

DEFENSE > L'Homme
et le robot

DROIT > La géolocalisation,
mode d'emploi

TECHNOLOGIE > Les
technologies s'emparent du
volant



REVUE

de la gendarmerie nationale

REVUE TRIMESTRIELLE / MARS 2014 / N° 249 / PRIX 6 EUROS

Les technologies
nouvelles

LES MONNAIES VIRTUELLES

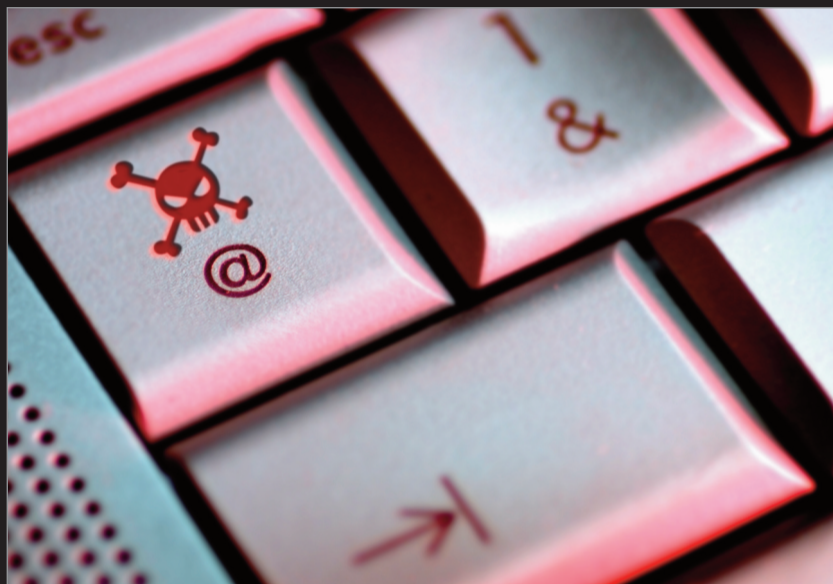
LES ROBOTS

LES DRONES CIVILS



retour sur images

NUMÉRO 248



Sirpa-gendarmerie - ADC F. Balsamo

LES DÉFIS DU CYBERESPACE

Les technologies nouvelles modifient tous nos concepts d'appropriation de nos terroirs et engagent un nouveau mode d'acquisition et de transmission de nos connaissances professionnelles.

RETROUVEZ LA
NOUVELLE
RUBRIQUE
TECHNIQUE
DE CE
NUMÉRO
EN PAGE 111 >>



© charmilliew

« Le progrès : trop robot pour être vrai »

Cette prévention, quelque peu caricaturale mais élégamment exprimée par Jacques Prévert (1900-1977), peut interpeller tous ceux qui ont à conduire le progrès au sein de leur entreprise ou de leur administration.

Dans ce numéro, nous allons explorer quelques technologies qui vont avoir une incidence directe sur le service des forces de sécurité et notamment de la gendarmerie nationale. Techniquement incontournables, elles vont optimiser l'appropriation de notre terroir par une capacité élargie de traitement de données disponibles dans des systèmes interconnectés. Elles influenceront sur nos méthodes de travail et la définition de nos référentiels de compétences. Elles dessinent les contours de métiers nouveaux où l'intelligence de nos personnels sera intimement mêlée à la dimension artificielle de celle des machines. Toutefois, cette modernité ne sera intégrée que si les concepteurs considèrent l'être humain en position centrale au travers de ses valeurs, de sa capacité à mettre de l'ordre et de la sensibilité dans la gestion des informations et de l'action. Enfin, ce n'est pas le moindre des débats, un droit nouveau va accompagner l'émergence de ces technologies dans les domaines de la communication, du transport, du commerce, de la cybersécurité et tout simplement de la protection des libertés individuelles.

