drone est changée, ce qui permet l'accomplissement immédiat d'une nouvelle mission. Dans le courant de l'année, le gouvernement du Rwanda commencera à utiliser ces drones pouvant effectuer jusqu'à 150 livraisons de sang par jour à 21 centres de transfusion situés dans la moitié ouest du pays. Le réseau national de drones du Rwanda se concentre avant tout sur la livraison de sang, mais l'objectif est d'étendre l'initiative aux vaccins, aux traitements du VIH/Sida, du paludisme et de la tuberculose, ainsi qu'à de nombreux autres traitements vitaux.

http://www.jeuneafrique.com/324322/societe/rwanda-drones-distribuer-sang-vaccins/

### *132-16-ST-22* DRONES ET AIDE HUMANITAIRE (MAI)

L'utilisation des drones ne cesse de se diversifier.
Depuis ces dernières années, c'est dans l'aide humanitaire et la réponse aux catastrophes qu'ils semblent avoir trouvé pleinement leur utilité. Ils ont été employés dès 2012 par l'Organisation Internationale pour la Migration à Haïti suite au séisme de 2010 afin d'évaluer les dommages, aux Philippines en 2013 après le typhon Haiyan pour piloter les efforts de reconstruction, et en 2014 en Papouasie-Nouvelle Guinée par Médecins sans Frontières pour la livraison de vaccins.
Le séisme d'avril 2015 au Népal est la dernière utilisation en date des drones, réquisitionnés pour des missions de recherche et de secours et pour cartographier les monuments, les sites du patrimoine mondial de l'humanité et les maisons détruits ou dévastés.
Leurs points forts : leur prix, leurs équipements de pointe, leur facilité d'utilisation et la rapidité de prise en main, qui permettent d'éviter l'envoi immédiat de personnels humanitaires dans les zones de catastrophe dans le but d'évaluer les besoins des survivants.
Leurs points faibles : l'éthique d'emploi, la légalité et la sécurité, parfois contestables, comme ce fut le cas au Népal. En effet, ils étaient très nombreux, volant partout y compris près d'installations de sécurité (d'où des craintes sur le détournement des images) et sans

retour d'informations auprès du Gouvernement, dans un pays alors non équipé d'une réglementation sur les drones. L'absence de contrôle et surtout de restrictions dans leur emploi ont été un poids supplémentaire pour le ministère de l'Intérieur népalais. La situation a changé puisque l'Autorité de l'aviation Civile a désormais interdit aux UAV de voler sans sa permission, restreignant le temps de vol à 15 minutes et introduisant des zones interdites au-dessus des maisons, des bâtiments d'agences de sécurité et de sites religieux ou culturels.

http://www.actualites-news-environnement.com/35440-drones-humanitaire.html

### *132-16-ST-23* UN NOUVEAU VENU CHEZ LES DRONES : LE DRONE-PLONGEUR (MARS)

Les drones n'en finissent pas de surprendre. Le 4 février 2016, le concours 2016 *Drones for Good*, « des drones pour faire le bien », s'est déroulé à Dubaï, aux Émirats arabes unis.
Il a sacré un petit robot à la fois capable de voler et d'évoluer sous l'eau. Le quadrirotor Loon Copter a en effet impressionné par ses capacités. Il a démontré être à même de voler, se poser sur l'eau, se déplacer à l'aide d'un aéroglisseur en usant de ses hélices, mais surtout de plonger afin d'effectuer une mission sous-marine. A la suite de cela, il est capable de rejoindre la surface pour reprendre son envol. De telles capacités ont poussé certains à le comparer à « un drone-canard ».
L'engin est parfaitement étanche. Pour autant, il n'est pas encore en mesure de s'immerger trop profondément. Il pourrait être utilisé dans le cadre d'opérations humanitaires ou écologiques, en vue, par exemple, de permettre le prélèvement d'échantillons afin de prévenir les risque de pollutions.
Le drone peut également enregistrer des vidéos mais ne peut encore les transmettre en direct durant la plongée. Il ne permet dont pas un pilotage en immersion.
Le même concours a aussi sacré le projet Navig8 reposant sur un drone conçu exclusivement pour les opérations de recherche en situation d'urgence. Équipé d'une caméra et de plusieurs capteurs, il est capable de repérer des victimes en atmosphère hostile et de transmettre leur localisation précise.

http://drones.blog.lemonde.fr/2016/02/07/un-drone-canard-sacre-champion-de-lhumanitaire/

### *132-16-ST-24* LE DRONE LANDAIS HELPER SPÉCIALISÉ DANS LES INTERVENTIONS EN MER PRIMÉ AU CONCOURS LÉPINE (SEPTEMBRE)

Le 17 septembre 2016, les concepteurs du drone Helper ont remporté « le prix du Premier ministre » lors de la remise des prix du concours Lépine, qui se déroulait à la foire européenne de Strasbourg. Homologué par la Direction générale de l'aviation civile, le drone Helper, expérimenté cet été pour la première fois sur les plages de Biscarosse, avait pour missions la surveillance des baigneurs et l'intervention en mer.
Équipé d'une caméra thermique et d'un système de largage d'une bouée, il procure aux sauveteurs une véritable aide au repérage visuel et technique pour les personnes en

difficulté. Fort d'une autonomie allant jusqu'à 40 minutes et pouvant atteindre 80km/heure, Helper est rapidement projetable sur les lieux, ce qui lui a permis d'effectuer 40 levées de doute et de sauver trois vies.
Helper sera représenté fin avril 2017 à Paris au concours Lépine international. En attendant sa commercialisation à l'été 2017, une nouvelle phase de tests est prévue en Angola, à la demande du groupe TOTAL, mais cette fois-ci, il aura la charge de surveiller les plateformes pétrolières et les éventuelles pollutions.

http://www.industrie-techno.com/helper-un-drone-sauveteur-prime-au-concours-lepine.
http://www.lefigaro.fr/secteur/high-tech/2016/08/19/32001-20160819ARTFIG00024-helper-le-drone-qui-vole-au-secours-des-sauveteurs-en-mer.php

### *132-16-ST-25* AUX ÉTATS-UNIS, LES DRONES DE LOISIRS DEVRONT ÊTRE ENREGISTRÉS AUPRÈS DES SERVICES DE L'ÉTAT (JANVIER)

L'administration fédérale de l'aviation a annoncé (voir article 121-15-ST-01 dans la revue du CREOGN de novembre 2015) comme nouvelle règle d'utilisation des drones de loisirs leur enregistrement préalable dans une base de données. Les propriétaires paieront cinq dollars et communiqueront leurs noms, adresses physique et électronique aux autorités. Le but est de responsabiliser les utilisateurs dans la pratique de leur loisir qui fait l'objet d'incidents signalés de plus en plus nombreux. La vente de près de 700 000 drones aux USA en 2015 semble justifier le besoin de réglementer leur utilisation.

*NDR : Au sein de l'Union européenne, la mise en place de normes est moins simple du fait des règles nationales. On peut cependant noter que la commission européenne tente d'imposer l'enregistrement des utilisateurs et de leur machine et a posé la réflexion d'une réorganisation des règles de l'espace aérien afin de considérer l'utilisation des drones.*

http://www.usnews.com/news/articles/2015-12-14/toy-drones-must-be-registered-with-the-government

### *132-16-ST-26* PREMIER DRONE CONNECTÉ DE TRANSPORT AUTONOME (JANVIER)

Une société chinoise EHANG a présenté lors du salon d'électronique CES 2016 de Las Vegas le premier drone connecté de transport autonome fonctionnant à l'électricité, le EHang 184. Ce drone vole à basse altitude et sur de courtes distances.
Cette première mondiale repose sur les mêmes technologies développées pour les engins de petites tailles. Ce drone de transport autonome dispose de huit hélices réparties sur quatre bras et d'une forme proche de ses homologues miniatures. Il peut atteindre une altitude de 500 mètres et filer à une vitesse moyenne de 100 km/heure. Avec son poids de 200 kg, il accueille un passager de maximum 100 kg. Ses bras rétractables lui permettent de se garer sur l'équivalent d'une place de voiture. Le passager ne pilote pas le drone de transport. La société chinoise a créé un système de guidage grâce auquel il suffit au

passager de rentrer sa destination sur la tablette placée devant le siège.
En phase d'essai actuellement, son autonomie reste très limitée (maximum 23 minutes de voyage). Autre contrainte imposante, les batteries se rechargent entre 2 à 4 heures. Plusieurs questions ont été posées lors de ce show : qui pourra stopper la progression de ce drone en cas d'obstacle sur son trajet ? Pourra-t-on atterrir partout ? Quels modèles économiques peut-on mettre en place ? Quelle sécurité pour le passager en cas de chute ? La marque envisage de commercialiser le EHang 184 en 2016 (entre 185 000 et 275 000 euros).

http://www.objetconnecte.net/ces-2016-drone-de-transport-autonome-taxi-futur/

### *132-16-ST-27* COMMERCIALISATION DU PREMIER DRONE SOLAIRE (NOVEMBRE)

Après quatre années de recherche, la start-up toulousaine SUNBIRDS, appuyée par le ministère de l'Économie, des Finances et de l'Industrie et portée par de nombreux financements, a lancé, en novembre 2016, le premier drone solaire baptisé SB4-Phoenix, à même de voler sans discontinuer pendant huit heures. Cette capacité de vol supérieure à celle des autres drones civils s'explique par sa légèreté (3 kg) et sa faculté à s'auto-alimenter grâce à des ailes d'envergure (3 mètres) recouvertes de cellules solaires. Appareil dédié à la surveillance des zones sensibles, à l'agriculture de précision ou encore à l'observation des espèces animales et végétales, sa commercialisation est prévue en 2020 pour un prix avoisinant les 30 000 euros.

http://www.infoprotection.fr/SURETE-ET-SECURITE/Article.htm?Zoom=fd8918bcb167eaa2870e37f9ba9f3511

### *132-16-ST-28* LA POLICE NÉERLANDAISE ENTRAÎNE DES RAPACES À ABATTRE DES DRONES (FÉVRIER)

Les rapaces voient d'un mauvais œil les drones car ils volent mal et représentent une menace.
Face à l'augmentation du nombre de drones dans l'espace aérien, les forces de sécurité des Pays-Bas manifestent une certaine inquiétude. Aussi, la police néerlandaise a fait appel aux aigles à tête blanche pour faire face aux drones qui représentent une menace dans l'espace aérien. C'est une société danoise (*Guard from above*) qui entraîne les rapaces à cibler et abattre les drones. Le directeur de cette société souligne que le rapace est une solution naturelle pour résoudre un problème technologique.
Les rapaces considèrent les drones comme une menace dans leurs espaces d'évolution. Les autres oiseaux voient le drone comme un prédateur. Les rapaces entraînés sont suffisamment agiles pour attaquer le drone de façon à ne pas se blesser. D'après un fauconnier de la société, il est fort probable que l'oiseau visualise les rotors du drone et les identifie comme la partie dangereuse de l'appareil.
Cette solution pour maîtriser l'espace aérien intéresse également la police londonienne ainsi

que Scotland-Yard.

*NDR : L'idée de solliciter un rapace pour maîtriser les drones est remarquable. L'aigle est en mesure de détecter et de se déplacer plus rapidement qu'un drone de défense. On peut imaginer ce type de solution à l'occasion de manifestations à caractère officiel.*

http://www.irishtimes.com/news/world/europe/eagle-eyed-dutch-police-train-birds-to-take-down-drones-1.2519550
http://www.theguardian.com/uk-news/2016/feb/08/scotland-yard-interested-in-using-eagles-to-take-down-drones
http://www.huffingtonpost.fr/2016/02/01/video-aigles-drones-arme-arsenal-anti-drones-police-hollandaise-insolite-techno_n_9131848.html

### *132-16-ST-29* DRONES ET RECHERCHE ENVIRONNEMENTALE (JANVIER)

De par leur facilité d'utilisation et l'aide précieuse apportée sur le terrain, de plus en plus d'organismes scientifiques et d'entreprises exploitent les drones dans la recherche.
Le ministère de l'Écologie suit cette tendance et veut favoriser leur utilisation pour la transition énergétique en accompagnant la collaboration entre les concepteurs et les possibles utilisateurs que sont les instituts de recherches, d'autant plus que le développement de nouveaux outils embarqués, comme les capteurs laser ou les capteurs de réflectance, permet de faire des mesures extrêmement précises et ouvre des champs nouveaux pour la recherche.
Quant à leur rentabilité sur le long terme, elle permet de relativiser le coût parfois important de ces drones, les plus perfectionnés pouvant atteindre 200 000 euros.

http://www.actu-environnement.com/ae/news/drones-innovation-recherche-environnemetale-agriculture-eau-meteo-faune-26003.php4

### *132-16-ST- 30* DROITS ET DEVOIRS POUR LES ROBOTS ? (SEPTEMBRE)

Si Isaac Asimov est à l'origine des trois Lois fondamentales de la robotique (lois protégeant les êtres humains et a priori inviolables et parfaites), la commission des affaires juridiques de l'institution européenne a, quant à elle, via son rapport en date du 31 mai 2016 (Rapport Delvaux contenant des recommandations à la Commission concernant des règles de droit sur la robotique) mené une réflexion autour du statut des robots et propose de leur attribuer le qualificatif de personnes électroniques dotées de droits et devoirs.
Le texte s'intéresse plus précisément aux machines capables de prendre des décisions autonomes et d'interagir de manière indépendante avec les tiers, à l'image d'une voiture sans conducteur, de robots industriels ou de compagnons humanoïdes domestiques conçus pour apprendre au contact de leur utilisateur.
Aussi la commission s'est-elle questionnée sur la possibilité de faire peser une responsabilité juridique sur ces robots dotés d'une certaine intelligence et non plus entièrement sur leur constructeur. De manière totalement innovante, le rapport préconise,

d'une part, d'imputer le cas échéant partiellement ou entièrement la faute et le résultat dommageable à ces machines et d'autre part, de créer un fonds de dédommagements des victimes alimenté par les fabricants et les utilisateurs.
En outre, la progression de cette technologie risque d'impacter le monde du travail en remplaçant progressivement les individus affectés à certaines tâches et ainsi de fragiliser le système de protection sociale et de retraite. Pour pallier cette éventualité, il est proposé la mise en place de cotisations sociales liées à la personne électronique.
Si le rapport met en exergue de grands principes afin de prévenir certaines difficultés à venir en raison de la place grandissante des robots dans les sociétés, il reconnaît également que de nouvelles règles ne doivent pas devenir un obstacle à l'innovation.

*NDR: Voir aussi la Note du CREOGN n°12 de juillet 2015 intitulée « Faut-il un droit des robots ? » (2ème lien).*

www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-582.443&format=PDF&language=FR&secondRef=01
http://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Droit-des-robots

***132-16-ST-31*** **AUSCHWITZ : LA RÉALITÉ VIRTUELLE AU SERVICE DE LA JUSTICE (NOVEMBRE)**

Un expert en imagerie numérique de la police judiciaire de Munich (LKA), en Bavière, a reproduit le camp d'Auschwitz des années 1940 en trois dimensions. Pour ce faire, il s'est fondé sur le cadastre polonais et plus de mille images d'époque. Il est également allé sur les lieux pour compléter les éléments manquants. Les baraques détruites en 1945 ont été reproduites grâce aux archives et aux plans laissés par les nazis.
Ainsi, les policiers et les procureurs allemands enquêtant sur les criminels de guerre peuvent, par le biais d'un casque de réalité virtuelle, se plonger dans le camp d'extermination. En effet, il est fréquent que les suspects clament leur innocence en arguant qu'ils ignoraient tout des faits commis à Auschwitz même s'ils y travaillaient.
La reproduction en 3D fournit de nombreux détails. Les arbres sont là où ils étaient pour déterminer s'ils pouvaient bloquer la vue depuis une certaine position. Elle permet également de se mettre dans la peau d'un surveillant qui se situe dans une tour de garde.
Cette technologie fut notamment utile en juin 2016 dans le procès d'un ancien garde SS reconnu coupable de complicité de meurtre dans le décès de 170 000 personnes et condamné à 5 ans de prison.
Actuellement, une dizaine d'autres cas occupe toujours le LKA. Certains sont encore vivants et pourraient donc être traduits en justice.
Une fois les dernières affaires closes, le LKA pourrait prêter sa modélisation 3D au mémorial de l'Holocauste Yad Vashem à Jérusalem ou à celui d'Auschwitz. Il aurait alors une fonction de mémoire.

http://www.20minutes.fr/insolite/1934555-20161002-realite-virtuelle-reconstitue-auschwitz-derniers-proces-nazisme-allemagne

http://www.realite-virtuelle.com/auschwitz-nazis-realite-virtuelle-0210
http://www.lepoint.fr/monde/auschwitz-a-l-heure-du-nazisme-04-10-2016-2073500_24.php

### *132-16-ST-32* L'AUTHENTIFICATION PAR EMPREINTE DIGITALE GRAND PUBLIC (MARS)

Quatre sociétés (Gemalto, Fingerprint Cards, Precise Biometrics et STMicroelectronics) ont dévoilé leur dernière technologie en matière d'authentification biométrique par empreinte digitale. Leurs produits peuvent permettre aux fabricants de déployer facilement cette fonctionnalité dans leurs futurs appareils portables pour, par exemple, le paiement en ligne, la billetterie, les e-mails sécurisés, l'accès à des espaces numériques.
Testée sur une smartwatch, elle intègre le capteur d'empreintes digitales de Fingerprint Cards, le logiciel de lecture d'empreintes digitales de Precise Biometrics, la solution CCP sécurisée et les microcontrôleurs à faible consommation d'énergie de STMicroelectronics. Rapide, sécurisée, simple d'utilisation, elle pourrait non seulement équiper toute une gamme d'objets connectés et d'outils à petits capteurs ou à plateformes limitées mais également servir à la sécurisation des programmes d'identification gouvernementaux.