**DÉFENSE-SÉCURITÉ****L'Homme et le Robot** 6

par Gérard De Boisboissel

**SOCIÉTÉ****Une révolution technologique et sociétale** 16

par Carlos Moreno

Nouvelles technologies et action des forces de sécurité 22

par Marc Watin-Augouard

**DOSSIER****Les technologies nouvelles** 32**TECHNIQUE****Les évolutions majeures des véhicules de demain** 111

Interview de Thierry Archambault

Véhicule communicant intelligent ou autonome 115

par Stéphane Milet et Pascal Cheylan

Les TIC s'emparent du volant 123

par Carole Lembezat

**DROIT/JURISPRUDENCE****La géolocalisation, mode d'emploi** 129

par Joël Ferry

DOSSIER

Les technologies nouvelles

- Indice de sécurité niveau 0...** 33
par "Avatar" d'officier de gendarmerie
- La ville : un complexe en pleine mutation** 39
par Carlos Moreno
- Sécurité et protection des citoyens : accroître la prévention et l'action grâce au numérique** 45
par Jean-Michel Corrieu et Philippe Sajhau
- SPY : la vidéo dans les véhicule pour des décisions plus rapides** 51
par Emmanuelle Villot et Éric Munier
- Les drones civils, une réglementation émergente** 59
par Christophe Masset
- Transport ferroviaire et cyberspace** 65
par Patrick Mervent
- La sécurité ou des moyens d'actions adaptés aux situations critiques** 71
par Laurent Denisot
- Évaluation comportementale des personnes et sûreté aérienne** 75
par Mickaël Terosier
- Monnaies virtuelles, l'exigence du régalien pour créer la confiance ?** 79
par par Mickaël Terosier
- Les produits de marquage codés** 87
par François Heulard
- L'ADN rapide à la portée de la gendarmerie** 93
par Emmanuel Pham-Hoai
- La filière nationale de sécurité : une opportunité pour la gendarmerie ?** 99
par Stéphane Schmolle
- L'impression 3D, enjeux et perspectives** 105
par Laurent Vidal



DES ROBOTS SUR UN THÉÂTRE OPÉRATIONNEL

- > Qu' implique la gestion de robots ?
- > Les robots doivent-ils être humanoïdes ?
- > Qui sera responsable des actes des robots ?

● La définition d'un corpus doctrinal qui puissent décliner les options stratégiques et tactiques de leur insertion dans la profondeur du théâtre d'opération.

● Une esthétique spécifique évitant le leurre d'un anthropomorphisme qui puisse évoquer une vision de parité avec son partenaire humain qui ne peut exister ni fonctionnellement, ni éthiquement.

● La définition d'une responsabilité spécifique du donneur d'ordre qui sera délicate à déterminer quand le robot aura acquis une capacité de déduction et de « réflexion » personnelle.

L'Homme et le Robot :

des partenaires au cœur du conflit

par GÉRARD DE BOISBOISSEL

L

L' introduction des systèmes terrestres robotisés sur le champ de bataille, déjà avérée lors de la seconde guerre mondiale avec l' apparition du Goliath, engin chenillé et téléopéré allemand, a pris son réel essor lors des conflits irakien et afghan au début du XXI^e siècle avec le déploiement massif des robots de déminage.

Leur utilisation ouvre une réflexion plus large dans les usages militaires. Selon la formule consacrée de Peter Singer ne se posent plus seulement la question de

savoir « *comment faire la guerre* » mais celle de déterminer celui « *qui fait la guerre* ».



GÉRARD DE BOISBOISSEL

ingénieur de recherche,
Centre de Recherche des
Ecoles de Saint-Cyr
Coetquidan

**Un concept global
mais un
équipement
différencié**

La technologie est en devenir pour la robotique, avec de rapides progrès de la science qui nous laissent entrevoir pour le XXI^e siècle une véritable « Robolution » dans les affaires militaires si, bien entendu, l'usage de ces machines est accepté par les soldats eux-mêmes. Si une nouvelle arme mal utilisée fait rarement perdre une guerre, elle peut être le facteur déterminant de l'issue de la bataille avec un concept d'emploi suffisamment novateur pour déstabiliser l'ennemi. Il suffira de prendre pour exemple l'emploi des chars de bataille et l'artillerie de campagne.