http://www.electronique-eci.com/news/lauthentification-par-empreinte-digitale-à-la-portée-de-tous

### *132-16-ST-33* DES CAPTEURS D'EMPREINTES DE SMARTPHONES TROMPÉS AVEC UNE SIMPLE IMPRIMANTE (AVRIL)

L'authentification par empreinte digitale se démocratise fortement ces dernières années. Certains smartphones sont d'ailleurs dotés de la technologie biométrique présentée comme un outil sécuritaire.
Pour autant, la sécurité est-elle maximale ? Il n'est pas évident de répondre par l'affirmative puisqu'il a déjà été démontré que des lecteurs d'empreintes pouvaient être trompés par le biais de l'impression 3D. Pour autant, cette dernière reste complexe et coûteuse.
A cette première expérience s'ajoute celle plus récente d'une équipe de chercheurs de l'université du Michigan. Il n'est plus question d'une imprimante 3D mais d'une simple imprimante à jet d'encre. Il suffit de récupérer l'empreinte du propriétaire, de l'imprimer sur papier brillant avec une encre conductrice à base d'argent, utilisée pour créer des circuits imprimés à bas coût. L'opération ne dure que quinze minutes. Avec cette technique, deux téléphones Android haut de gamme ont été leurrés et se sont déverrouillés.
Cette expérience montre bien les vulnérabilités de l'authentification par empreinte digitale. Or, de plus en plus de services envisagent de recourir à la biométrie pour valider une action comme les services de paiement mobile. Pour pallier cette difficulté, des techniques anti-usurpation sont déjà en cours de développement.

http://www.20min.ch/ro/multimedia/stories/story/12933067
http://www.metronews.fr/high-tech/iphone-samsung-huawei-le-capteur-biometrique-de-

votre-smartphone-hacke-en-15-minutes-chrono/mpch!DHo2hxDTohWHw/
http://www.presse-citron.net/les-capteurs-dempreintes-digitales-sont-piratables-avec-une-simple-imprimante/

### *132-26-ST-34* IDENTIFICATION BIOMÉTRIQUE PAR L'OREILLE (AVRIL)

La technologie, mise au point par NEC Corporation, fait appel à un écouteur capable de détecter les particularités de chaque conduit auditif grâce à un signal sonore infime émi par un haut-parleur, répercuté sur le conduit interne de l'oreille, puis capté en retour par un petit micro intégré.
Le processus ne dure que quelques centaines de millisecondes, ce qui permet une utilisation en mouvements et en continu. Commercialisé dès 2018, il pourrait être utilisé lors de missions sous haute sécurité et/ou nécessitant la discrétion, comme, par exemple, autoriser les accès à des sites sensibles pour les opérations de maintenance.

http://www.atelier.net/trends/articles/oreille-nouveau-systeme-identification-biometrique_440670?banner=1

### *132-16-ST-35* DÉVELOPPEMENT DE LA RECONNAISSANCE FACIALE (JANVIER)

Les entreprises de biométrie travaillent désormais à l'élaboration d'outils permettant non seulement la reconnaissance d'individus recherchés, mais également leur traçage à travers les flux vidéos.
Ainsi, Thalès a présenté en 2015 sa solution destinée aux aéroports, qui utilise la remontée automatique et intelligente de flux vidéo et alerte ainsi automatiquement l'opérateur dès qu'une identification est réalisée (besoin d'une base de données de traitement vidéo).
Pour faire face à la forte augmentation du volume de données de vidéo-surveillance, la filiale de Safran, Morpho, spécialisée dans les solutions biométriques, a développé un outil dénommé Morpho Video Investigator, qui va aider les enquêteurs à trier et classifier les informations en traitant plusieurs centaines d'heures de vidéo en quelques heures (détection, enregistrement et classement des éléments en mouvement contenus dans les images). Il devrait être commercialisé en février 2016 et déployé tout d'abord aux États-Unis.
Quant à la société Spikenet Technology, elle a mis au point une technologie de reconnaissance biométrique qui se fonde non pas sur les caractéristiques faciales d'un individu (comme les autres outils), mais sur la reconnaissance de forme. Elle peut identifier à la volée des personnes, des véhicules ou tout autre élément, en temps réel. D'ici deux ans, la société devrait même voir aboutir un projet de suivi multicible, réalisé avec des financements de la Direction générale de l'armement.

http://www.latribune.fr/technos-medias/electronique/la-reconnaissance-faciale-outil-de-tracage-prometteur-537258.html

## *132-16-ST-36* DES LUNETTES POUR DÉJOUER LA RECONNAISSANCE FACIALE ? (NOVEMBRE)

Le 6 novembre 2016, le site du Figaro a publié un article relatif aux résultats surprenants d'une étude menée par des chercheurs de la Carnegie Mellon University de Pittsburgh, selon laquelle il serait possible d'induire en erreur les outils d'identification fondés sur l'intelligence artificielle par le port de lunettes spéciales, dotées de motifs colorés et psychédéliques.
L'équipe est ainsi parvenue à faire passer certains de ses chercheurs pour d'autres membres du groupe ou pour certaines personnalités, dont l'actrice Milla Jovovich. Leur étude, relayée par le site Quartz, a été rendue publique le 28 octobre 2016, lors d'une conférence de cybersécurité à Vienne.
En faisant passer leurs propriétaires pour d'autres personnes, les lunettes développées par la Carnegie Mellon University sont plus sophistiquées que les parades anti reconnaissance faciale déployées jusqu'alors. Elles ont également l'avantage d'être plus discrètes que les lunettes AVG, utilisées pour aveugler les capteurs par l'émission d'une lumière ou que les techniques de camouflage présentées en 2010 par Adam Harvey, sous le nom de CV Dazzle. Ces dernières proposaient des façons de se coiffer ou de se maquiller propices à l'anonymat, mais difficiles à assumer en public.
Selon un spécialiste de la cybersécurité chez Visa, à New York, les systèmes d'identification ne tarderont pas à déjouer ce genre d'astuces. « Tout le monde est doté de ce qu'on pourrait appeler une empreinte physique multidimensionnelle. Le visage n'est qu'une seule de ces dimensions parmi d'autres, dont les cheveux, la silhouette, mais aussi les données liées à nos comportements, à nos trajets, à nos achats en ligne... Même en évitant la reconnaissance faciale, il va devenir de plus en plus difficile d'échapper à ce genre d'identification, à moins de prendre de très importantes précautions et de se tenir à une discipline précise que peu de personnes sont prêtes à respecter à la lettre ».

http://www.lefigaro.fr/secteur/high-tech/2016/11/06/32001-20161106ARTFIG00046-des-lunettes-pour-tromper-la-reconnaissance-faciale.php

## *132-16-ST-37* NOUVELLE VIDÉOSURVEILLANCE INTELLIGENTE (AVRIL)

Une équipe de chercheurs de l'IFSTTAR (Institut Français des Sciences et Technologies des Transports, de l'Aménagement et des Réseaux) a mis au point un boîtier de vidéo et audio surveillance dénommé DéGIV (détection et gestion d'incidents dans un véhicule ferroviaire) capable de détecter de manière autonome et en temps réel les comportements et situations inhabituels.
Résultat de dizaines d'années d'études sur les comportements et de modélisations dans les lieux d'attente comme les gares, les stations de métro ou les aéroports, il devait initialement être embarqué dans les trains mais ses capacités d'adaptation en font un outil prometteur pour la surveillance de tous les lieux publics. Il peut déjà assurer le suivi de personnes et pourra à terme identifier et ré-identifier des individus enregistrés par différentes caméras (exemple d'un individu identifié avec une valise puis à nouveau détecté sans).
En termes de prévention des actes de terrorisme, le système pourrait être affiné par

l'intégration d'une étude des comportements des poseurs de bombe, ce qui nécessiterait cependant l'accès aux images des attentats.

Actuellement en phase de pré-industrialisation par les entreprises partenaires comme Thalès et le Commissariat à l'énergie atomique et aux énergies alternatives (CEA), il fait également l'objet d'une offre de recherche auprès des pouvoirs publics.

http://www.20minutes.fr/lille/1813231-20160324-lille-systeme-videosurveillance-intelligent-securiser-lieux-publics

### *132-16-ST-38* « IRIS VISÉO » TESTÉE À PAU (AVRIL)

Dans notre revue N°125 du mois de mars 2015 (article 115-15-ST-03), nous évoquions la prévention et la surveillance des lieux publics grâce à un véhicule à cabine télescopique nommé « l'Iris VISEO ». Depuis mars 2016 , les policiers municipaux de Pau (Pyrénées-Atlantiques) testent cette voiture à l'allure futuriste, 100 % électrique, à poste de pilotage télescopique pouvant monter jusqu'à 3 mètres de hauteur.
L'entreprise qui commercialise ce véhicule vise désormais les marchés des enseignes de la grande distribution pour la surveillance des parkings, des grandes entreprises pour la surveillance de leurs sites ou encore les organisateurs d'événements. Les premières livraisons de ce véhicule sont prévues pour juillet 2016.

http://sciencepost.fr/2016/03/a-pau-police-teste-vehicule-electrique-etonnant/

### *132-16-ST-39* DES BALLONS D'OBSERVATIONS « MUNICIPAUX » DANS LE CIEL DU CHILI (OCTOBRE)

Dans le numéro de septembre 2016 de la Revue d'anthropologie des connaissances, deux sociologues de l'Université catholique du Chili publient un article intitulé « Urbanisme militarisé et situation cosmopolite, le cas des ballons aérostatiques de surveillance à Santiago du Chili ».
Dans deux des plus riches communes de Santiago du Chili, un système moderne de surveillance par aérostats a été mis en place, les ballons se situant à une altitude élevée avec des caméras à haute résolution contrôlées à distance. Ce système auto-identifié comme « smart », conçu initialement pour les guerres et les contrôles frontaliers, a été porté par des entités municipales pour pouvoir engager « la guerre contre la délinquance » et « gérer l'espace public plus efficacement ». Néanmoins, il a immédiatement généré une série de conflits liés aux profondes atteintes à la vie privée et à la surveillance excessive que pourrait impliquer ce dispositif dans la ville. Cet article décrit les tactiques diverses et opposées déployées par les acteurs impliqués dans la controverse : d'une part, le travail de ses promoteurs pour démilitariser et décontextualiser la technologie ; et d'autre part, la tentative de ses opposants de remilitariser et repolitiser cet artefact technologique de surveillance. Cette étude analyse de plus les opérations *in situ* de maintenance et de fonctionnement de ces aérostats de surveillance, ainsi que les façons qu'ont les personnes

de cohabiter avec ces dispositifs et de les aborder, en les intégrant dans leur vie quotidienne. À travers l'analyse de ces dynamiques, cet article montre comment cette technologie de surveillance étrangère adopte différents degrés de fonctionnement et se situe en tant qu'acteur avec différentes nuances, visions et activités.

http://www.cairn.info/revue-anthropologie-des-connaissances-2016-3-page-433.htm.

### *132-16-ST-40* TRANSFORMATION DE PORTRAITS DESSINÉS EN PHOTOS (JUIN)

Dans un article intitulé «Convolutional Sketch Inversion », une équipe de chercheurs de l'université de Radboud, aux Pays-Bas, décrit ses travaux sur une intelligence artificielle pouvant transformer divers types de portraits dessinés en images photoréalistes. Ils ont en effet développé « un réseau neuronal profond » capable de transformer un portrait dessiné à main levée en image photoréaliste. Cette nouvelle technologie pourrait être utilisée pour croiser des portraits-robots avec les bases de données de criminels fichés.

http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/technologie-cette-ia-transforme-portraits-dessines-photos-63192/

### *132-16-ST-41* L'INTELLIGENCE ARTIFICIELLE LUTTE CONTRE LES COMMENTAIRES VIOLENTS EN LIGNE (OCTOBRE)

Les sites Internet et les réseaux sociaux sont de plus en plus critiqués pour leur mauvaise modération des commentaires violents, haineux ou racistes. Pour autant, des êtres humains ne peuvent pas examiner à eux seuls des milliards de données par jour.
C'est pourquoi la filiale d'Alphabet, Jigsaw, a mis au point, en collaboration avec le New York Times, le projet d'intelligence artificielle « Conversation AI ». Ce dernier peut détecter les messages violents ou de harcèlement et donc aider les modérateurs à réagir plus rapidement. Pour ce faire, il a étudié pas moins de 17 millions de commentaires du journal précité pour comprendre ce qui est autorisé et ce qu'il ne l'est pas. D'après les créateurs du projet, le taux de réussite est de 92 %.
Pour contourner le programme, des utilisateurs assurent qu'il suffit de remplacer des mots injurieux par d'autres noms communs. Il est déjà possible de voir sur la Toile que les Juifs deviennent des Skypes, les Arabes des Skittles ou encore les homosexuels des papillons.
Pour Jigsaw, ce stratagème n'est en aucune manière efficace puisque « Conversation AI » utilise des technologies de learning très sophistiquées.

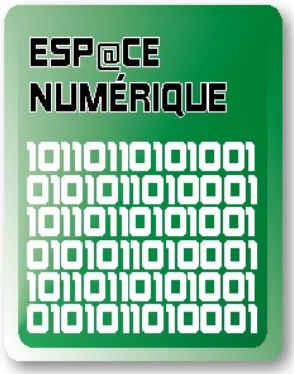
http://www.lefigaro.fr/secteur/high-tech/2016/09/22/32001-20160922ARTFIG00001-l-intelligence-artificielle-nouvelle-arme-contre-les-commentaires-violents-sur-internet.php
http://www.slate.fr/story/124475/racisme-google-yahoo-skype

### *132-16-ST-42* CHINE : LANCEMENT D'UN SATELLITE QUANTIQUE POUR BOULEVERSER LE MONDE DU CRYPTAGE (SEPTEMBRE)

La Chine a effectué, le 16 août 2016, le premier lancement mondial d'un satellite à communication quantique, l'objectif à long terme étant d'édifier un réseau mondial de communications cryptées et inviolables.
Mais qu'est-ce que la « communication quantique » aussi appelée la « téléportation quantique » ? Ces termes font référence à l'utilisation de photons, des particules fondamentales du champ électromagnétique, pour envoyer les clés de cryptage indispensables au décodage de l'information. Les données contenues dans ces photons sont impossibles à intercepter et toute tentative entraînerait leur autodestruction.
Il est vrai que cette technologie a déjà montré son efficacité mais sur de courtes distances (moins de 300 km). La Chine souhaite désormais devenir le pionnier de cette technique en plein essor sur des distances plus significatives. En effet, son nouveau satellite devra prochainement tenter d'envoyer des données entre Pékin et la capitale de la région du Xinjiang, Urumqi, deux villes séparées par près de 2500 km. Or, « ce sera comme lancer une pièce de monnaie d'un avion volant à 100 km d'altitude et espérer qu'elle vienne se ficher exactement dans la fente d'une tirelire-cochon en rotation », a expliqué Wang Jianyu, le chef du projet. Il n'est pas certain que la communication quantique soit pour demain. Formulé de cette manière, il n'est pas évident de croire que la communication quantique sur de longues distances sera opérationnelle sous peu.

http://www.lexpress.fr/actualite/sciences/avec-son-premier-satellite-quantique-la-chine-veut-revolutionner-le-cryptage_1821700.html
http://hightech.bfmtv.com/securite/la-chine-lance-un-satellite-quantique-pour-rendre-ses-communications-inviolables-1026905.html
http://www.usinenouvelle.com/editorial/comment-fonctionne-la-cryptologie-quantique-de-l-espace-mise-au-point-par-la-chine.N426367

## *ESPACE NUMÉRIQUE*




### *132-16-EN-01* RAPPORT D'ACTIVITÉ 2014-2015 DE L'HADOPI (JANVIER)

La Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet a mis en ligne son cinquième rapport d'activité annuel.
Le rapport rappelle les missions de l'HADOPI, à savoir encourager le développement de l'offre légale sur Internet, évaluer les expérimentations menées sur la reconnaissance des contenus et les filtres, étudier les moyens techniques pour utiliser illégalement des œuvres protégées par des droits d'auteur, réguler et veiller les dispositifs techniques de protection et d'identification des œuvres protégées, protéger les œuvres et objets protégés bénéficiant d'un droit d'auteur.
S'agissant des modes de consommation, le rapport constate que la gratuité est largement privilégiée par les internautes (93 % pour les programmes TV, 83 % pour les films et 69 % pour les livres en streaming, les chiffres étant respectivement de 88 %, 79 % et 66 % pour le téléchargement). Les internautes qui ont des pratiques illégales jugent inefficaces les mesures de fermeture et de blocage de sites puisqu'ils parviennent le plus souvent à trouver une offre alternative. En revanche, depuis la fermeture du site Megaupload, ils constatent un éparpillement de l'offre et une baisse qualitative des contenus.
L'HADOPI propose un nouveau service destiné aux internautes qui ne trouvent pas en ligne la diffusion légale d'une œuvre. Ils peuvent signaler des œuvres qu'ils recherchent en vain. L'objectif est de proposer des solutions de téléchargement légales lorsqu'elles existent et de signaler aux ayant-droits l'intérêt du public pour une œuvre particulière. Une liste des œuvres signalées par les internautes est disponible sur le site de l'HADOPI.
S'agissant de la procédure de réponse graduée aux comportements illicites, l'HADOPI a adressé 4,9 millions premières recommandations, 482667 recommandations de second niveau et a envoyé 2712 lettres recommandées à des internautes, avec au final 361 transmissions au procureur de la République. Sur le plan financier, l'HADOPI a connu un exercice déficitaire à hauteur de 2,46 millions € (8,19 millions € de charges)
En annexe 3, un tableau présente les dispositifs de lutte contre la contrefaçon dans neuf pays (Allemagne, Australie, Canada, Etats-Unis, Irlande, Nouvelle-Zélande, Royaume-Uni, Suisse et Taïwan).

http://www.hadopi.fr/sites/default/files/HADOPI_RA_2014-2015.pdf

### *132-16-EN-02* LES RÈGLES DE LA NEUTRALITÉ DU NET CONFIRMÉES EN APPEL AUX ÉTATS-UNIS (JUIN)

Une cour d'appel américaine a confirmé les règles de la neutralité du Net, empêchant les fournisseurs d'accès de différencier leurs tarifs selon leurs abonnés ou de bloquer l'accès à certains services en ligne. Les fournisseurs d'accès au Net sont appelés à respecter les

règles de neutralité et à ne pas différencier leurs tarifs selon leurs abonnés. Les règles de la neutralité du Net sont en effet des principes de régulation qui visent à empêcher un Internet à deux vitesses, dans lequel tous les abonnés ne seraient pas soumis aux mêmes tarifs ou n'auraient pas accès aux mêmes services. Elles ont été confirmées par la Cour d'appel fédérale de Washington, qui a appuyé la décision de la Commission Fédérale des Communications (FCC) : celle-ci considère les Fournisseurs d'Accès Internet (FAI) comme des compagnies de télécommunications normales et soumises aux mêmes réglementations. Cette décision était contestée notamment par les deux plus gros opérateurs téléphoniques américains Verizon et AT&T qui affirment qu'elles aboutissent à réduire les possibilités d'accès et découragent l'investissement. Le juge a estimé dans sa décision que la FCC n'avait pas outrepassé son pouvoir réglementaire. « *Le rôle des fournisseurs d'accès à haut débit est analogue à celui des services de télécommunications : ils doivent agir en tant qu'opérateurs neutres et non discriminants dans la transmission des communications de tous les usagers* », a-t-il souligné. Cette décision est une victoire pour les associations de consommateurs et certains autres fournisseurs qui estimaient que si la décision de la FCC avait été infirmée, des services comme Netflix auraient pu voir leur diffusion handicapée par les fournisseurs souhaitant favoriser leurs propres programmes. Cette décision s'applique également aux fournisseurs d'accès pour les appareils mobiles. Deux précédentes tentatives de la FCC pour garantir la neutralité du Net avaient été rejetées en appel mais l'agence a eu recours pour sa troisième tentative à une base légale différente lui permettant de s'appuyer sur une réglementation de 1994 s'appliquant aux compagnies de téléphone. Cette décision peut toutefois encore faire l'objet d'un examen et d'une décision de la Cour suprême des États-Unis.

http://www.sciencesetavenir.fr/high-tech/informatique/20160615.OBS2592/les-regles-de-la-neutralite-du-net-confirmees-en-appel-aux-etats-unis.html

### *132-16-EN-03* LA CNIL RÉFLÉCHIT À LA NOTION DE PARTAGE DANS LE MONDE NUMÉRIQUE (SEPTEMBRE)

Dans un cahier IP (innovation et prospective) de juin 2016, la CNIL se penche sur les « motivations et contreparties au partage de soi dans la société numérique ». Dans ce document de 18 pages, les rédacteurs détaillent dans un premier chapitre la nature et les modalités du partage numérique. Ils étudient ensuite la manière dont la valeur se partage (ou pas) puis les conséquences de ce partage sur l'équilibre des pouvoirs. Enfin, le dernier chapitre s'intéresse aux leviers de régulation.
Le premier chapitre comprend un guide de lecture fort explicite qui détaille ce que partagent, dans quelles conditions et pour quelles raisons, un utilisateur de Wikipedia, un client d'AirBnB, un titulaire de compte Facebook, un utilisateur de l'application Waze ou encore un chauffeur travaillant pour la société Uber. La partie consacrée au partage de la valeur pose les questions incontournables sur la valeur de la donnée et la notion de propriété.
Le chapitre consacré à l'équilibre des pouvoirs (entre l'État, les individus et les sociétés commerciales) comprend un cas concret virtuel : un scénario fictif basé sur la réflexion et l'état de la réglementation et de la technologie invite à envisager les conséquences sur les libertés individuelles du développement d'une « clef universelle de réputation » ainsi que la

vision juridique qu'auraient les instances européennes de ce dispositif.
Ce cahier très didactique offre un support très argumenté pour qui souhaite réfléchir aux notions de propriété des données et de la valeur ajoutée créée autour de ces dernières dans l'espace numérique.

https://www.cnil.fr/sites/default/files/atoms/files/cnil_cahier_ip_partage_version_finale_web_1.pdf

### *132-16-EN-04* LOI POUR UNE RÉPUBLIQUE NUMÉRIQUE (OCTOBRE)

Publiée au Journal Officiel du 8 octobre 2016, la loi relative à une République numérique aborde, en trois titres, les aspects fondamentaux liés à cette nouvelle technologie. Véritable loi fondamentale de l'espace du numérique, le texte traite successivement de la circulation des données et du savoir, de la protection des droits dans la société numérique (environnement ouvert, protection de la vie privée en ligne) et, dans son dernier titre, de l'accès au numérique (territoire, facilitation des usages, accès aux publics fragiles). Autour de ce triptyque, il convient de souligner deux points touchant à la gouvernance, prémisses de changements majeurs. S'agissant du premier, la Commission Nationale Informatique et des Libertés (CNIL) et la Commission d'Accès aux Documents Administratifs (CADA) disposent légalement du droit de se réunir dans un collège unique lorsqu'un sujet d'intérêt commun le justifie. Pour certains juristes et avocats, cette nouvelle disposition serait l'amorce d'une fusion de la CNIL et de la CADA. L'autre point de la loi porte sur la réflexion que le Gouvernement aura à engager à propos de la création d'un Commissariat à la souveraineté numérique. L'article 29 de la loi prévoit que le Gouvernement remette un rapport d'opportunité au Parlement dans un délai de trois mois à compter de sa promulgation. Ce Commissariat participerait, dans le cyberespace, à l'exercice de la souveraineté nationale, des droits et des libertés individuels et collectifs en vigueur en France. Pêle-mêle, cette loi aborde des sujets sensibles allant de l'usage des algorithmes dans les services publics au champ d'application de l'article 40 du Code de procédure pénale (CPP) en matière de défense. Sauf exceptions légales, lorsqu'un algorithme participe à la prise d'une décision individuelle rendue par un service public, l'intéressé doit en être informé par une mention explicite. À la demande de cet usager, l'administration devra communiquer les principales caractéristiques de la mise en œuvre de ce traitement algorithmique. S'agissant de la mise en œuvre de l'article 40 du CPP, la loi insère dans le Code de la défense une disposition qui vise à protéger « l'agent de bonne foi qui transmet à la seule Autorité Nationale de Sécurité des Systèmes d'Information (ANSSI) une information sur l'existence d'une vulnérabilité concernant la sécurité d'un Système de Traitement Automatisé de Données (STAD) ».

*NDR : La loi pour une République numérique impacte pas moins de 23 codes et 11 lois dans ses dispositions. À ce titre, elle constitue bien une véritable loi fondamentale au regard des évolutions et/ou modifications qu'elle apporte dans différents instruments de valeurs normatives.*

https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000033202746

## *132-16-EN-05* RAPPORT 2015 DE L'ARCEP (SEPTEMBRE)

L'Autorité de Régulation des Communications Électroniques et des Postes a mis en ligne en juin 2016 son rapport d'activité 2015. Ce document de 264 pages fait le point sur l'ensemble des missions de cette autorité administrative indépendante. Son manifeste, qui figure en tête du rapport, rappelle que « les réseaux d'échanges Internet, télécom fixes, mobiles et postaux, constituent une infrastructure de liberté ». Leur développement doit se faire comme celui d'un « bien commun » : accessibilité, universalité, performance, neutralité, confiance et loyauté constituent des éléments sur lesquels l'ARCEP est par conséquent extrêmement vigilante.
S'agissant de mobilité, les chiffres clés livrés par le rapport permettent de se faire une juste idée du développement de ce secteur. En 2015, la France compte 26,9 millions d'abonnements fixes en haut et très haut débit (900 000 de plus qu'en 2014) quand ce chiffre était de 700 000 en 2008. Le nombre de cartes SIM en service atteint 72,1 millions, soit 450 000 de plus qu'en 2014. Les clients changent beaucoup d'opérateurs puisque 6 millions de numéros ont bénéficié de la portabilité d'un opérateur à l'autre. Le rapport constate que les deux tiers des contrats sont sans engagement de durée, ceci favorisant cela. Par ailleurs, 22 millions de personnes utilisent Internet mobile. En moyenne, chaque carte échange 679 Mo de données par mois. Ramenée aux seuls utilisateurs d'Internet, la masse de données envoyées et reçues par carte atteint 1,2 Go par mois. S'agissant des SMS et MMS, plus de 206 milliards de ces messages ont été envoyés.
Les objets connectés utilisent également des cartes SIM, non comptabilisées dans les chiffres déjà cités. Elles sont 10,55 millions en 2015, soit 2,3 millions de plus qu'en 2014.
80 % des Français de 12 ans et plus ont un ordinateur, 58 % un smartphone, 35 % une tablette. En tout, 83 % ont accès à Internet. Les Français non connectés ont tous plus de 40 ans (59 % ont 70 ans et plus), ont de faibles revenus et sont peu diplômés. Les deux tiers sont retraités et 52 % habitent des communes de moins de 20 000 habitants.
Le rapport comporte de nombreux autres chiffres qui dressent un portrait très fin de la France numérique et des évolutions en cours. Ainsi, plus de la moitié des utilisateurs d'Internet effectuent des démarches administratives et vont sur les réseaux sociaux. Notons que ces utilisateurs des réseaux sociaux s'en servent à 71 % pour s'informer (contre 54 % en 2014). Un tiers des Français envisage désormais d'utiliser des services domotiques, 6 % ayant déjà franchi le pas (ils étaient 4 % en 2014).
L'ensemble des mesures envisagées pour répondre aux objectifs stratégiques de l'ARCEP sont développées dans ce document.

http://www.ladocumentationfrancaise.fr/rapports-publics/164000561-rapport-public-d-activite-de-l-arcep-2015?xtor=EPR-526

## *132-16-EN-06* SAISINE DE L'ADMINISTRATION PAR LES USAGERS À L'AIDE D'UN TÉLÉSERVICE (JUIN)

Un décret du 27 mai 2016 encadre la mise en œuvre du droit des usagers de saisir l'administration par voie électronique. Ce texte est applicable seulement à l'État et à ses

établissements publics à caractère administratif. Les catégories d'usagers concernés sont : les particuliers, les entreprises et les associations. Dans le cadre des diverses saisines et instructions des demandes provenant de certains usages, les téléservices recueilleront un nombre conséquent de données à caractère personnel. En raison de la nature sensible de ce type de données, le décret prévoit une traçabilité des accès des systèmes de traitement automatisés effectués par les agents habilités à cet effet. Cette traçabilité des accès englobe les opérations de consultation, de création, de modification ou de suppression des données émises par les usagers. L'article 4 alinéa 1er du décret prévoit de manière expresse que « la durée de conservation des données à caractère personnel et informations enregistrées ne peut excéder de deux années le délai d'instruction des saisines ». Cependant, une politique de mise en œuvre de conservation en base intermédiaire des données relatives aux saisines des usagers est autorisée sous certaines conditions : accès restrictifs, durée maximale de dix années. Au-delà de la durée d'utilité administrative, les données sont régies par les dispositions du Code du patrimoine. Dans sa délibération du 21 avril 2016, la Commission Nationale Informatique et Libertés (CNIL) souligne que même si la simplification des démarches administratives et l'amélioration des relations entre les administrés et l'administration constituent des finalités légitimes, des mesures de sécurité appropriées doivent être prévues, tout comme le respect des droits des personnes.

https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000032592483
https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000032593065

### *132-16-EN-07* PANORAMA MONDIAL 2015 DE LA CYBERCRIMINALITÉ (FÉVRIER)

C'est à l'occasion d'un colloque, organisé le 14 janvier 2016 par le Club de la sécurité de l'information français (Clusif), qu'un bilan a été réalisé concernant l'état de la cybercriminalité mondiale. Tout d'abord, il est convenu que l'année 2015 a encore été marquée par la technicité et la ruse déployées par les cybercriminels, afin de détourner des objets et des systèmes à des fins frauduleuses et aboutissant à une certaine forme de « célébrité » sans oublier l'encaissement de gains considérables.
Le DarkNet voit s'ouvrir régulièrement de nouvelles boutiques en ligne où se vendent, par exemple, des produits à haute valeur ajoutée (site TheRealDeal) tels que des codes O-day (Zero-Day), permettant des attaques sur les failles encore indétectées des systèmes d'exploitations. Le marché est très juteux et favorise le développement de métiers tels que le Bug Bounty (révélation de failles aux éditeurs contre forte rémunération) et de plateformes où se versent des primes considérables à chaque découverte. Un autre danger est la récupération récente du DarkNet et de ses boutiques par les djihadistes, et plus particulièrement ceux de Daesh, où ils dispensent, via leurs spécialistes, des conseils en matière de communication et de chiffrement.
Par ailleurs, Internet et ses réseaux sociaux sont désormais largement exploités par les groupes extrémistes à des fins de radicalisation, de recrutement et de marketing. D'où, suite à une prise de conscience des autorités et des forces de l'ordre, le développement de l'antiterrorisme 2.0. Depuis janvier 2015, les signalements effectués sur la plate-forme Pharos ont été multipliés par 10 par rapport à la normale et ne cessent d'augmenter,

permettant une lutte active grâce aux dénonciations de plus en plus pertinentes de contenus annonçant des attentats ou relevant de l'apologie. Par ailleurs, la coopération entre les services antiterroristes et de lutte contre la cybercriminalité progresse régulièrement, favorisant des échanges entre expertise et soutien technico-judiciaire dans le cyber.
Sur le plan juridique, les textes consacrés à la prévention du terrorisme se sont multipliés, suscitant critiques et débats de fond : loi du 24 juillet 2015 relative au renseignement, loi du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, loi du 20 novembre 2015 déclarant l'état d'urgence et compléments apportés à la loi de 1955 (ajout de pouvoirs d'investigation numérique aux prérogatives administratives de la police, possibilité accordée au ministre de l'Intérieur d'ordonner l'interruption d'un service de communication en ligne faisant l'apologie ou provoquant à la commission d'actes terroristes). Différents projets de loi devraient être adoptés cette année : le projet de loi constitutionnelle pour la protection de la Nation, la proposition de loi renforçant la lutte contre le crime organisé et son financement, l'efficacité et les garanties de la procédure pénale ou encore le droit au chiffrement.
L'innovation 2015 la plus sérieuse et aux enjeux des plus élevés, est le piratage des objets connectés (poupées, fusils de sniper, babyphones, matériels médicaux...), et plus particulièrement des voitures connectées dont les conséquences d'un détournement pourraient être extrêmement graves. L'importance quantitative (et qualitative) de ces attaques réussies met en avant les défauts de conception de ces objets et des tests de sécurité, chaque type d'objet devant avoir un système de sécurité adapté, ce qui nécessite non seulement les compétences nécessaires mais une réflexion de fonds sur leur sécurisation et leur régime juridique (gestion des données collectées).

https://www.expoprotection.com/CYBERSECURITE/Article.htm?Zoom=59126d59684d63a536973a34c02c3b7a

### *132-16-EN-08* RAPPORT 2016 DE SÉCURITÉ CISCO (FÉVRIER)

Cisco a profité du Forum International de la Cybersécurité (FIC), organisé les 25 et 26 janvier 2016, pour dévoiler son rapport 2016. Réalisé suite à une enquête menée auprès de 2400 professionnels et grâce à une surveillance interne du Web, il constate en premier lieu la confirmation du développement des ransomwares (rançongiciels), dits malwares « faciles ». Le rapport pointe également le peu d'implication des DNS (Domain Name System) dans la cybersécurité et le risque lié aux extensions malveillantes des navigateurs. Enfin, la société remarque que les entreprises sont toujours aussi frileuses dans leur réaction face aux attaques ; très peu les annoncent aux partenaires (moins de 25%) et encore moins le font aux autorités et aux assureurs.
Il est encore rappelé les bons réflexes à adopter pour se prémunir au mieux : faire des sauvegardes régulières, éduquer les utilisateurs, se doter des outils nécessaires à la détection et à l'analyse des menaces…

http://www.linformaticien.com/actualites/id/39295/cisco-devoile-son-rapport-annuel-de-securite.aspx

### *132-16-EN-09* 2015 : UNE VINGTAINE DE CYBERATTAQUES MAJEURES CONTRE LA FRANCE (SEPTEMBRE)

C'est ce qu'a révélé le premier rapport d'activité rédigé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), rattachée au Secrétariat Général de la Défense et la Sécurité Nationale (SGDSN) et publié le 13 septembre 2016.
En augmentation de 50 % par rapport à 2014, plus fortes et mieux organisées, elles auraient principalement touché les entreprises lors d'appels d'offres internationaux, ce qui indique un espionnage économique évident. Elles mettent également à mal les réseaux informatiques touchés car il faut compter entre six mois et deux ans de réparations. A été constatée l'émergence de nouvelles attaques, dont les « rançongiciels », des logiciels malveillants chiffrant les données d'un ordinateur, qui sont alors prises en otage le temps de payer une rançon. 2300 codes malveillants ont été identifiés en 2015. L'année 2015 a également été marquée par 568 avis de correctifs de sécurité et quinze alertes sur des vulnérabilités critiques concernant des OIV (Opérateur d'Importance Vitale).

http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/la-france-a-ete-la-cible-d-une-vingtaine-de-cyberattaques-majeures-en-2015-598189.html#xtor=EPR-2-[industrie-services]-20160913