Les principaux avantages qu'offre la robotique militaire concernent la protection du soldat en l'éloignant des zones dangereuses (déminage, NRBC), la possibilité d'effectuer des missions répétitives (surveillance, patrouille), ou sans intérêt pour l'homme (comme porter des charges). Cela permet de sauvegarder la ressource humaine pour

des missions où sa valeur ajoutée sera forte et enfin d'apporter un plus tactique au combattant (voir plus loin, augmenter la zone contrôlée par une unité). Un système robotisé est ainsi une aide proposée au combattant, un outil qui est mis à sa disposition et qui peut lui donner un avantage inédit dans l'histoire militaire.

Les équipements terrestres actuels, UGV (*Unmanned Ground Vehicle*) et mini ou micro UAV (*Unmanned Aerial Vehicle*), sont communément appelés robots. La plupart sont en réalité totalement sous le contrôle d'opérateurs ce qui signifie qu'ils devraient à proprement parler être qualifiés de drones téléopérés ou d'objets à autonomie variable. Le terme « robot » dans cette étude, sera pris au sens large et couvrira les systèmes terrestres robotisés téléopérés, ou avec une certaine forme d'autonomie, ainsi que les robots autonomes à venir. Ils se caractérisent de nos jours par une faible autonomie tant énergétique que décisionnelle et leur portée visuelle tout comme leur portée de communication restent dépendantes du terrain (le milieu terrestre est très hétérogène et soumis à de nombreux obstacles).

Ils permettent d'embarquer et de mettre à disposition du fantassin des modules intégrant des capteurs (caméras, microphones, sniffeurs, détecteurs de départ de coup, etc.), ou des effecteurs (fumigènes, brouilleurs, bras articulés, etc.). L'ensemble peut permettre une

prise de décision rapide selon les menaces par un processus d'identification et d'alertes fiable et immédiat. Les robots terrestres, comme partie intégrante de l'action militaire, seront donc un outil que le chef intégrera dans l'action militaire dès la préparation de la mission et dans son ordre initial. Il pourra servir également de renfort, selon l'évolution de la manœuvre.

Une dimension stratégique et tactique nouvelle :

Sur un plan stratégique et politique, l'usage des robots en formations autonomes modifiera les modes de combat, en ce sens que le premier contact pourra leur être confié alors que l'occupation et l'organisation du terrain conquis seront dédiées aux forces

(1) Christian Malis, « *La guerre robotisée* », édition Economica, P 62.

traditionnelles⁽¹⁾. Le commandement pourra ainsi choisir

d'utiliser un « *écran robotique* » qui sera le premier à subir un choc ou à se risquer pour obtenir un renseignement. Les capacités de surveillance et d'observation constantes, de jour comme de nuit, avec interconnexion des systèmes robotisés aériens et terrestres, permettront de contrôler des zones et de tenir des espaces plus larges. Ainsi, à une époque où le format de nos armées diminue, la « *ressource humaine* » se doit d'être réservée à des actions où elle aura une forte valeur ajoutée, et de laisser à des machines des fonctions considérées

comme moins dangereuses ou répétitives. La robotique permettrait également à un adversaire plus faible d'augmenter ses possibilités d'action déportée, en utilisant des robots technologiquement simples et bon marché. Elle pourrait donner du volume à sa manœuvre en lui permettant d'opérer sur une zone plus large et de surprendre nos forces qui ne sont pas entraînées à affronter un ennemi utilisant des robots.

En termes tactiques, les catégories de missions militaires pour lesquelles les robots vont progressivement trouver leur place, sont celles où les trois avantages qu'ils offrent (protection, durabilité et accroissement de l'efficacité tactique) seront mis à profit.