### *132-16-EN-10* L'ÉTUDE D'EUROSTAT SUR LA PERMÉABILITÉ DE L'INTERNET EUROPÉEN FACE AUX PROBLÈMES DE SÉCURITÉ (FÉVRIER)

À la veille de la « Journée mondiale pour un Internet plus sûr » qui s'est déroulée le 09 février 2016, l'Office statistique de l'Union européenne (Eurostat) a publié un communiqué de presse relatif à une enquête sur les internautes européens qui ont rencontré un problème de sécurité en 2015.
De prime abord, il convient de préciser les critères retenus. L'enquête porte sur des personnes âgées de 16 à 74 ans (sans pour autant en préciser le nombre) et sur leur usage d'Internet lors des douze mois précédant ladite enquête. Le communiqué précise par ailleurs la définition de « problème de sécurité » qui désigne un des cinq incidents suivants : le virus, la violation de la vie privée, la perte financière suite à un phishing, la perte financière due à un paiement frauduleux par carte et l'accès par des enfants à des sites web inappropriés.
Sur cette base, l'enquête a conclu que 25 % des utilisateurs européens d'Internet ont rencontré, au cours de l'année 2015, un problème de sécurité. Néanmoins, la réalité est bien plus disparate puisque en République Tchèque, au Pays-Bas ou encore en Slovaquie, ce chiffre est inférieur à 15 % contre 33 % en France ou 42 % en Croatie.
Le principal problème de sécurité est lié aux virus et aux infections informatiques avec 21 % des internautes de l'UE touchés en 2015. Il convient de souligner que ce chiffre révèle une nette amélioration par rapport à 2010 (31%).
Les craintes liées à la sécurité conduisent inévitablement certains utilisateurs à s'abstenir d'effectuer certaines activités en ligne. A titre d'exemples, 1 personne sur 5 n'a effectué aucun achat en ligne ou encore 13 % des internautes ne se connectent jamais à un réseau

Wi-FI autre que celui de leur domicile.

http://ec.europa.eu/eurostat/documents/2995521/7151128/4-08022016-AP-FR.pdf/9561ece2-b393-4360-bf18-5d4dffc11e0d

***132-16-EN-11*** **LES INQUIÉTANTES PERSPECTIVES DE LA CYBERCRIMINALITÉ POUR 2016 (JANVIER)**

L'année 2015 a été celle de l'augmentation des piratages informatiques. Selon les prévisions, la tendance devrait se prolonger pour 2016. De nombreux organismes, comme le Cercle européen de la sécurité et des systèmes d'information ont effectué cette mise en garde. « Un cyber-sabotage » de grande ampleur est même redouté pour 2016.
Le cabinet PricewaterhouseCoopers a pointé du doigt le fait que les cyber-attaques à l'encontre des entreprises ont augmenté de 38% en un an dans le monde et de 51% pour la France sur cette même période. Les pertes financières pour les entreprises touchées sont considérables et se chiffrent en moyenne aux alentours de 4 millions d'euros par entreprise. Mais à l'échelle des particuliers, les escroqueries, comme le vol de données bancaires, se sont accrues.
Aujourd'hui, le danger est considéré comme pouvant venir de partout. Dès lors, difficile de pouvoir le cerner. En 2015, l'Allemagne a ainsi été la cible de deux types d'attaques particuliers : la mise hors-service d'un haut fourneau et le piratage de l'ordinateur personnel de la chancelière, Angela Merkel. La France, quant à elle, avait subi l'attaque de la chaîne TV5Monde.
Les hackers utilisent des méthodes de plus en plus sophistiquées. L'entreprise de sécurité informatique Bitdefender prévoit des évolutions pour 2016. Le monde de l'entreprise devrait être encore plus touché. Le vol d'informations devrait se retrouver plus que jamais au cœur des problématiques, la multiplication des objets connectés tendant à accroître le mouvement.
Une convergence accrue des formes de terrorisme physique et virtuel est également redoutée.
Face à cela, les organisations sont incitées à renforcer leurs pratiques de sécurité et les gouvernements à poursuivre leurs efforts dans la mise en place de réglementations plus claires en faveur de la lutte contre les cybermenaces. Le développement des technologies de chiffrement ainsi que leur plus grande mise à disposition de tous est également une des thématiques de réflexion pour 2016.

http://www.ouest-france.fr/faits-divers/attentat/cybercriminalite-crainte-dattentats-declenches-distance-en-2016-3945942
http://www.infodsi.com/articles/160284/cybercriminalite-libertes-individuelles-ur-preoccupations-securite-2016-jean-francois-pruvot-regional-director-france-chez-cyberark.html
http://www.rfi.fr/france/20151228-cybercriminalite-informatique-systemes-malware-cryptogramme-connecte-hacker-securite

## *132-16-EN-12* LES DERNIÈRES PRÉVISIONS EN CYBERCRIMINALITÉ (JANVIER)

Symantec et Norton (éditeurs de solutions de sécurité informatique) font le point sur les risques qui pèsent sur nos données et notre patrimoine digital en 2016 et dans un futur proche, et donnent quelques recommandations.
En matière de vulnérabilité : chaque utilisateur d'Internet doit s'approprier le concept de « sécurité dès la conception » (*Security by Design*, en anglais), qu'il soit particulier, industriel ou appartenant au secteur de la sécurité, prendre en compte l'ensemble des menaces se développant (attaques via les objets connectés et les smartphones, les liens publicitaires et rançongiciels, les voitures et appareils médicaux connectés,…), faire évoluer les stratégies de protection des données et adopter les bons comportements. Les modes de production des nouvelles technologies devront intégrer une sécurisation des programmations, des mises à jour et de l'identification des utilisateurs, particulièrement en ce qui concerne la robotique, les Smart Cities et les Smart Grids.
En ce qui concerne la cyberassurance, les utilisateurs seront encouragés par les assureurs à adopter des pratiques de sécurité tandis que les personnels suivront des formations.
Du côté législatif, la prochaine directive européenne sur la protection des données incitera les entreprises à respecter de nouvelles exigences en matière de traitement des données personnelles et des règles de conformité plus strictes.
L'étude de l'évolution des menaces démontre que la sophistication des attaques ne concerne plus seulement celles d'origine étatique mais également celles réalisées par des individus ou des groupes malveillants, leur professionnalisme s'améliorant. Par ailleurs, il est noté un ciblage de plus en plus précis des attaques, soit dans le but d'être le moins repérable possible (recours à des serveurs dédiés, à des logiciels inédits,...) , soit à des fins politiques. La détection et la protection passeront par une meilleure corrélation entre les différents secteurs d'activité et les pays et la mise en place de partenariats.
Enfin, il est fortement envisagé le développement de nouveaux moyens d'authentification, notamment via les électrocardiogrammes (ECG) et les veines de la main. En effet, l'association identifiant/mot de passe n'est plus assez sécurisée.

https://www.expoprotection.com/CYBERSECURITE/Article.htm?Zoom=be10679d81f01aa1d56961988082e075&SType=CRITERIA&Start=20&Search=TAGMENU1_C_

## *132-16-EN-13* CYBERCRIMINALITÉ ET PAIX EN AFRIQUE FRANCOPHONE (FÉVRIER)

À l'initiative de l'Organisation Internationale de la Francophonie (OIF), en partenariat avec le gouvernement ivoirien et l'Agence de Régulation des Télécommunications de la Côte d'Ivoire (ARTCI), une conférence internationale sur le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone s'est tenue, du 8 au 10 février 2016, à Grand-Bassam, en Côte d'Ivoire.
Pour ces experts d'une vingtaine de pays francophones, la cybercriminalité constitue un obstacle au développement économique et social et une menace pour la paix et la stabilité.

Les participants se sont accordés sur la mise en place de stratégies politiques et juridiques nationales avec le respect des droits fondamentaux, une meilleure collaboration et une mutualisation des ressources. Ils ont aussi insisté sur l'importance de l'éducation aux nouvelles technologies et à leur sécurité des jeunes. Un comité scientifique et un observatoire sur la cybersécurité et la cyberdéfense de l'espace francophone seraient envisageables.

*NDR : L'OIF lance la 2ème saison des « Innovathons » de la Francophonie sur la cybersécurité à travers le concours #Ris[S] (Recettes informatiques de Scripts et Kits), qui propose aux participants d'explorer les systèmes informatiques similaires à ceux utilisés par les administrations publiques, afin d'identifier les risques de cyberintrusion qu'elles encourent au quotidien et apporter des solutions pour parer à ces périls potentiels.*

http://www.afriqueitnews.com/2015/09/09/cybercriminalite-lafrique-prend-mesure-danger/
http://www.francophonie.org/Discours-d-Adama-Ouane-a-Grand.html
http://www.francophonie.org/IMG/pdf/note_conceptuelle_conference_cybersecurite_abidjan_2016.pdf
http://www.lemonde.fr/afrique/article/2016/02/09/la-cybercriminalite-une-menace-contre-la-paix-en-afrique-francophone_4861845_3212.html

***132-16-EN-14*** **L'AVIATION CIVILE N'EST PAS À L'ABRI DU CYBER-TERRORISME (JANVIER)**

En octobre 2015, lors d'un petit-déjeuner organisé par l'Association des Journalistes Professionnels de l'Aéronautique et de l'Espace (AJPAE), le directeur exécutif de l'Agence Européenne de Sécurité Aérienne (AESA) avait prévenu : « l'aviation civile doit se préparer aux cyber-risques ». Il est formel : le piratage informatique est possible et la cybercriminalité représente bien une menace pour le transport aérien. Pour illustrer ses propos, il a fait appel à un hacker, titulaire d'une licence de pilote d'avion commercial, qui est parvenu en quelques minutes à entrer dans le système de messagerie ACARS (Aircraft Communication Addressing and Reporting System) en se faisant passer pour un des administrateurs du réseau. Ce système permet aux compagnies aériennes d'échanger des informations entre l'avion et le sol sous forme numérique codée par liaison radio ou satellite, pour s'assurer du bon fonctionnement des systèmes critiques de l'avion. Il n'a fallu au hacker que deux ou trois jours pour pénétrer dans le système de contrôle d'un avion au sol.
Pour limiter les risques de piratage, l'AESA pourrait, à long terme, se charger de certifier les équipements contre les risques de cyberattaques sachant qu'elle a déjà la responsabilité de certifier les aéronefs en Europe. A court terme, le directeur exécutif de l'agence voudrait mettre en place des « réseaux spécifiques » de spécialistes en cyberattaques pour « informer de la menace et des moyens de s'en prévenir ».

https://www.expoprotection.com/SURETE-ET-SECURITE/Article.htm?Zoom=bd9a0c2c2da1c8663814ea0b9e1606a1

### *132-16-EN-15* INTERNET DES OBJETS, SÉCURITÉ ET VIGILANCE (MARS)

Le site zdnet.fr met en ligne un article traitant du « cauchemar sécuritaire » de l'Internet des objets (IoT – *Internet of Things*). Selon les estimations, 6,5 milliards d'objets seront connectés en 2016, 5 millions se rajoutant chaque jour à ce chiffre. Selon l'auteur de l'article, l'IoT se développe d'une part en connectant entre eux des systèmes pré-existants, d'autre part en englobant des systèmes spécialement créés à cet effet, souvent en ne considérant la sécurité qu'en second plan, bien après l'usage. Il en résulte deux types de menaces différentes. Au-delà des questions de piratage proprement dit se pose l'enjeu des données privées, collectées et utilisées en masse par les objets connectés. De l'usage des appareils connectés dépend le niveau de danger induit par un piratage éventuel : il est a priori moins dangereux de prendre le contrôle d'une ampoule électrique que d'un véhicule circulant sur une voie rapide… D'autre part, plus l'objet est autonome et plus le niveau de risque est susceptible d'augmenter. Selon l'auteur, le salut pourrait bien venir de l'informatique en nuage, le fameux cloud. Il suppose en effet que des offres de services viendront bientôt proposer aux usagers de superviser et sécuriser les objets connectés. Par ailleurs, le chiffrement des données en transit sera également un élément de réponse à la menace. « L'IoT requerra la capacité de segmenter le réseau et de considérer que nombre des terminaux connectés à celui-ci sont au mieux vulnérables et au pire un risque de sécurité », avance le journaliste.

http://www.zdnet.fr/actualites/internet-des-objets-trouver-un-moyen-de-sortir-du-cauchemar-securitaire-39833608.htm

### *132-16-EN-16* LE SECTEUR ÉNERGÉTIQUE EXPOSÉ À LA CYBERMENACE EN EUROPE (SEPTEMBRE)

Un document, mis en ligne par l'Institut Français des Relations Internationales (IFRI) se présente comme une synthèse sur la cybermenace dans le secteur énergétique. L'analyse et le traitement des données appliqués aux systèmes industriels ouvrent de nouvelles opportunités mais exposent également à de nouvelles menaces. Or, l'industrie énergétique n'y serait pas totalement préparée, pour trois raisons principales : les compétences informatiques requises pour faire face à ce type de risques ne sont pas encore suffisamment identifiées ; jusqu'à cette révolution numérique, les logiciels utilisés dans les processus industriels étaient le plus souvent développés en interne et donc échappaient à une éventuelle prise en main extérieure, ce n'est plus le cas aujourd'hui avec, par exemple, les systèmes d'exploitation tels Windows ou Linux ; d'ordre organisationnel : les « canaux de communication » entre le site de production et les autres services, transformation, transport etc, les accès à distance, la complexité des mises à jour ont créé d'importantes vulnérabilités.
Les incidents de sécurité les plus importants sont rappelés : en décembre 2015 en Ukraine, coupure de plusieurs opérateurs électriques privant d'électricité 200 000 foyers ; en 2010 le ver informatique Stuxnet impactant des infrastructures nucléaires iraniennes. Une simulation de la compagnie d'assurance Lloyd's a évalué à un minimum de 243 milliards de dollars le coût de la remise en service du réseau électrique de 15 États américains si ceux-ci étaient

victimes d'une cyberattaque.
Les Systèmes de Contrôle Industriels (SCI) étant souvent similaires d'une industrie à l'autre, incluant différents secteurs d'activité, les mêmes logiciels malveillants « circulent facilement entre les entreprises ». En Europe, l'interconnexion des réseaux électriques rend le système fragile, avec un fort risque d'impact « en cascade ».
La note s'achève par le bilan des actions entreprises pour se prémunir contre d'éventuelles attaques, en montrant les progrès accomplis et les limites de l'harmonisation et de la coopération européennes.

https://www.ifri.org/sites/default/files/atoms/files/edito_desarnaud_cybermenace_energie.pdf

### *132-16-EN-17* PROFESSIONNALISATION DU CYBERCRIME (MAI)

Le blog Knowledge de l'INSEAD a mis en ligne le 11 avril 2016 un article sur la professionnalisation des cybercriminels. Son auteur, titulaire de la chaire de gouvernance et de stratégie d'entreprise, explique que l'activité criminelle sur Internet a pris un tour professionnel notamment grâce aux facilités offertes par le *dark net*. Véritable marché guidé par la demande, le crime s'est organisé en adaptant la qualité et la diversité de ses offres de service. Pour reprendre les termes du langage économique, le crime en tant que service (« *crime as a service* ») fonctionne aussi bien en Business-to-Business (entre professionnels) qu'en Business-to-Consumer (relation professionnel-consommateur). Ainsi, des criminels proposent à d'autres criminels des services tels que la fourniture de logiciels malicieux, la mise à disposition d'outils de développement de logiciels ou encore de capacités matérielles, voire des prestations d'ingénierie sociale destinées à commettre des arnaques. S'agissant des offres « grand public », la qualité croissante des produits proposés et le niveau d'auto régulation de ce marché parallèle sont soulignés : dans ce business trouble comme sur l'Internet « normal », la confiance est nécessaire pour faire des affaires…
En conclusion, l'auteur rappelle que si les grandes firmes peuvent s'offrir des systèmes de protection de bon niveau, la situation des petites et moyennes entreprises est souvent précaire en termes de sécurité informatique et de protection contre la cybercriminalité, quelque forme qu'elle puisse revêtir.

http://knowledge.insead.edu/blog/insead-blog/the-professionalisation-of-cyber-criminals-4626

### *132-16-EN-18* COMPLICITÉ CHEZ LES OPÉRATEURS TÉLÉCOMS EN MATIÈRE DE CYBERCRIMINALITÉ (SEPTEMBRE)

Dans un rapport publié en août 2016 et intitulé « Threat intelligence report for the telecommunications industry », Kaspersky détaille, outre celles visant les abonnés, les 4 principales menaces qui visent les opérateurs de télécommunications et fournisseurs d'accès à Internet (FAI) : les attaques en déni de service distribué (en hausse), l'exploitation de failles dans leur réseau et les terminaux clients, la compromission d'abonnés (par

ingénierie sociale, phishing ou malware) et, enfin, le recrutement de personnes capables d'aider les cybercriminels au sein de l'entreprise.
Sur ce dernier point, l'anticipation est compliquée et les motivations sont diverses : appât du gain, mécontentement, coercition (menace ou chantage) ou tout simplement négligence. Dans son rapport, Kaspersky estime que cette menace est en progression et que les conséquences sont d'autant plus graves qu'elles peuvent concerner des données de haute valeur.

http://www.lemondeinformatique.fr/actualites/lire-les-pirates-recrutent-des-complices-chez-les-operateurs-telecoms-65709.html
https://securelist.com/analysis/publications/75846/threat-intelligence-report-for-the-telecommunications-industry/