Intégré dans les missions de reconnaissance, le robot va permettre de déporter plus loin l'œil, le nez et les oreilles du combattant, et ainsi lui permettre d'anticiper la manœuvre de l'ennemi. Ce sera par la voie des airs (les drones tactiques permettent un rapide survol de zone) mais aussi par voie terrestre car certaines zones ne sont observables qu'à partir du sol : buses, grottes, espace urbain, sous-sols, égouts, et des zones restent masquées du ciel par la végétation. Le robot peut être le premier élément d'éclairage, permettant de relever des menaces (présence d'ennemis, pollution, engins explosifs improvisés) en avant de la progression des forces ou des convois, sur les routes

ou les chemins. Résistant aux contraintes d'environnement, le robot permettra de progresser et de rester dans des environnements extrêmes tels que les zones désertiques chaudes, les zones montagneuses froides, le fond des étangs ou les zones contaminées par des pollutions (chimiques ou nucléaires).

Le robot n'a pas froid, ne ressent pas de fatigue ou la faim (si tant est que son autonomie énergétique est suffisante). Cela en fait un acteur naturel de la surveillance et du contrôle de zone : un robot offre ainsi l'avantage de surveiller une zone dans la durée, tout en offrant une mobilité qui permet de compléter les systèmes de surveillance fixes existant. Il peut assurer la surveillance de grands espaces urbains (zones industrielles, hangars) ou ruraux (campagne, désert), des patrouilles autour de points sensibles à protéger ou surveiller (monuments, pylônes), d'installations militaires (*Forward Operating Bases* : FOB, base) ou de campement (bivouac) et proposer une aide à la levée de doute sur des espaces déjà équipés de mécanismes statiques de surveillance : frontières, zones protégées, bâtiments.

Les robots peuvent être une aide pour les missions traditionnelles de l'Arme du Génie comme l'aménagement de l'espace de bataille, entre autres pour le déminage (équipes de Neutralisation, enlèvement, destruction des explosifs (NEDEX)), et l'appui à la progression et à



Le robot remplacera le premier échelon de combat.

la mobilité. Dans le cadre de *check point*, le robot peut détecter des substances explosives ou toxiques sur des véhicules ou des personnes. Il peut également participer à l'arrêt de véhicules suspects en mouvement, en bloquant une route par lâcher de clous ou lâcher de filets agrippants.

La délicate question de la gestion des foules

Le contrôle de foule, mission traditionnellement dévolue à la gendarmerie, peut être mise en œuvre lors des opérations de maintien de la paix. On peut imaginer des robots permettant d'aider au maintien de la foule à distance par l'emploi de gaz, de hauts

parleurs ou aidant à la protection des forces en portant des boucliers. Il nous semble néanmoins que son utilisation face à une foule est peu souhaitable. Si l'objectif de nos forces est de gagner les esprits et les cœurs, voire d'empêcher des actes malveillants de la part d'une population hostile, l'utilisation de robots aura un effet inverse de celui escompté en donnant un message de non respect de la valeur humaine, en osant mettre en face d'hommes de chair et de sentiments des machines de fer et sans âme, donc sans bravoure. Néanmoins des robots très discrets (micro drones) peuvent permettre de surveiller la foule, et de détecter les meneurs, de les photographier. L'utilisation de formes

zoomorphes (oiseaux, chiens) facilitera cette discrétion, tout en réduisant l'hostilité des foules par l'empathie qu'elles généreront.

Le cœur du métier ou l'acte de combat

En laissant à l'homme toute autorisation et décision de tir, ce qui est une position claire de l'état-major de l'armée de Terre, la possibilité d'intégrer un robot en appui du combat peut s'avérer un élément déterminant au cœur de la bataille. Ce dernier en effet peut accompagner le combattant ou bien être un pion de plus à sa disposition, déporté au profit de l'effet recherché.

Le robot non armé : un robot effecteur peut porter de façon dynamique un effet sur une zone (ex : caméra pour détecter la menace, phare aveuglant, gaz lacrymogène, fumigènes, sirène hurlante). Il peut également protéger le soldat par une action passive de protection, telle que la détection de départ de coup de feu, la remontée d'alarmes concernant le dispositif ami (détection de menaces chimiques, progression de l'ennemi). Il peut bien entendu en combat urbain, reconnaître l'intérieur d'un bâtiment ou un carrefour au profit de l'unité. Il peut enfin contribuer à la déception de l'adversaire, en émettant des bruits imitant les équipements de bataille (bruit d'hélicoptère, de chars, de tirs), en contournant ou non la position ennemie.