### *132-16-EN-19* DÉTECTION D'UNE VULNÉRABILITÉ DANS L'APPLICATION WAZE (MAI)

Waze est une application mobile spécialisée dans la navigation par GPS et fonctionne de façon communautaire, les utilisateurs s'informant les uns les autres quand un événement particulier survient sur la voie publique (accident, bouchon, police, danger…). En s'intéressant à cette application, une équipe de chercheurs en sécurité informatique de l'université californienne de Santa Barbara a constaté une faille dans le système de sécurité. Ces chercheurs ont en effet découvert le moyen d'interférer dans les communications entre utilisateurs de smartphone et serveurs de Waze, puis de créer un programme leur permettant de suivre en temps réel n'importe quel usager. Pour le démontrer, ils ont suivi durant trois jours les déplacements d'une journaliste américaine, y compris lorsqu'elle empruntait les transports en commun ou prenait un taxi. Les seuls instants où la filature numérique a fait défaut furent ceux des trajets en métro, à cause de la perte du signal. Pour parvenir à ce résultat, les experts ont dû se placer sur la trajectoire de la liaison entre le smartphone de l'utilisatrice et les serveurs de Waze. Malgré l'existence d'une connexion sécurisée, les chercheurs sont quand même parvenus à analyser les données transitant d'un point à l'autre et ainsi connaître avec précision les déplacements de la journaliste. Les chercheurs indiquent que cette faille n'est pas propre à Waze et que l'ensemble des services de cartographie et de navigation sont vulnérables.
Les utilisateurs peuvent cependant contourner cette vulnérabilité en activant le mode invisible. Il est rappelé que l'activation du mode invisible est nécessaire à chaque fois que Waze est relancé, l'option se désactivant quand l'application est fermée.

http://www.zone-numerique.com/waze-application-communautaire-cartographie-hacker-faille-conduite.html

### *132-16-EN-20* DANGER DES BORNES DE RECHARGEMENT USB (JUIN)

Selon les experts de Kaspersky Lab, qui ont d'ailleurs mené l'expérience à l'aide d'un PC, d'un câble micro USB standard et de commandes spéciales, il est possible d'infecter un

téléphone mobile avec un malware alors qu'il est connecté en USB sur un ordinateur ou en recharge, et encore plus sûrement s'il est en charge sur des bornes publiques.
Ce phénomène, déjà observé par le passé, est possible du fait que l'appareil ainsi branché transfère à l'extérieur une importante quantité de données, notamment son nom, son fabricant, son type, son numéro de série, des indications concernant son firmware et son système d'exploitation, son système de fichiers et la liste de ses fichiers ou encore l'identifiant de sa puce électronique. L'utilisateur court ainsi le risque de se faire pister et de voir son téléphone chargé avec un logiciel malveillant notamment de type adware (logiciel publicitaire) ou ransomware (rançongiciel).

http://www.itrnews.com/articles/163290/bornes-rechargement-usb-publiques-aussi-deviennent-menace-potentielle.html?key=c7da54689a4c6637

### *132-16-EN-21* LA CROISSANCE DU NOMBRE DE MALWARES INQUIÈTE L'ITALIE (FÉVRIER)

Selon un rapport mensuel de la société Check Point Software Technologies, le nombre de malwares détectés a augmenté de près de 17% en décembre 2015 en Italie. Cette augmentation fait du pays le quatrième plus touché par la menace en Europe, après le Monténégro, la Pologne et la Grèce.
Le malware « Conficker » est le plus répandu sur les ordinateurs. En décembre, il était responsable d'un quart des attaques recensées. Le malware « Xinyin » est devenu de son côté un best-seller sur smartphone.
Si l'augmentation de la menace affecte le monde entier, l'Italie a des raisons de s'en inquiéter. Elle est le 53ème pays le plus touché à l'échelle mondiale. Le rapport révèle que les techniques de détournement des machines par le biais de ces malwares ont elles aussi beaucoup évolué. Elles sont en effet capables de désactiver les systèmes de sécurité des machines pour en prendre plus facilement le contrôle.
L'Italie se montre donc fragile face à de telles menaces, ce qui appelle à une réaction rapide.

http://www.repubblica.it/tecnologia/sicurezza/2016/02/05/news/malware_crescita_inarrestabile_17_a_dicembre-132773886/

### *132-16-EN-22* L'AUTHENTIFICATION EN DEUX ÉTAPES PAR SMS : UNE OPÉRATION À RISQUE (SEPTEMBRE)

L'authentification en deux étapes par SMS est une méthode qui consiste à sécuriser des opérations importantes tels que les paiements en ligne par carte bancaire ou la connexion à un compte (Facebook, Google, Twitter, etc.). Concrètement, au moment de payer un achat en ligne ou d'authentifier un compte, l'utilisateur reçoit un SMS contenant un code à usage unique et doit alors saisir ces chiffres sur la page Internet pour finaliser son opération. L'objectif est de vérifier que l'utilisateur est bien le titulaire de la carte bancaire utilisée ou le propriétaire du compte et non un usurpateur.

Ce processus n'est pas sans risque selon l'Institut national américain des normes et de la technologie (NIST). Des pirates peuvent, en effet, rediriger l'envoi du SMS vers un autre téléphone par le biais d'un logiciel malveillant préalablement installé sur le téléphone des victimes. Ils peuvent également avoir recours à l'usurpation d'identité des usagers en se faisant passer pour eux auprès de leur opérateur pour demander une réémission de la carte SIM et intercepter les SMS.
Pour se prémunir, le NIST recommande l'envoi des codes dans des applications sécurisées comme Authenticator, l'outil de Google qui demande de saisir son mot de passe habituel ainsi qu'un code temporaire généré directement par l'application.
Concernant plus particulièrement les paiements en ligne, l'Observatoire de la sécurité des cartes de paiement, dans son rapport de 2015 publié le 1er juillet 2016, incite les opérateurs téléphoniques à améliorer le processus de réémission des cartes SIM et notamment l'identification des usagers. En outre, il pousse les banques à chercher d'autres alternatives à l'instar de BNP Paribas avec sa « clé digitale » qui permet de sécuriser les opérations sensibles (paiement, ajout de bénéficiaires de virement, etc.) sans avoir recours au SMS.

http://www.lemonde.fr/pixels/article/2016/07/29/une-agence-americaine-deconseille-le-recours-a-l-authentification-en-deux-etapes-par-sms_4976136_4408996.html
http://www.cbanque.com/actu/58893/le-code-sms-point-faible-de-la-securite-des-paiements-en-ligne
http://www.cbanque.com/actu/59391/carte-bancaire-3d-secure-dangereux-pour-les-utilisateurs
http://www.cbanque.com/actu/58032/bnp-paribas-une-cle-digitale-pour-des-virements-plus-surs

### *132-16-EN-23* PIRATAGE DU SITE DU CENTRE D'IDENTIFICATION DES MATÉRIELS DE LA DÉFENSE (MARS)

Le Centre d'Identification des Matériels de la Défense (CIMD) est une structure chargée de la nomenclature des matériels de défense selon les normes OTAN. Autrement dit, il établit une liste de critères de qualité pour les entreprises concourant aux marchés de la Défense. Cette mission l'oblige alors à être en contact avec des sous-traitants, prestataires et fournisseurs et à détenir des informations sur ceux-ci.
Malgré sa discrétion, son site Internet a subi, le 22 février 2016, une attaque informatique d'un collectif se prétendant d'Anonymous. Les documents volés, comportant quelque 10 000 lignes de textes, ont été ensuite publiés sur un site de partage de données. Ils divulguent notamment les coordonnées (noms, numéros de téléphone, adresses e-mail) de personnes travaillant pour la Défense à l'instar de quelque trois cents employés de Thalès. Des informations relatives au serveur du CIMD avec des adresses IP internes, des identifiants et des mots de passe sont également dévoilées.
Les assaillants affirment agir de la sorte pour protester contre la prolongation de l'état d'urgence et les ventes d'armes dans le monde, notamment celles de la France à l'Arabie Saoudite.
Les données extraites et divulguées pourraient faire l'objet, à plus ou moins long terme, d'utilisations malveillantes. Les employés ayant des relations avec la Défense pourraient

faire l'objet eux-aussi d'attaques informatiques.
Pour autant, cet événement n'est pas isolé puisque le site de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) et celui du ministère de la Défense sont des cibles régulières de cyberattaques.

http://www.lefigaro.fr/secteur/high-tech/2016/02/23/32001-20160223ARTFIG00282-anonymous-pirate-une-base-de-donnees-du-ministere-de-la-defense.php
http://www.lesechos.fr/tech-medias/hightech/021718335427-anonymous-publie-des-informations-confidentielles-sur-des-clients-de-larmee-francaise-1202369.php

### *132-16-EN-24* LES HACKERS S'EN PRENNENT TOUJOURS PLUS AUX HÔPITAUX (MARS)

Les cyberattaques visant les hôpitaux se sont multipliées depuis plusieurs mois. En Californie, un centre médical d'Hollywood a été victime d'un *ransomware*, un logiciel de racket neutralisant à la fois les réseaux et les ordinateurs. Le logiciel Locky a réussi à bloquer totalement le système informatique de l'hôpital. Afin d'envisager un retour à la normale, les pirates ont rapidement exigé la remise d'une rançon de près de 9000 bitcoins, soit l'équivalent de 3,5 millions de dollars.
De tels programmes sont aujourd'hui devenus de plus en plus courants et prennent le contrôle d'un ordinateur en en verrouillant l'accès aux fichiers et programmes. Ce type d'action pousse les établissements de santé à un retour provisoire vers des procédures simplifiées (papier, retour du fax…). Certains patients se retrouvent transférés dans d'autres hôpitaux afin de ne pas voir leur santé mise en péril.
En l'espèce, c'est après plus d'une semaine de paralysie que le centre médical hollywoodien a fini par céder et payer une rançon de 17000 dollars, bien loin de la requête initiale des pirates.
Mais le phénomène affecte également les hôpitaux français. En avril 2015, c'est un laboratoire d'analyse qui avait fait l'objet du même type d'attaque. Cependant, l'entreprise avait réussi à désactiver les accès les plus touchés et n'avait pas versé de rançon.
Or une grande partie des données soumises au chantage, essentiellement des dossiers de patients, avait par la suite été diffusée sur le « Dark Web ».
Peu après, c'est le ministère français des Transports qui était victime du procédé.
Désormais, ce type de virus se transmet le plus couramment par le biais de pièces jointes, de fenêtres pop-up, des espaces de stockage dématérialisés…, mais une simple navigation sur Internet peut suffire à déclencher l'infection, d'autant plus que les solutions antivirus ont du mal à détecter certains de ces *ransomware*.
Les sociétés de cybersécurité développent actuellement des « rançongiciels » destinés à surveiller les activités informatiques et à détecter les actions de base des programmes de verrouillage. Les développeurs recommandent avant tout d'effectuer des sauvegardes régulières.

http://www.lemonde.fr/pixels/article/2016/02/16/un-hopital-americain-paralyse-par-des-pirates-informatiques_4866243_4408996.html
http://www.lefigaro.fr/secteur/high-tech/2016/02/16/32001-20160216ARTFIG00205-un-

hopital-americain-paralyse-par-des-pirates-informatiques.php
http://www.lemonde.fr/pixels/article/2016/02/24/des-hopitaux-francais-eux-aussi-victimes-de-chantage-informatique_4870885_4408996.html

### *132-16-EN-25* NOUVEAU RANSOMWARE « PETYA » (AVRIL)

En 2015, l 'éditeur de solutions de sécurité Symantec a constaté un doublement des attaques utilisant les rançongiciels. Ces programmes malveillants prennent en otage des données numériques présentes dans le disque dur de l'ordinateur puis sont « libérées » moyennant rançon. Ils prennent ainsi le contrôle des ordinateurs, des tablettes et des smartphones à distance. Ces pirates du web utilisent ces logiciels pour crypter et rendre inaccessible le contenu des fichiers personnels ou confidentiels des internautes. Menacées alors de destruction totale de leurs données, les victimes s'acquittent généralement d'une rançon en passant par un dispositif de paiement en ligne. Les méthodes employées ont considérablement évolué comme le démontre le nouveau rançongiciel « Petya ». Petya s'est répandu via une série de courriels rédigés en allemand et émanant d'un chercheur d'emploi qui envoie aux départements des ressources humaines des entreprises son CV à télécharger sur Dropbox, un service gratuit de stockage et de partage de fichiers en ligne. Ce logiciel s'attaque aux zones de démarrage des disques durs puis à la Master File Table (MFT), la table de fichiers principale qui contient toutes les informations des fichiers stockés sur le disque dur. Des instructions vous expliquent ensuite comment procéder au paiement d'une rançon d'environ 370 euros à convertir en Bitcoin. Elle devra être versée via une adresse cachée sur le réseau anonyme TOR sous sept jours, après quoi son montant sera doublé. Selon les experts en cyber-sécurité, il est impossible de récupérer ses données sans payer. Face à cette menace, il est recommandé :

-de ne jamais ouvrir de fichier attaché ou de lien hypertexte dans un courriel dont on ne connaît pas l'expéditeur ;

- de posséder un antivirus mis à jour régulièrement ;

- de pratiquer des sauvegardes régulières des données et de les stocker sur un support indépendant ;

- consulter régulièrement le site CERT-FR (ANSSI) pour se tenir informé des menaces existantes.

Des chercheurs en sécurité informatique sont parvenus à casser la clé de chiffrement utilisée par Petya. Les fichiers sont en fait encodés en Base64, et le chiffrement peut facilement être inversé. Afin de rendre la trouvaille accessible à n'importe qui, le chercheur Fabian Wosar a développé le logiciel Petya Extractor.

http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/securite-petya-redoutable-rancongiciel-prend-disques-durs-otage-62229/
http://www.cnetfrance.fr/news/petya-extractor-la-solution-pour-vous-liberer-du-ransomware-petya-39835486.htm

### *132-16-EN-26* TRÈS POPULAIRE AUX ÉTATS-UNIS, L'APPLICATION CANADIENNE KIK OFFRE L'ANONYMAT POUR LES ADOLESCENTS ET LEURS PRÉDATEURS… (FÉVRIER)

L'application KIK, qui annonce 275 millions d'abonnés dont 70 % d'Américains, est utilisée par de nombreux délinquants qui prennent pour cible les adolescents. Aux États-Unis, 40 % des adolescents, d'après KIK, utiliseraient cette application. Ce qui les attire c'est non seulement sa gratuité mais également l'anonymat que KIK garantit. Si l'application demande des éléments d'identification, rien n'empêche l'utilisateur de s'inscrire sous un pseudo. Il peut alors rentrer en communication avec d'autres utilisateurs et échanger des documents de tout type. Ce qui attire les adolescents attire également leurs prédateurs dans cet espace virtuel.
Les forces de police américaines sont particulièrement inquiètes, le nombre de faits d'extorsion, de chantages et de diffusion d'images pédopornographiques étant importants. Il existe par ailleurs certains faits d'enlèvement et d'atteintes physiques sur des adolescents.
L'étude des faits constatés permet de mettre en évidence que les adolescents qui se laissent piéger par un prédateur sont dans la très grande majorité des cas socialement isolés ou en situation de fragilité du fait d'événements familiaux ou de difficultés scolaires. Les prédateurs détectent et profitent de ces faiblesses pour, sous une fausse identité et un profil inventé, manipuler leur victime en obtenant d'elle ce qu'ils souhaitent.
Le système d'anonymisation peut être levé partiellement pour les forces de sécurité afin qu'elles puissent avoir accès à certaines données. Mais la politique de gestion des données ne permet pas d'accéder à l'ensemble de celles-ci, nombre d'entre elles sont en effet effacées. Par ailleurs, pour les forces de police américaines, le fait que le siège social de KIK se trouve au Canada est un obstacle de plus dans la course contre la montre qui est engagée dans le cadre d'investigations pour rechercher une jeune victime notamment.