Le robot explosif ou suicide : en cas de nécessité, un robot pourra détruire un obstacle pour faciliter la progression des combattants, une porte ou un mur notamment. Son avantage là encore est sa mobilité et le fait que c'est lui qui s'exposera à la place du combattant.

Le robot déporté peut permettre également de déterminer et d'identifier des cibles, voire de relayer la position d'une cible pour un tir au-delà de la vue directe. La discrimination reste néanmoins un point critique et qui nécessitera la confirmation par un opérateur, le discernement ne pouvant être effectué par une machine.

Enfin le robot armé : objet de toutes les craintes véhiculées par la science-fiction, un robot armé, dont la décision de tir est sous contrôle d'un opérateur, peut néanmoins interdire une zone délimitée, dans un temps délimité, et ainsi faire effort là où l'homme n'est pas présent ou ne veut pas se risquer : il pourrait par exemple flanc-garder un raid, porter le feu dans une zone trop dangereuse pour exposer la vie des hommes (comme contourner un mur pour porter le feu à l'arrière), intervenir dans une zone contaminée, et dans le cas de guerres plus conventionnelles battre de son feu des zones face à l'ennemi.



Une utilisation différenciée selon les missions.

Une place prépondérante au sein de la fonction de soutien

Le robot peut également avoir une place de plus en plus prépondérante dans le soutien des unités militaires :

De tout temps le fantassin a dû porter de lourdes charges. C'est encore extrêmement vrai de nos jours avec les protections que le soldat doit porter (casque, gilet pare-balles), en plus de son équipement de combat (munitions, armes, *etc.*), pour un poids total supérieur à 40 kg. Décharger le combattant du transport de son matériel lui apporterait une liberté de mouvement et une endurance supérieures. Les robots mules,

pouvant progresser au rythme de la manœuvre, sans ni accélérer ni ralentir son action, et capables de suivre le combattant là où il se déplace, apporterait un avantage de confort. Dans une situation comme celle de la bataille de Grosny en 1995, où apporter le ravitaillement aux troupes russes sous la menace ennemie s'avérait extrêmement dangereux, un robot porte-charge ou mule aurait permis de porter le ravitaillement vers le front (nourriture, effets personnels voire munitions) et ainsi de n'exposer que du matériel à un tireur embusqué potentiel.

Une mule peut porter des équipements qui pourraient être utiles au fantassin, mais seulement si l'évolution de la situation le demande : une échelle télescopique, des explosifs de destruction d'obstacles, du matériel de progression, etc. La mule peut également servir de rechargement énergétique, en rechargeant des batteries dans un chargeur alimenté par le moteur du robot lui-même. Les convois logistiques sont quant à eux extrêmement gourmands en personnel pour les escortes de protection. Là encore, un convoi logistique robotisé pourrait permettre d'embarquer moins d'hommes dans le convoi, et de ne conserver que ceux dont la mission est d'escorter.

Les robots peuvent servir de relais de télécommunications, notamment lors du déploiement dans des zones où le terrain comporte des zones d'ombre ou des masques empêchant une couverture complète du réseau de communication, entre les équipements numérisés et les soldats. Le robot relais de télécommunication, mobile, pourra alors se déplacer vers l'endroit optimal permettant le relais des transmissions et l'amplification du signal (entrée de grottes, points hauts, etc.).

Une préparation à l'emploi spécifique

Les conditions d'emploi de ce matériel sont variables en fonction de l'effet recherché par le chef. Le robot se doit d'être par essence modulable et de

pouvoir embarquer des modules fonctionnels propres à la mission pour lequel il est prévu. Il faudra donc prévoir une phase amont de préparation de mission où le robot sera configuré pour celle-ci. Ce peut être un équipement de jour ou de nuit, un chargement de la cartographie du lieu pour qu'il se repère, la sélection de roues ou de chenilles pour la progression, etc.