*NDR : Ce cas pratique, présenté dans un média américain, met en évidence toute la problématique, côté victime, des médias sociaux accessibles sans contrainte d'identité ou de contrepartie financière aux mineurs. Côté opérateur et applications, ce cas met en évidence les contraintes d'une gestion des données qui se veut sans traces.*

http://www.nytimes.com/2016/02/06/us/social-media-apps-anonymous-kik-crime.html

### *132-16-EN-27* ABUS SEXUELS D'ENFANTS EN DIRECT SUR INTERNET EN HAUSSE SELON INTERPOL (OCTOBRE)

C'est sur le darknet, partie obscure d'Internet chiffrée, non référencée dans les moteurs de recherche classiques et offrant un degré d'anonymat élevé à ses utilisateurs, que se déroulent les activités les plus illégales. Le constat est alarmant. Dans le rapport annuel d'Interpol sur l'évaluation de la menace du cybercrime organisé sorti fin septembre 2016, « la maltraitance d'enfant en direct à distance est une menace grandissante ». Ce genre de crime diffusé de manière continue implique un agresseur « dirigeant l'abus en direct à un moment pré-établi à travers des plateformes de partage vidéo ». Il peut être « adapté aux

exigences du ou des criminel(s) solliciteur(s) et enregistré ». Les enfants vulnérables sont de plus en plus victimes des prédateurs sexuels. Initialement davantage localisé en Asie du Sud-Est, particulièrement aux Philippines, ce phénomène d'abus d'enfants en direct s'étend à d'autres pays. Selon Europol, qui ne cite pas de pays en particulier, les malfaiteurs ciblent les régions du monde « aux niveaux élevés de pauvreté, aux mesures de protection des mineurs limitées et au contact aisé avec les enfants ». Une série de vidéos d'information concernant les dangers de l'abus sexuel en ligne devraient bientôt être diffusées dans des écoles de plusieurs pays européens.

https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016
http://www.sudouest.fr/2016/09/28/cybercriminalite-l-abus-sexuel-d-enfant-sur-internet-est-en-hausse-2516632-4697.php

### *132-16-EN-28* REVENGE PORN, UN PHÉNOMÈNE MIEUX CONNU (JUIN)

Le site The daily beast a mis en ligne le 18 juin 2016 un article appelant les victimes de « pornographie non-consensuelle » (nonconsensual pornography) à ne pas sombrer dans des idées mortifères. Alors qu'une étude de 2013 menée par le CCRI (Cyber Civil Rights Initiative) montrait que 51% des victimes de ce type de harcèlement avaient pensé à se suicider et que 3% d'entre elles avaient été jusqu'à changer de nom, un numéro d'appel national a été mis en place aux États-Unis pour aider les victimes à passer cette épreuve difficile. Le rédacteur de l'article rappelle que le fait de mettre en ligne des images dénudées sans le consentement de la personne est désormais poursuivi par la loi dans 34 États ainsi que dans le district de Washington. Par ailleurs, selon l'âge de la victime, les auteurs tombent sous le coup des lois anti pédopornographie. Chez les plus jeunes victimes, pourtant, la perspective de porter plainte et de permettre la condamnation de leur bourreau ne parvient souvent pas à atténuer le choc subi et les cas de suicide continuent à se multiplier.
Cet article est l'occasion de rappeler qu'il est extrêmement imprudent de laisser un tiers prendre des photos de soi dans des situations embarrassantes et qu'il est illusoire de penser que jamais ce type de cliché ne se retrouvera sur Internet. Outre la vie privée, c'est également la vie professionnelle qui se trouve potentiellement affectée à la suite de ces violences commises par support numérique interposé…

http://www.thedailybeast.com/articles/2016/06/18/dear-revenge-porn-victims-it-gets-better.html

### *132-16-EN-29* L'APPLICATION GOSSIP DANS LE VISEUR DE LA CNIL (NOVEMBRE)

Le 26 septembre 2016, la Commission Nationale de l'Informatique et des Libertés (CNIL) a mis en demeure l'entreprise W.M.G, qui édite l'application « Gossip, les potins anonymes »,

de se conformer à la loi dans un délai d'un mois.
Cette application a vu le jour en mai 2015. Elle permet de partager des rumeurs de manière anonyme sous la forme de texte, de photo ou de vidéo. Chacune de ces rumeurs est associée à un contact et toute personne possédant ce contact dans son répertoire ou sur Facebook peut recevoir le « ragot ». Ainsi, il est possible de voir une image avec pour commentaire « [prénom, nom de famille] au moment de son viol » ou de lire « M. [nom de famille] professeur au lycée [nom de lycée, ville et code postal] est un pédophile ».
La CNIL a relevé deux manquements à la loi informatique et liberté. Sur le fond, une personne qui n'a pas l'application peut être victime d'une rumeur sans pour autant en être informée. Gossip n'est donc pas conforme avec l'article 1er de la loi informatique et libertés qui dispose que l'informatique « ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».
Quant à la forme, la collecte des numéros de téléphone ne repose sur aucune base légale. En effet, l'application puise dans le répertoire de ses utilisateurs, y compris des informations de personnes ne disposant pas de Gossip et en l'absence de leur consentement.
W.M.G a désormais le choix entre la mise en conformité de son application ou l'enclenchement d'une véritable procédure de sanction.

https://www.cnil.fr/sites/default/files/atoms/files/d2016-079_med_w.m.g.pdf
http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/harcelement-la-cnil-met-en-demeure-l-appli-gossip-14-10-2016-2076019_506.php
http://www.lemonde.fr/pixels/article/2016/10/14/la-cnil-met-en-demeure-l-application-de-rumeurs-gossip-de-se-conformer-a-la-loi_5013951_4408996.html

### *132-16-EN-30* UNE APPLICATION ANTISÉMITE SUPPRIMÉE PAR GOOGLE PLAY (JUIN)

Créée par Alternative Right, un groupe d'extrême droite américain, l'application « the Coincidence Detector », téléchargeable depuis Google Play, avait pour le moins une description évasive « Aider à détecter les coïncidences des personnes qui sont impliquées dans les sphères politico-médiatiques ». Autrement dit, il s'agissait de pourchasser les patronymes juifs sur Internet. Les internautes pouvaient s'en servir soit pour identifier des personnalités juives déjà préenregistrées dans le catalogue, soit pour ajouter de nouveaux patronymes dans la base. Près de 9000 Juifs ont ainsi été reconnus.
Pour ce faire, il y avait un code à respecter : (((écho))). La triple parenthèse était déjà utilisée par un autre groupe néonazi, the Right Stuff, qui affirmait que les parenthèses représentaient « la destruction de la famille par les Juifs, leur pouvoir dans le monde, et la subversion du foyer national ». Ainsi, Michael Blommberg, ex-maire de New-York, a vu son nom changé par (((Bloomberg))).
Notée 5 étoiles sur 5 par les internautes, l'application « the Coincidence Detector » n'a été supprimée que récemment par Google Play.
Cette application n'est pas la première du genre. Déjà en 2011, l'application pour Iphone et Ipad « Juif ou pas Juif » permettait d'interroger une base de données avec des noms d'origine juive. Les associations anti-racistes ont abandonné leur action en justice après le retrait dans le monde entier de l'application.

http://www.lepoint.fr/high-tech-internet/cette-application-qui-traque-les-juifs-sur-internet-13-06-2016-2046280_47.php
http://www.atlantico.fr/pepites/etats-unis-groupe-neonazi-cree-application-pour-traquer-juifs-internet-2732346.html#oI1GZsX6E8Vcxwp6.99
http://www.lemonde.fr/technologies/article/2011/10/27/iphone-l-application-juif-ou-pas-juif-devant-la-justice_1595333_651865.html
http://www.lefigaro.fr/secteur/high-tech/2011/11/24/01007-20111124ARTFIG00493-l-appli-juif-ou-pas-juif-retiree-dans-le-monde-entier.php

### *132-16-EN-31* PROTECTION DE LA VIE PRIVÉE ET CRYPTAGE DES DONNÉES (FÉVRIER)

Le site « Presse-citron », dans un article mis en ligne le 10 février 2016, rapporte que l'opérateur de messagerie Gmail qui crypte les messages pendant leur transit souhaite pousser les autres opérateurs à agir de même. Les utilisateurs d'un compte Gmail pourront ainsi être informés, via une fenêtre qui s'ouvrira en cliquant sur une icône rouge, que le service qui reçoit le message ne met pas en œuvre de mesure de chiffrement. Dans ce cas, il est suggéré à l'utilisateur de ne pas envoyer de données sensibles à cette adresse, voire de la supprimer carrément de sa liste d'adresses ! De la même manière, les messages reçus via des opérateurs « non sécurisés » seront également marqués, dans une optique similaire (un point d'interrogation rouge apparaîtra devant le nom de l'envoyeur). La démarche de Gmail illustre la question de la protection de la vie privée et des données, entre démarche de chiffrement que certains souhaitent obligatoire et approche récalcitrante de certains services qui voient dans le chiffrement une atteinte portée à l'efficacité des enquêtes. Ces interrogations ont, de fait, constitué la ligne rouge du dernier FIC qui s'est tenu les 25 et 26 janvier 2016 à Lille.

http://www.presse-citron.net/gmail-veut-forcer-ses-concurrents-a-adopter-le-chiffrement/

### *132-16-EN-32* LE FBI PIRATE LE DARK WEB POUR DÉBUSQUER DES PÉDOPHILES (MARS)

Ils pensaient que leur identité était protégée grâce au réseau d'anonymisation TOR. Et pourtant, en piratant leurs ordinateurs lors d'une opération de grande ampleur, de nombreux internautes amateurs de pédopornographie ont été piégés par le FBI. Tous naviguaient sur Playpen (en référence au parc pour bébé éponyme), un site de partage et de téléchargement d'images pédopornographiques uniquement accessible à travers TOR. Un mois après son lancement en août 2014, le site comptait déjà 60 000 membres et jusqu'à 215 000 l'année suivante, avec une moyenne de 11 000 visiteurs uniques chaque semaine et un total de 117 000 posts. La plupart de ces posts contenaient des images pédophiles d'une extrême violence, d'autres proposaient des conseils pour les agresseurs sexuels afin d'utiliser Internet sans se faire repérer. Le FBI a mis la main sur le serveur hébergeant ce site en février 2015. Au lieu de le mettre hors service, les autorités ont maintenu le site en

ligne et du 20 février au 4 mars 2015, l'ont hébergé sur leurs propres ordinateurs. L'introduction d'un « malware » sur le site infectant les ordinateurs des membres qui s'y connectent a permis au FBI de repérer leur adresse IP.
Grâce à cet outil de piratage appelé « NIT » (Network Investigative Technique), 1 300 adresses IP ont pu être ainsi collectées, permettant l'identification des visiteurs et menant à 137 inculpations.

http://www.journaldugeek.com/2016/01/08/fbi-pirate-deep-web-pedophiles/
http://rue89.nouvelobs.com/2016/01/07/quand-fbi-pirate-millier-dordis-262744

### *132-16-EN-33* L'INTERNET DES OBJETS, OUTIL AU SERVICE DES GOUVERNEMENTS (FÉVRIER)

Le directeur national du renseignement américain a déclaré devant deux comités du Sénat américain qu'il estime que l'Internet des objets (Internet of Things ou IoT) peut constituer un moyen pour des gouvernements d'accéder à des informations de façon détournée ou, en clair, de faire de l'espionnage. Selon lui, les appareils connectés comme les smart grids, les véhicules, les applications domotiques constituent des portes d'accès permettant, si l'on s'en donne les moyens, de recueillir des données personnelles. Il estime ainsi que, « dans le futur, les services de renseignement pourraient utiliser l'IoT pour effectuer de l'identification, de la surveillance, du suivi, de la géolocalisation, du ciblage en vue d'un recrutement ou pour accéder à des réseaux ou aux identifiants d'utilisateurs ».
Les objets connectés constituent déjà des éléments importants pour la collecte de preuves dans un contexte judiciaire. Ce dont il est ici question est en revanche différent puisque l'utilisation envisagée s'effectuerait évidemment en dehors d'un cadre judiciaire. Plus que jamais, cette déclaration vient souligner que, si les objets connectés constituent des éléments concourant au confort et à la sécurité de leurs utilisateurs, il ne faut pas oublier qu'ils offrent dans le même temps des opportunités nouvelles à tous ceux qui cherchent à rassembler des informations sur telle personne, tel groupe d'individus ou telle société commerciale.

http://arstechnica.com/tech-policy/2016/02/us-intelligence-chief-says-iot-climate-change-add-to-global-instability/

### *132-16-EN-34* SOUS LES PAVÉS NUMÉRIQUES, LA PLAGE, VRAIMENT ?… (NOVEMBRE)

Les manifestants autour d'un projet de pipeline dans une réserve du Dakota du Nord (États-Unis) ont découvert que la police utilisait Facebook pour surveiller les évolutions du mouvement. La police se servait notamment de la géolocalisation des comptes pour avoir une idée des effectifs des manifestants. Pour contrer cette utilisation particulière du réseau social, les organisateurs ont demandé aux abonnés de montrer leur solidarité en se géolocalisant sur le site, qu'ils soient effectivement présents ou non. Leur objectif est de saturer de données la police afin de l'empêcher d'avoir une idée claire du nombre de

personnes présentes et de leur identité.
Cette décision est révélatrice d'une part d'une utilisation croissante des réseaux sociaux par des services de police pour essayer de comprendre les ressorts d'un mouvement contestataire, d'autre part de la prise de conscience des activistes d'une éventuelle vulnérabilité liée à leur usage. Si les réseaux sociaux offrent effectivement des possibilités intéressantes en termes de mobilisation des foules (diffusion de messages, de lieux et d'horaires de rendez-vous, de consignes…), ils permettent en contrepartie d'observer un certain nombre de choses, en raison même de leur utilisation parfois intrusive des données personnelles et des capacités de géolocalisation des appareils portables.

http://www.numerama.com/politique/205761-ils-se-geolocalisent-dans-les-manifestations-pour-troubler-les-outils-de-surveillance.html?utm_content=buffera7b11&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

### *132-16-EN-35* L'ARME FATALE CONTRE LA FRAUDE (JUIN)

Le site Presse-citron.net rapporte le 20 juin 2016 que les autorités algériennes ont choisi de prendre à bras-le-corps le problème de la tricherie aux examens via les réseaux sociaux. Alors que des fuites sur ces réseaux contraignent des milliers de candidats au bac à plancher à nouveau, l'accès à Facebook, Twitter et autres réseaux sociaux a été momentanément coupé. Bien entendu, cette restriction touche l'ensemble des internautes du pays, pas les seuls candidats au baccalauréat…
Cet exemple extrême illustre, d'une part, l'omniprésence des réseaux sociaux dans nos sociétés et d'autre part, les difficultés rencontrées pour éviter des phénomènes délinquants de grande ampleur. La diversité des moyens permettant d'accéder au Web (montres connectées et autres appareils de petite taille) rend la tâche de contrôle du déroulement des examens de plus en plus complexe.

http://www.presse-citron.net/lalgerie-bloque-facebook-et-twitter-durant-les-epreuves-du-bac/

### *132-16-EN-36* LENTILLES DE CONTACT CAMÉRAS (MAI)

Le site *the daily beast* publie le 14 mai 2016 un article relatant le dépôt par les firmes Sony et Google de brevets relatifs à des caméras directement liées à l'œil, soit par le biais d'une lentille de contact, soit par l'implant d'une caméra dans l'œil. La première est censée être pilotée par des clignements d'œil effectués selon des combinaisons particulières. S'agissant de la seconde, la firme américaine semble prévoir qu'elle puisse être connectée, géolocalisée et dotée d'une puce NFC, anticipant donc l'utilisation des données recueillies par des services en ligne. Le rédacteur de l'article rappelle la réaction épidermique qui avait secoué le public lorsque Google avait sorti ses lunettes connectées : après de nombreux cas de brutalités exercées contre des porteurs de *Googleglasses* par des quidams souhaitant éviter de figurer sur des vidéos tournées à leur insu, le produit avait été abandonné. Dans le cas des yeux directement équipés, le journaliste pose des questions

très pertinentes : comment savoir si la personne en face de vous est en train de vous filmer ? Comment, pour les forces de l'ordre ou les organisateurs de spectacle, empêcher le public de filmer alors qu'il n'en a pas le droit ? Ces systèmes ne vont-ils pas engendrer une paranoïa collective ? Enfin, les données émises par ces caméras très intimes ne risquent-elles pas d'échapper à leur propriétaires pour être exploitées par d'autres ? « Si c'est gratuit, c'est que vous êtes le produit », a-t-on coutume de dire s'agissant des services en lignes gratuits. En la matière, Google (parmi d'autres) s'est fait spécialiste et il est fort probable que les caméras oculaires participent à la grande collecte générale de données privées.

http://www.thedailybeast.com/articles/2016/05/14/google-wants-to-put-a-camera-in-your-eye.html

### *132-16-EN-37* « MAISON CONNECTÉE » : UN NOUVEAU DISPOSITIF DE PROTECTION DE SON HABITAT À DISTANCE (MAI)

Sept Français sur dix ont été cambriolés au moins une fois dans leur vie (enquête « Cadre de vie et sécurité » de INSEE en 2007), un incendie a lieu toutes les deux minutes et un cambriolage toutes les 90 secondes (Bulletin 2012 de l'ONDRP, janvier 2013).
Dans une optique de prévention de ces drames, le groupe MACIF et IMA Protect (société de télésurveillance) présentent leur « maison connectée » par le biais de la nouvelle gamme « Macif Protect ». L'objectif affiché est de mieux protéger son logement par l'utilisation d'objets connectés. Il est vrai que le groupe AXA a déjà présenté un produit similaire en 2015 mais dans une approche différente puisqu'AXA propose un service d'assistance en complément de l'offre de centrale d'alarme proposée par MyFox. À l'inverse, la MACIF est le concepteur de l'offre.
L'abonnement de base est à 12€ par mois mais pour ce prix, il ne comprend pas l'achat du matériel (149€) qui se compose d'une centrale d'alarme, d'un détecteur de fumée, d'un détecteur d'intrusion, d'un détecteur d'ouverture de porte et d'un clavier de commande pour activer ou désactiver l'alarme.
Tous ces objets sont connectés au smartphone du client via une application mobile. Autrement dit, en cas de feux ou d'intrusion par exemple, un appel est passé au propriétaire des lieux qui pourra lui-même contacter les numéros utiles. S'il ne répond pas, deux autres numéros que l'usager aura préalablement donnés seront contactés.
En contrepartie de l'adhésion, aucune baisse des cotisations d'assurance n'est prévue mais les franchises sur d'éventuels sinistres sont supprimées. Par ailleurs, il est impossible de souscrire à cette offre pour le temps des vacances ou d'un week-end. D'ailleurs, les frais de résiliation de 149 € lors de la première année démontrent bien que le contrat est amené à s'inscrire dans le temps.

http://www.boursorama.com/actualites/quand-la-maison-connectee-sert-a-securiser-son-logement-6375a7a103e250d27608e6c8079c8a75
http://www.lesechos.fr/finance-marches/banque-assurances/021835723082-les-assureurs-entrent-dans-la-maison-connectee-1213329.php
https://www.macif.fr/web/site/offres/accueil/particuliers/telesurveillance

***132-16-EN-38*** **INVENTION D'UNE COQUE IPHONE ANTI-ESPIONNAGE (SEPTEMBRE)**

L'ancien analyste de la NSA, Edward Snowden, a travaillé en collaboration avec le hacker Andrew « bunnie » Huang sur une coque-batterie pour iPhone capable de détecter toute tentative de surveillance à distance. L'objectif est de fournir, notamment aux journalistes ainsi qu'aux activistes, un moyen de se protéger contre une mise sur écoute, un vol de données ou une géolocalisation. L'idée consiste à réaliser une coque de smartphone avec batterie « dans laquelle est inséré un oscilloscope miniature. Le dispositif va alors surveiller en permanence l'activité électrique du circuit utilisé par le modem sans fil et détecter lorsque le modem est utilisé pour écouter ou transmettre des informations alors que le téléphone est censé être en mode avion et ne plus émettre ni recevoir aucune donnée ».

http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/smartphone-edward-snowden-invente-coque-iphone-anti-espionnage-63653/
http://www.atlantico.fr/decryptage/comment-edward-snowden-concoit-prototype-coque-anti-espionnage-pour-iphone-2772496.html

***132-16-EN-39*** **RÉSEAU SOCIAL CITOYEN (AVRIL)**

L'association nationale des auditeurs jeunes de l'IHEDN (ANAJ-IHEDN) a mis en ligne en mars 2016 l'interview des deux fondateurs du réseau social Qwidam. Ce réseau fonctionne sur le principe de l'entraide entre personnes situées dans un proche périmètre. Les membres du réseau ont leur réseau d'amis et peuvent « voir » sur leur smartphone si d'autres membres se trouvent à proximité lorsqu'ils rencontrent un problème. Si les membres sont anonymes (sauf le réseau des amis), ils sont en revanche géolocalisés. L'idée du réseau est de signaler un problème local ou de lancer un message d'appel à assistance qui est diffusé uniquement aux membres se trouvant à proximité de l'appelant. Les membres peuvent lancer un SOS (une demande d'aide immédiate) ou une alerte (mise en garde des autres usagers). Enfin, le réseau s'appuie sur un autre réseau, celui des Volontaires Internationaux en Soutien Opérationnel Virtuel (VISOV).
Interrogés sur le risque pour un membre du réseau d'être mis en cause pour non assistance à personne en danger, les deux fondateurs estiment que celui-ci est quasiment nul du fait que « c'est très compliqué de mettre quelqu'un en cause pour non-assistance à personne en danger car il faut montrer qu'il ait eu connaissance de la situation, qu'il ait été à proximité, qu'il ait eu un visuel direct sur la situation et qu'il ait été en capacité d'agir sans se mettre lui-même en danger ». De même, ils ne pensent pas que le fait d'envoyer un SOS ou une alerte puisse mettre la personne en danger face à d'autres individus qui voudraient profiter de la situation...
Ce type de service participe au mouvement consistant à renforcer la solidarité entre individus. L'interview détaille les notions de *crowdsourcing* (recherche d'information sur les réseaux sociaux), de *crowdchecking* (vérification des informations) et de *crowdmapping (*cartographie établie à partir des informations), autant d'outils qui s'appuient sur une analyse de données en source ouverte, à la limite entre le Big Data et le social engineering.