La place du robot dans le dispositif doit être parfaitement comprise et intégrée par les combattants. Ce pour de multiples raisons, comme éviter des tirs fratricides, éviter de dévoiler le dispositif, éviter une confiance excessive dans son emploi qui créerait une faiblesse potentiellement exploitable par l'ennemi. Il n'existe qu'un seul moyen de se protéger de tels risques, c'est de s'entraîner de façon constante avec le robot.

Enfin le robot peut être utilisé en meute ou en essaim (le *swarming*). Les avantages sont multiples, soit de décupler les effets (plusieurs caméras sur plusieurs angles d'observation, plusieurs effecteurs létaux ou non létaux), soit de suppléer à la perte d'un robot par un redéploiement automatique du dispositif, ou de provoquer un effet psychologique de masse.

Un robot doit faire face à des contraintes opérationnelles : il doit être fiable et fonctionnel 100 % du temps, et son autonomie doit lui permettre d'effectuer

idéalement des missions diurnes de 12 heures, ou le double si on inclue des phases nocturnes. Il doit progresser au rythme de la manœuvre, ni trop lentement ni trop rapidement, et être discret pour éviter de faire repérer les forces amies. Il faut aussi le transporter, ce qui est une problématique majeure aujourd'hui car il n'y a plus de place disponible dans les véhicules militaires de l'avant, sauf à placer ce robot en superstructure lors des mouvements (accroissant sa vulnérabilité).

Il doit aussi faire face à des contraintes environnementales. Être opérationnel quelles que soient les conditions météo (chaleur, froid, neige, boue, sable), pouvoir se repérer de nuit, et surtout éviter des obstacles naturels du terrain : des haies, des arbres, des rochers. Pour ces derniers, un robot terrestre pourra ponctuellement s'affranchir de ces obstacles s'il intègre des capacités de saut, ou même de vol temporaire.

Il existe également des contraintes de communication. Aujourd'hui, le spectre des fréquences est facilement saturé or une ressource en fréquence est indispensable pour pouvoir mobiliser le robot, avec une bande passante permettant de transmettre des données qui sont souvent des vidéos. Or la ressource « fréquence » se fait rare pour les militaires, dans un spectre très utilisé par des opérateurs civils. Bien entendu, les données échangées doivent être sécurisées, pour éviter à l'ennemi

d'écouter, et même de prendre le contrôle de la machine. L'organe de pilotage d'un robot est aujourd'hui principalement manuel donc les limites de son utilisation sont propres à celles de l'homme qui l'utilise. Or, durant le combat ou une opération de maintien de l'ordre, le soldat préfère généralement garder ses mains libres pour assurer sa propre protection (sur son arme ou son bouclier de défense). Il faut donc un système de pilotage simple et qui ne capte pas l'attention de l'opérateur. Il est également nécessaire de ne pas surinformer le soldat par les données que peut rapporter un système robotique. Enfin, le soldat ne doit pas faire preuve d'empathie pour son robot afin de ne pas risquer sa vie pour le récupérer sous le danger. L'apparence du robot doit donc être mécanique ou bien il devra ressembler à un insecte⁽²⁾.

(2) Serge Tisseron, « La guerre robotisée », édition Economica, P 228.

Un enjeu éthique et juridique quant à l'emploi des robots

Un adversaire ou un ennemi pourrait investir le champ de la robotique pour observer nos troupes, notre dispositif et de filmer nos réactions durant l'action militaire. Sur le plan médiatique, le moindre écart de nos soldats pourrait ainsi être transmis aux médias internationaux et être le vecteur d'accusations qui fragiliseraient notre action militaire ou retourneraient une opinion publique favorable initialement.

L'utilisation de robots autonomes, qui est une nouvelle problématique contemporaine, entraîne la question de la responsabilité en cas de faute(s) et de dommage(s). La responsabilité de l'être humain sera nécessairement recherchée, quelque soit l'autonomie de la machine. Dans une telle recherche, c'est toute la chaîne des responsabilités qu'il faudra considérer, depuis les responsables de l'expression du besoin, du cahier des charges, du développement de ses composantes, de leur intégration, de leur validation, de leur certification et de leur utilisation jusqu'à l'autorité en charge du robot au moment de l'action. Un cas de figure complexe, quoique encore futuriste, concerne celui de la machine entièrement autonome, avec potentiellement une capacité d'auto apprentissage. La recherche de responsabilité, en cas de faute, sera déduite des circonstances du cas précis, et non pas sur un postulat

(3) Sur la question d'un statut juridique spécifique pour un système robotique autonome, l'étude montre qu'il n'est pas nécessaire de lui en créer un. En effet, un tel statut reviendrait à lui donner des droits, ce qui serait totalement déraisonnable : on n'imagine pas en effet de droits du robot s'il est « fait prisonnier ».

théorique *a priori* (3). Sur les questions éthiques, nous rejoignons encore la question de l'autonomie, car bien qu'il semble qu'il n'y ait pas d'obstacles

juridiques à l'utilisation de robots autonomes, la vraie question est celle de savoir si on peut éthiquement laisser à une machine la possibilité de déterminer par elle-même ses cibles et d'utiliser (ou non) une arme contre elles. Ces

problématiques, qui seront applicables à la gendarmerie nationale en terme d'appropriation du territoire ou lors d'opérations en Opex, montrent que le travail collaboratif homme-robot ne fait que commencer et requiert un accompagnement juridique sérieux et continu.

La robotique comporte un risque de rejet ponctuel par les soldats et le lot des déceptions inéluctables qu'engendreront les systèmes robotisés, notamment lorsque les résultats de leur action sur le terrain seront inférieurs aux effets attendus. Toutefois, elle est en marche et devrait s'intégrer progressivement dans l'action militaire, portée par la réduction du format des armées et les avancées technologiques de demain. Il reste que l'homme devra toujours rester au centre de l'action militaire, que les robots ne devront jamais être une excuse pour l'arrêt ou l'abandon d'une mission, et qu'en termes de judiciarisation du théâtre d'opération, leur emploi ne sera pas exonérateur de responsabilité.



© nirutti

REVOLUTIONS TECHNOLOGIQUES

- > Quels en sont les moteurs ?
- > Quel est l'objectif d'une prospective pour une institution comme la gendarmerie nationale ?

- La miniaturisation des composants et des coûts
L'adoption de normes mondiales au travers de grandes majors de distribution et de conception.
L'interconnexion des données et des systèmes.
- Anticiper et acquérir les nouveaux champs délictuels.
Prévoir une gestion des métiers et des savoirs.
Intégrer les innovations dans les matériels et les mentalités des personnels.
Mettre en œuvre des solutions respectant strictement les libertés individuelles.

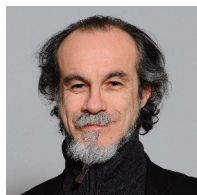
Une révolution technologique et sociétale

par **CARLOS MORENO**

A

Au-delà des nouveaux outils et pratiques qu'elles engendrent, les nouvelles technologies suscitent une forte rupture au cœur de nos sociétés en créant de nouveaux paradigmes. Elles bouleversent en effet en profondeur nos modes d'organisation et l'ensemble de nos vies, dans un monde soumis par ailleurs à de profondes mutations. Dans ce contexte, il paraît crucial pour la gendarmerie d'adopter une démarche prospective lui permettant de faciliter la gestion des crises et de les anticiper en

interprétant
l'ensemble des
signes
annonciateurs de
ruptures et de
transformations.



CARLOS MORENO

Conseiller Scientifique du
Président de COFELY
INEO.
Membre CSFRS (Conseil
Supérieur de la Formation
et la Recherche
Stratégiques)

Des

bouleversements profonds à l'échelle planétaire

(1) [http://fr.wikipedia.org/
wiki/Francis_Fukuyama](http://fr.wikipedia.org/wiki/Francis_Fukuyama)

Francis Fukuyama⁽¹⁾
nous prédisait la

« *fin de l'histoire* ». Bien au contraire, on observe à l'heure actuelle de puissants bouleversements à l'échelle mondiale, qui remettent en cause les équilibres socio-économiques et font émerger de nouveaux centres de pouvoir – annonçant un nouveau monde en pleine construction.