*NDR : Nous évoquions dans la Revue du CREOGN N°120 d'octobre 2015 (article 120-15-ST-03) une application pour smartphone utilisée sur les campus américains pour lutter contre les agressions.*

http://www.anaj-ihedn.org/WordPress3/wp-content/uploads/2016/03/Qwidam-ANAJ-2016.pdf
http://www.visov.org/

### *132-16-EN-40* LES FOURNISSEURS D'INFRASTRUCTURES CLOUD SE DOTENT D'UN CODE DE BONNE CONDUITE EUROPÉEN (OCTOBRE)

Le 27 septembre 2016, à Bruxelles, l'entreprise française OVH, leader européen et troisième acteur mondial du cloud, a dévoilé un code de bonne conduite relatif à la protection des données. Devançant l'entrée en vigueur, en mai 2018, du Règlement Général sur la protection des données, ce code de conduite, approuvé par plus de 20 fournisseurs européens de services d'infrastructures cloud, s'attache à « maintenir le degré le plus élevé de protection des données ». Conformément aux modalités prévues dans le nouveau Règlement, les hébergeurs de données laissent à leurs clients le contrôle et la propriété de leurs données, tout en garantissant un traitement et un stockage intégral des données en Europe. L'utilisation des données à des fins commerciales est par ailleurs proscrite. Les entreprises qui s'engagent à respecter le code de bonne conduite se verront attribuer un label de conformité.

https://www.ovh.com/fr/news/cp2362.des_fournisseurs_dinfrastructures_cloud_lancent_le_tout_premier_code_de_conduite_europeen_relatif_a_la_protection_des_donnees
http://www.lemonde.fr/economie/article/2016/09/27/en-europe-les-hebergeurs-de-donnees-a-l-offensive_5003970_3234.html

### *132-16-EN-41* PARTENARIAT SUR L'ÉTHIQUE PAR LES GÉANTS DU WEB (OCTOBRE)

Les innovations et progrès en intelligence artificielle (IA) suscitent, sans doute légitimement, quelques craintes. Afin de rassurer la société civile et les gouvernements, les géants du Web, Google, Facebook, IBM, Microsoft et Amazon (Apple n'a pas, pour le moment, donné suite aux sollicitations) ont noué un partenariat à but non lucratif, officialisé fin septembre, en vue, notamment, de définir de bonnes pratiques qui soient respectueuses de l'éthique et de les communiquer en toute transparence et sans activité de lobbying. La note d'intention publiée pour l'occasion confère à l'organisation (qui devrait être constituée à parts égales de représentants des entreprises concernées et de chercheurs, associations et membres de la société civile) une mission « d'éducation aux technologies d'IA » et émet quelques grands principes : garantir la protection de la vie privée et la sécurité des individus, ne pas développer ou utiliser des « technologies d'IA qui violeraient les conventions internationales ou les droits humains ». Cependant, dans l'article du Monde, il est souligné que le problème

n'est pas tant posé par les technologies elles-mêmes que par leur usage. De plus, les engagements pris n'auront pas de valeur contraignante. Néanmoins, cette annonce de partenariat entre les entreprises les plus puissantes du secteur peut être considérée comme un premier pas vers une réflexion commune sur l'impact de l'IA sur notre quotidien et sur l'évolution de l'humanité.

http://www.lemonde.fr/pixels/article/2016/09/28/intelligence-artificielle-les-geants-du-web-lancent-un-partenariat-sur-l-ethique_5005123_4408996.html
http://www.lefigaro.fr/secteur/high-tech/2016/09/29/32001-20160929ARTFIG00153-les-geants-du-web-s-unissent-pour-maitriser-l-intelligence-artificielle.php
http://www.lesechos.fr/idees-debats/sciences-prospective/0211337588119-les-geants-du-net-sengagent-pour-lethique-de-lintelligence-artificielle-2031003.php

***132-16-EN-42*** **RÉALITÉ VIRTUELLE : SERONS-NOUS HEUREUX DANS LA MATRICE ? (MARS)**

La réalité virtuelle devient un enjeu majeur pour les géants du numérique. Cette nouvelle technologie suscitera selon eux un véritable engouement auprès des populations en proposant pour tous un droit au « bonheur par procuration». Les concepteurs voudraient proposer aux communs des mortels de vivre une partie des plus belles expériences jusque-là réservées aux riches grâce aux capacités de synthèse et de réplique qu'offre la réalité virtuelle. Ainsi, une promenade en forêt équatoriale, une visite du château de Versailles, seront à la portée de n'importe quel individu, où qu'il soit sur la planète. Considérée par certains de manière positive comme la prochaine plate-forme sociale, d'autres soulignent un « fantasme dangereux » à l'instar des dérives du transhumanisme. En effet, la frange la plus sensible de la population pourrait être tentée d'évoluer en permanence dans un environnement virtuel avec en corollaire les risques d'addiction en devenir.

*NDR : La réalité virtuelle invite à une réflexion sur l'évolution du lien social et le seuil de résilience des sociétés contemporaines.*

http://www.cnetfrance.fr/news/realite-virtuelle-nous-serons-heureux-dans-la-matrice-39833614.htm

RETOUR


***132-16-EE-01*** **SÉCURITÉ DES DONNÉES EN ENTREPRISE – RAPPORT 2016 DE GEMALTO (AVRIL)**

Alors qu'en 2015, GEMALTO révélait que 53 % des attaques informatiques concernaient les données personnelles, une étude de 2016 annonce que 75% des utilisateurs (deux fois plus que l'année précédente), pensent que les entreprises ne prennent pas au sérieux la question de la sécurité des données, et que 64 % ne feront pas appel à une entreprise ayant subi un vol de données.
L'étude fait particulièrement le point sur les attentes des utilisateurs et les conséquences pour les entreprises victimes de cyberattaques. En effet, confiance et fidélité dépendent des services et des garanties que peuvent offrir les entreprises à leurs clients, d'autant plus que le nombre de comptes en ligne détenus par les individus est important, que les espaces de stockage de données personnelles se multiplient (data centers, cloud…) et que les vies numériques sont de plus en plus nomades.
Finalement, la sécurité des données doit s'adapter aux modes de conservation disponibles (fixes ou mobiles) et les entreprises doivent pouvoir offrir les services de protection adéquats et investir dans des stratégies défensives évolutives et innovantes ; pare-feu, détections d'intrusions et technologies AV (audio et vidéo) et SIEM (Security Information and Event Management) ne sont plus suffisantes. Prévenir autour d'un périmètre en particulier ne doit plus être le seul moyen de défense car les attaques peuvent se produire depuis les objets connectés, dont le nombre est en constante augmentation, et que les environnements à défendre se diversifient.
Si l'enjeu est important pour les utilisateurs, il est fondamental pour les entreprises, car leurs chiffres d'affaires peuvent être impactés par les failles, et des employés (voire des dirigeants) perdre leur emploi.
La confiance numérique devrait monter en puissance, avec la prise de conscience des utilisateurs quant à l'importance de sécuriser leur identité numérique, et celle des entreprises quant à son impact sur leur viabilité.

http://www.infodsi.com/articles/162042/donnees-personnelles-cibles-privilegiees-cyberattaques-2016.html?key=
http://www.gemalto.com/press/Pages/Gemalto-Releases-Findings-of-First-Half-2015-Breach-Level-Index.aspx
http://www.gemalto.com/press/Pages/Global-survey-by-Gemalto-reveals-impact-of-data-breaches-on-customer-loyalty.aspx

RETOUR

## *SANTÉ- ENVIRONNEMENT*


### *132-16-SE-01* APPARITION D'UNE APPLICATION VISANT À PRÉVENIR LES SUICIDES (FÉVRIER)

L'université de Stanford, associée au centre de recherche du Merseycare de Liverpool, a développé une application pour smartphone capable de détecter les intentions suicidaires des individus. L'application se base sur le contenu des écrits laissés sur les réseaux sociaux. Lorsqu'une personne rédige en ligne des phrases détectées comme suspectes, l'application est à même d'alerter les spécialistes de la question.
Combien sont aujourd'hui les cas où, avant de passer à l'acte, des individus ont fait part de leurs intentions sur les réseaux sociaux sans que cela soit nécessairement pris au sérieux ? L'application fonctionne avec les statuts Facebook et Twitter mais remarque également lorsqu'une personne ne se présente pas à un rendez-vous fixé. L'objectif est de prévenir la commission de l'acte extrême.
L'application devant encore faire l'objet de tests, elle sera disponible dans le courant de l'année 2016. Elle tend à devenir un appui précieux en prévenant les personnes en mesure de venir en aide à l'individu en détresse. Le directeur du centre de recherche voit en cette application un potentiel incroyable.
Il ne s'agit pas du premier projet de la sorte. L'université Dartmouth avait déjà développé l'algorithme Durkheim capable d'identifier les mots les plus utilisés dans les cas de suicides. En effet, les chercheurs ont mis en évidence que dans près de 65% de ces cas, les individus avaient auparavant laissé transparaître leurs intentions via les réseaux sociaux.
L'application vise ainsi à devenir un radar dans la prévention des risques de suicides.

http://www.repubblica.it/tecnologia/social-network/2016/02/05/news/arriva_una_app_per_prevenire_i_suicidi-132784088/

### *132-16-SE-02* CRÉATION DE TISSUS HUMAINS AVEC UNE IMPRIMANTE 3D LASER (FÉVRIER)

Créée en 2014 par un ancien chercheur de l'INSERM (Institut National de Santé et de Recherche Médicale) et située près de Bordeaux, la start-up française Poietis (« fabriquer » en grec) a réussi à mettre en œuvre une technologie basée sur une imprimante 3D laser permettant de produire de la peau. Il est vrai qu'il existe déjà des technologies de bio-impression mais l'entreprise Poietis est la seule à utiliser la lumière laser qui a pour considérable avantage une grande précision. La viabilité des cellules est de l'ordre de 95 à 100 %.
Pour l'heure, cette imprimante 3D met en moyenne trois semaines pour créer de la peau et peut même réparer le crâne d'une souris blessée directement sur le sujet.
A court terme, la start-up souhaite se diriger vers la recherche cosmétique et pharmaceutique. Depuis l'interdiction en 2013 des tests sur animaux pour les cosmétiques

dans l'Union européenne, la production de peaux saines et pathologiques par ce procédé peut s'avérer être une bonne alternative. Puis, Poietis envisage de créer, dans une dizaine d'années, des greffons de peau à partir des cellules même du patient.
Cette technologie ne manquera certainement pas de poser des questions éthiques surtout si elle est utilisée non plus à des fins de réparation tissulaire mais d'augmentation ou d'amélioration des tissus.

http://www.sciencesetavenir.fr/sante/20160209.OBS4272/produire-des-tissus-humains-par-imprimante-3d-le-defi-de-poietis.html

### *132-16-SE-03* FACEBOOK UTILISÉ POUR LE COMMERCE ILLÉGAL D'ESPÈCES MENACÉES (MARS)

Nouvelle tendance qui se confirme et dénoncée dans un rapport de l'ONG Traffic publié début mars 2016 : le recours aux portails en ligne et aux réseaux sociaux pour la vente de produits issus d'espèces sauvages menacées (ivoire, cornes, spécimens rares…).
En effet, les trafiquants, agissant via des forums en ligne protégés ou des groupes fermés, sont plus difficilement détectés, peuvent agrandir leur clientèle et utilisent des modes de transaction plus pratiques, proposant même la livraison à domicile et fournissant leurs coordonnées.
La clientèle visée est essentiellement asiatique (Chine, Malaisie,….) car cette région du monde développe ses nouvelles technologies et reste sensible aux médecines traditionnelles, utilisatrices de produits issus des animaux.
Sur 50 heures d'observations de Facebook, 14 groupes créés depuis la Malaisie ont pu être détectés, représentant près de 68 000 utilisateurs et 106 vendeurs.
Il est surtout clair que la lutte doit à présent se moderniser et trouver des solutions innovantes, voire obtenir la collaboration des sites concernés.
Facebook n'a pas commenté cette information mais a fait part à l 'ONG de sa volonté de collaborer et ainsi de mettre fin à ces abus, notamment par la suppression de tout contenu violant les conditions d'utilisation.

http://www.lematin.ch/monde/asie-trafic-propose-facebook/story/30192911

### *132-16-SE-04* FACEBOOK ET BRACONNIERS (NOVEMBRE)

La Wildlife Justice Commission (WJC) a présenté les 14 et 15 novembre 2016, au Palais de la Paix de La Haye, une enquête révélant l'arrestation d'un groupe d'environ 50 braconniers qui auraient utilisé Facebook pour commercer illégalement sur le plan international en vendant des produits interdits provenant d'animaux sauvages. Installés au Vietnam (l'Asie et notamment la Chine abritent le principal marché du braconnage) dans un village ayant déjà abrité des braconniers, ils avaient également utilisé le réseau social chinois WeChat pour leur trafic.
Déclarant vouloir collaborer en supprimant les contenus illicites et contraires aux règles de « la communauté », Facebook est malgré tout utilisé, notamment pour l'organisation

d'enchères illégales.

http://www.numerama.com/politique/208632-facebook-le-reseau-social-prefere-des-braconniers.html
https://wildlifejustice.org/viet-nam-wildlife-crime-investigation-public-hearing-announced/

### *132-16-SE-05* DRONE CONTRE FRELON ASIATIQUE (JUIN)

Fléau pour les campagnes du sud-ouest de la France, mais désormais présent dans les trois-quarts du pays, cet insecte dévore les abeilles autochtones, incapables de se défendre, et met donc en péril l'écosystème par une disparition des insectes pollinisateurs. Or, son éradication est difficile et dangereuse car les nids sont souvent perchés entre 3 et 30 mètres de hauteur.
Aucun outil n'étant adapté, l'entreprise locale LGF (Landes Guêpes et Frelons) qui lutte depuis 5 ans contre cet insecte, a fait appel à la société Drone Volt, leader français des drones, pour concevoir un engin spécialement destiné à la chasse au frelon asiatique : le Spray Hornet. Equipé d'une bombe aérosol remplie de 750 ml de biocide avec jet inclinable, ce dispositif est chargé de pulvériser la partie centrale du nid aux entrées et sorties des insectes de manière très précise afin de les détruire en atteignant le moins possible l'environnement alentour.
Pesant à vide 3,15 kg et d'une autonomie de 9 à 18 minutes (selon qu'il embarque 1 ou 2 batteries), il est également équipé d'un parachute et d'une caméra HD. Son prix est élevé (9900 € HT) mais il engendre un gain important de productivité car la destruction d'un nid passe d'une heure à dix minutes environ.

https://www.expoprotection.com/RISQUES-ENVIRONNEMENTAUX/Article.htm?Zoom=4debb93c14e0bb3f894a74529f5f8a34

### *132-16-SE-06* OPÉRATION PANGEA IX : LUTTE CONTRE LA VENTE ILLICITE DE MÉDICAMENTS SUR INTERNET (JUIN)

L'opération internationale visant à lutter contre la vente illicite de médicaments sur Internet, baptisée Pangea IX, s'est déroulée du 30 mai au 7 juin 2016. Coordonnée par Interpol, en partenariat avec l'Organisation Mondiale des Douanes (OMD), Europol, le Permanent Forum on International Pharmaceutical Crime (PFIPC), le Head of Medecine Agencies Working Group of Enforcement Officers (HMA/WGEO) et soutenue par les industriels du médicament, elle a été suivie dans 103 pays. Elle a donné lieu à 393 arrestations dans le monde et à la saisie de plus de 53 millions de dollars de médicaments potentiellement dangereux.
En France, l'opération Pangea IX a associé les services de police, de gendarmerie, des douanes ainsi que les autorités de régulation et de contrôle compétentes en matière de médicaments et de santé publique, avec également le concours de compagnies privées de l'Internet et de moyens de paiement. Au total, ce sont 961 192 produits de santé illicites et 1 422 kg de produits de santé en vrac qui ont été saisis. Les prises, dont la majorité a été

interceptée à l'aéroport de Roissy dans des valises et des bagages en soute, se composent essentiellement de médicaments sans autorisation de mise sur le marché en France (580 000), de produits de santé contrefaisants (près de 190 000 comprimés) et de médicaments détournés de leur usage et utilisés comme stupéfiants (plus de 30 000 doses). Plus de 77 % des produits saisis provenaient d'Asie (principalement d'Inde pour 64,22 %). 24 enquêtes judiciaires ont été ouvertes par le Service National de Douane Judiciaire (SNDJ), portant sur différents médicaments, produits cosmétiques interdits et substances dopantes. L'opération a permis l'identification de 55 sites Internet illégaux vendant des faux médicaments : 33 ont été identifiés par le service douanier Cyberdouane, dont 28 ont été signalés auprès de l'Association Française pour le Nommage Internet en Coopération (AFNIC) pour des demandes de vérification d'éligibilité. 7 sites sont d'ores et déjà fermés. Les 22 autres sites, identifiés par l'Office Central de Lutte contre les Atteintes à l'Environnement et à la Santé Publique (OCLAESP) et le Service Central du Renseignement Criminel/Division de lutte contre la Cybercriminalité (SCRC/C3N), ont fait l'objet de procédures judiciaires. 6 sites francophones hébergés à l'étranger ont été signalés aux pays concernés pour enquête. On constate également une recrudescence de l'utilisation d'ordonnances falsifiées aux fins d'obtenir des psychotropes, de la morphine ou des substituts de stupéfiants. L'Agence Nationale de Sécurité du Médicament et des produits de santé (ANSM) rappelle aux consommateurs qui achètent des médicaments sur Internet en dehors des circuits légaux qu'« ils s'exposent à utiliser des produits dont la qualité n'est pas assurée, dont les conditions de transport ne sont pas garanties et dont le bénéfice/risque n'a pas été évalué ».

http://www.douane.gouv.fr/articles/a12864-operation-pangea-ix-contre-la-vente-illicite-de-medicaments-sur-internet
http://www.contrefacon-riposte.info/international/5141-operation-pangea-ix-pres-de-5-000-sites-de-vente-en-ligne-de-faux-medicaments-et-de-dispositifs-medicaux-illicites-fermes-en-huit-jours

### *132-16-SE-07* LA RÉALITÉ VIRTUELLE S'INVITE DANS LE DOMAINE DE LA PARAPLÉGIE (SEPTEMBRE)

La réalité virtuelle devient de plus en plus omniprésente dans notre quotidien. Des jeux vidéo au cinéma, en passant par l'enseignement, elle révolutionne nombre de secteurs et plus particulièrement le monde scientifique et médical. En effet, publiée le 11 août 2016 dans la revue américaine *Scientific Reports*, une étude démontre que des paraplégiques ont pu retrouver des sensations et le contrôle partiel de leurs jambes par le biais d'immersions intensives dans la réalité virtuelle.
Pendant une année, des chercheurs de l'université de Duke en Caroline du Nord ont mené une expérience sur huit patients présentant tous une paralysie totale et de longue durée (trois à treize ans) des membres inférieurs. Chacun a été équipé d'une interface cerveau-machine, c'est-à-dire un système de liaison directe entre le cerveau et un ordinateur. Ensuite, les malades ont été plongés dans une réalité virtuelle et ont dû s'imaginer en train de marcher. L'ordinateur servait alors de relais pour transmettre les ordres donnés par le cerveau aux jambes.

Les résultats sont édifiants : au bout d'une année de rééducation, il a été constaté que plusieurs nerfs s'étaient réactivés. Au bout de vingt mois, les chercheurs ont ainsi requalifié les paraplégies de sept patients de totales à partielles. Par ailleurs, certains ont pu mieux contrôler leur vessie et/ou leur intestin, réduisant de la sorte leur dépendance aux laxatifs et aux sondes. Une femme enceinte a même pu sentir son bébé ainsi que les contractions lors de son accouchement.
Cette recherche n'en est certainement qu'à son début. La méthode pourrait notamment être utilisée sur des patients paralysés depuis peu ou être testée sur d'autres pathologies comme les maladies dégénératives.

http://www.leparisien.fr/societe/paralyses-l-incroyable-avancee-12-08-2016-6034017.php
http://www.rfi.fr/science/20160811-paraplegiques-retrouvent-capacite-mouvement-grace-realite-virtuelle
http://www.nature.com/articles/srep30383
http://www.lepoint.fr/sante/des-paraplegiques-retrouvent-une-capacite-de-mouvement-11-08-2016-2060568_40.php

### *132-16-SE-08* PARTAGE DES DONNÉES DE SANTÉ ENTRE PATIENTS ET ACTEURS MÉDICAUX (SEPTEMBRE)

Aux États-Unis, depuis 2010, 150 millions de personnes ont un accès sélectif à leurs données médicales grâce au programme « Blue Button » (un bouton bleu apparaît sur les sites des organismes adhérents). Ce procédé est appelé « *Smart Disclosure* » *ou* « divulgation intelligente ». 150 prestataires de santé y participent, régimes d'assurance santé, mutuelles, cliniques, hôpitaux, cabinets médicaux, pharmacies… Les patients peuvent télécharger leur historique de santé et leur dossier médical et le porter à la connaissance des différents acteurs de santé qu'ils consultent. Plusieurs applications mobiles existent. Ce système a été imaginé après qu'il a été constaté que les professionnels de santé, malgré les standards informatiques créés, communiquaient peu entre eux. L'idée a donc été d'en donner l'initiative aux patients eux-mêmes, ce qui a également le mérite d'instaurer un rééquilibrage dans la relation médicale. Les données sont stockées sur les téléphones portables et cryptées. La ministre des Affaires sociales et de la Santé française a annoncé en 2015 le développement futur d'un « Blue Button ». C'est pourquoi la FING (Fondation Internet Nouvelle Génération, think tank sur les transformations numériques) a mis en ligne récemment les travaux d'un groupe de travail ayant réfléchi pendant un an aux enjeux d'un tel projet. L'argument majeur est que l'open et le big data ne suffisent pas, il faut que les personnes puissent en maîtriser les usages, « avoir de nouvelles capacités d'action », pour ne pas avoir le sentiment que les données relevant de leur vie privée leur échappent.
Il s'agit donc de faciliter l'émergence d'un « self data » en croisant des informations d'ordre strictement médical, celles issues des objets connectés (certains appareils d'auto-mesure sont conformes aux prescriptions réglementaires européennes pour les appareils médicaux) et d'autres données publiques, de contexte par exemple, comme un taux de pollution ou de pollen, l'incidence d'une pathologie dans telle zone géographique, ce qui permet d'établir une cartographie pour chaque individu. En effet, « ce qui fait sens pour l'individu en matière

de santé ne se limite pas aux données “médicales” ». Un « Blue Button » à la française se différenciera nécessairement du modèle américain, les contraintes d'utilisation des données personnelles et de protection des individus étant plus fortes, mais un certain nombre de principes retenus en amont et rassemblés au sein d'une charte (lisibilité et compréhension des données par le patient, qu'il contrôle, en ciblant ce qu'il souhaite partager, avec qui, pour une durée limitée...) « pourraient permettre aux acteurs de la santé, de l’innovation, aux associations de patients… de converger vers une vision commune ». Cependant, un « mauvais » usage des données par le patient pourrait lui être préjudiciable et cette question ne peut être éludée.

http://fing.org/?Publication-du-livret-MesInfos
http://www.cercle-decideurs-sante.fr/ressources/les-ressources/518-focus-international-blue-button-la-france-a-beaucoup-plus-de-chances-de-reussir-a-l-echelle-nationale-que-les-etats-unis.html

### *132-16-SE-09* LA TECHNOLOGIE « GENE DRIVE » (SEPTEMBRE)

Le « Gene drive » est un forçage génétique. C'est « une technique de manipulation génétique qui permet de booster la propagation d’une mutation dans une population. En relâchant simplement quelques individus qui possèdent une portion d’ADN élaborée par l’homme (appelée cassette « G*ene drive* ») dans une population naturelle, on peut théoriquement obtenir en quelques dizaines de générations une population entièrement contaminée par la cassette G*ene drive* ».
Certes, ce procédé pourrait permettre l'éradication des espèces invasives et de maladies telles que le paludisme. Mais ces aspects positifs ne sauraient, selon un philosophe et une biologiste directrice au CNRS qui nous mettent en garde, en écarter les enjeux éthiques qui seraient encore plus importants que pour les OGM classiques.
En effet, cette technique, qui serait peu coûteuse, facile à réaliser en laboratoire et applicable à l'ensemble des animaux et des plantes (sexuées), modifie les espèces naturelles et sauvages au profit et pour l'usage des humains, leur conférant un pouvoir de domestication sans précédent. « Le « Gene drive » manipule à son avantage les trois piliers de la sélection naturelle : mutation, hérédité et adaptation ». Cette capacité de transformation de la nature qui serait à notre portée pose des questions sur les limites de l'action humaine, sur l'usage malveillant qui pourrait en être fait (notamment au profit d'un groupe humain en particulier) et sur les risques d'un usage bienveillant (modification d'un génome se transmettant à une population non ciblée, erreurs de manipulation entraînant un effet inverse à celui recherché, comme par exemple une résistance aux insecticides). L'enjeu serait « métaphysique, politique et économique » et nécessiterait un débat.

http://www.trop-libre.fr/la-technologie-gene-drive-une-r%C3%A9volution-en-biologie/

### *132-16-SE-10* VICTEAMS, LOGICIEL DE SIMULATION MÉDICAL (OCTOBRE)

Afin de mieux former les « leaders » des équipes de secouristes face aux situations de

crise, une équipe de chercheurs (informaticiens, psychologues, ergonomes, chercheurs en neurosciences mais aussi médecins militaires et sapeurs-pompiers) met au point un simulateur s'utilisant avec un casque de réalité virtuelle, le logiciel Victeams.
Le « leader » est le médecin qui va gérer les membres d'une équipe, assigner des tâches ou les pratiquer lui-même. Des scénarios sont établis : sauvetage au combat impliquant des blessures par balle, catastrophe environnementale, gestion d'attentat. Simulant un afflux massif de blessés, le logiciel plongera ce médecin dans une situation de stress (des cris, des sirènes, des bruits de moteur…), avec une équipe et des patients pas toujours faciles à gérer et le confrontera à des dilemmes : toutes les personnes ne pourront pas être secourues, il devra faire des choix. Victeams permettra ainsi aux secouristes de savoir prendre des décisions plus rapidement, en immersion, pour pratiquer des soins et plus seulement pour trier les patients. La formation avec ce logiciel offrira un gain de temps. En une journée, une vingtaine de stagiaires s'entraîneront avec 2 formateurs alors que pour une simulation avec un mannequin, 4 formateurs sont actuellement nécessaires pour 12 stagiaires. Ce projet, au budget de près de 3 millions d'euros, est cofinancé par l'Agence Nationale de la Recherche (ANR) et la Direction Générale de l'Armement (DGA). Il bénéficie du soutien de la Région Hauts de France et du Fonds Européen de Développement Régional (FEDER). Un prototype de ce logiciel est attendu à partir de 2019.

http://rue89.nouvelobs.com/2016/10/04/realite-virtuelle-prepare-les-secouristes-attentats-265331
https://lejournal.cnrs.fr/articles/un-simulateur-virtuel-pour-les-equipes-durgence

RETOUR

## *ADDICTIONS*


***132-16-AD-01*** **LE DÉVELOPPEMENT INQUIÉTANT DES MALADIES DITES DE « CONNEXION » (MARS)**

Une question anime de plus en plus les spécialistes de la santé : l'accroissement de pathologies liées à « l'hyperconnexion » telles que les anxiétés, les angoisses, les phobies et le stress.
Selon l'étude menée par un designer et malgré ses avantages, la connexion permanente présente de nombreux effets nuisibles sur la santé. La présence constante des médias sociaux y est pour beaucoup. Ces derniers ont contribué à créer des comportements compulsifs comme la peur de manquer de quelque chose.
La puissance des réseaux sociaux a tendance à fasciner mais les individus préfèrent souvent en minimiser les conséquences.
De nouvelles maladies sont ainsi apparues à l'instar des « junkies de la validation », obsédés par les likes, favoris et partages en ligne ; ou des « input junkies », obsédés à nourrir les réseaux sociaux.
Certains vont même à imaginer à l'avenir la nécessité d'imposer aux réseaux sociaux une limitation d'accès aux contenus. Des start-up se sont créées afin d'évaluer la dépendance à la connectivité à travers le ciblage des malaises provoqués par une sous ou sur connectivité.
Un autre comportement a été observé, la « syllogomanie du Cloud » consistant à conserver compulsivement les documents, jusqu'à dépasser les limites de stockage.
On parle aussi de « tachylalie online » pour désigner le partage permanent de contenus en ligne ; de « monophobie online » pour désigner une peur morbide de se retrouver seul sur les réseaux sociaux ; du syndrome de « l'assombrissement » pour un trouble du jugement lié au fait de s'être trop renseigné sur une personne en ligne et d'en ressentir des conséquences néfastes dans la vie quotidienne…
Face à cela, les observateurs prônent une nouvelle hygiène des données en améliorant la conception des systèmes. C'est ainsi que les appels à la déconnexion se multiplient de part et d'autre et que les entreprises commencent à s'intéresser aux effets des services qu'elles mettent en ligne car dans le futur, c'est la question de la responsabilité de ces maladies qui se posera.

http://internetactu.blog.lemonde.fr/2016/02/25/qui-sera-responsable-des-maladies-de-la-connexion/

RETOUR

## *SOCIÉTÉ*


### *132-16-SO-01* AU ROYAUME-UNI UN GUIDE POUR LUTTER CONTRE LE *SEXTING* DANS LES ÉCOLES (JUIN)

Le *sexting* est de plus en plus constaté dans les établissements scolaires britanniques et n'est pas sans poser des problèmes notamment sur l'incrimination des mineurs sur ces faits. Afin d'éclairer au mieux policiers, éducateurs et élèves sur ce problème, les responsables de la police envisagent, dès la rentrée prochaine, de mettre à disposition des unités de police et des écoles un guide pour mieux expliquer et appréhender ce phénomène.
Les élèves ont accès aux images pornographiques et ne reçoivent ni cours d'éducation sexuelle ni cours sur ce que doivent être les rapports entre les personnes. Il en résulte l'absence de connaissances sur ce qu'est le consentement et une augmentation sensible des faits de *sexting*. Sur ce type de faits, la répression montre ses limites. C'est avant tout un effort d'éducation et de formation qui s'impose.
Le but de ce guide est donc de faire prendre conscience des risques de l'utilisation du *sexting*.
Dans le même temps, il s'agirait également d'intégrer dans la scolarité une formation sur les relations et la place de la sexualité. Plus globalement, il s'agit de lutter contre toutes les formes de harcèlement et de violence à caractère sexuel. L'union nationale des professeurs y est favorable et appelle à une stratégie nationale dans ce domaine. Elle reste consciente du manque de temps pour dispenser ce type de modules dans des programmes déjà très serrés.
Ce travail sur la prise de conscience du *sexting* n'enlève rien aux mesures coercitives pour les faits de harcèlement ou de violences à caractère sexuel qui sont constatés.

*NDR : Face un véritable problème qui a pris de l'ampleur dans les établissements scolaires du Royaume-Uni, l'action répressive montre ses limites. La situation conduit à chercher une action sur les causes du problème qui reposent essentiellement sur des lacunes éducatives. Le partenariat forces de police et monde de l'éducation semble être en mesure d'apporter des solutions sans pour autant sous-estimer les faits de délinquance. On peut noter qu'en France, le Haut comité à l'égalité entre les hommes et les femmes pointe, dans un récent rapport, la frilosité de l'éducation nationale sur le thème de l'éducation à la sexualité qui conduit les jeunes à s'informer sur Internet.*

https://www.theguardian.com/society/2016/jun/14/police-chiefs-sexting-guidance-schools
http://www.haut-conseil-egalite.gouv.fr/sante-droits-sexuels-et/actualites-53/article/remise-du-rapport-relatif-a-l

RETOUR

## *RÉDACTEURS ET PARTENAIRES*

1. G[al] d'armée (2s) Marc WATIN-AUGOUARD, CREOGN, Directeur (Ligne éditoriale) ;
2. Col Laurent VIDAL, CREOGN, Rédacteur en chef (Technologies, pratiques policières étrangères, international, libertés publiques) ;
3. Lcl Jean-Marc JAFFRÉ, CREOGN (International, pratiques policières, société) ;
4. CEN Jérôme LAGASSE, CREOGN (Droit, libertés publiques, intelligence économique, technologies) ;
5. Mdl Jennifer DODIER, CREOGN (Sécurité routière, sciences et technologies) ;
6. Mme Sabine OLIVIER, CREOGN (Politique de la ville, aménagement du territoire, collectivités territoriales, associations, droits de l'homme) ;
7. Mme Sabine DRIESCH, CREOGN (Écologie, environnement durable) ;
8. Mme Odile NETZER, CREOGN (Faits sociaux contemporains, société, idées) ;
9. Mme Lucette FRANEL, CREOGN (Affaires maritimes, sécurité intérieure, terrorisme) ;
10. ASP Élodie Laurent, CREOGN ;
11. BRI Camille MIRAMBEAU, CREOGN.

RETOUR