Parmi les grandes tendances à souligner, nous retiendrons d'abord l'explosion démographique planétaire : en 1960, nous étions 3 milliards d'habitants sur Terre. Nous sommes aujourd'hui 7 milliards et serons plus de 8,3 milliards en 2030. Dans le même temps, alors qu'on annonçait, à une époque pas si lointaine, un rééquilibrage entre zones urbaines et zones rurales, grâce au développement d'infrastructures de transport de qualité et du télé-travail, on



observe, au niveau mondial, un phénomène d'explosion urbaine : aujourd'hui, pour la première fois dans l'histoire de l'humanité, plus de 50% de la population mondiale vit dans les villes. En Europe, ce chiffre atteint 77%. Et l'on estime qu'en 2030, sur 8,3 milliards de personnes, près de 5 milliards vivront dans des zones urbaines. Tandis que la population augmente et avec elle les besoins de consommation, les experts nous alertent depuis plusieurs années sur l'inquiétante diminution des ressources naturelles, les effets dramatiques du

réchauffement climatique et l'augmentation de la pollution sur tous les territoires du globe.

Dans le même temps, on observe un basculement du monde vers de nouveaux centres de pouvoir économique. La Chine, l'Inde, le Brésil, le Mexique comptent déjà parmi les grandes puissances économiques de demain. Parallèlement, dans les pays émergents, on constate le développement d'une classe moyenne qui, avec un pouvoir d'achat devenant de plus en plus

significatif, aspire à vivre selon un modèle de confort auparavant inconnu, miroir de notre axe Nord-Ouest mal en point, avec des envies de possession, de biens, de nouveaux loisirs.

Quatre révolutions technologiques simultanées

Outre ce bouleversement des anciens équilibres socio-économiques mondiaux, nous vivons une époque tout à fait exceptionnelle d'un point de vue scientifique. Pour la première fois dans l'histoire de l'humanité, nous connaissons quatre révolutions technologiques de manière simultanée : numérique, bio-systémique, robotique-cognitive et nano-technologique.

Avec les nanotechnologies, nous sommes devenus capables de travailler au niveau du nanomètre (milliardième de mètre) avec une précision quasi atomique, ce qui devrait nous permettre de créer de nouveaux matériaux aux propriétés inédites, mais aussi à terme, de produire des nanorobots capables, par exemple, de réparer les dégâts causés par les maladies ou le vieillissement dans notre corps. La bio-systémique, quant à elle, ouvre des possibilités tout à fait nouvelles pour l'humanité, puisque nous devrions être capables à terme, d'agir directement sur l'ADN en créant par exemple de nouveaux types d'êtres vivants ou en modifiant profondément la structure de notre organisme. La révolution robotique-cognitive, en combinant les avancées des

neurosciences et de l'informatique, nous laisse quant à elle entrevoir une possible création d'intelligences artificielles qui pourraient à terme devenir égales voire, pour certains, supérieures à la nôtre.

Quant à la révolution numérique, elle bouleverse nos vies au quotidien depuis l'avènement de la première génération des ordinateurs personnels, il y a maintenant 30 ans, suivi de la naissance du web, puis, plus récemment, de celle des réseaux sociaux qui sont désormais une référence collective. Selon moi, l'actuelle révolution numérique se caractérise ainsi, principalement, par la présence diffuse du numérique au plus profond des activités humaines, via un phénomène de maillage à évolution illimitée qui se développe et qui conduit à l'omniprésence du numérique.

La révolution ubiquitaire, une « révolution dans la révolution »

L'apparition, depuis 5 ans environ, ce que l'on appelle les *smart devices* et de l'« *Internet des Objets* » est en effet en train de donner lieu à ce que je continue d'appeler une véritable «*révolution dans la révolution*» numérique : la révolution ubiquitaire, qui se caractérise par la capacité à bénéficier d'une connexion technologique au reste du monde en tout lieu et à tout moment. Avec celle-ci, des possibilités inédites s'offrent désormais aux hommes : une instantanéité de la communication, la création d'espaces transversaux caractérisés par une



© Tsiumpa

Un maillage social reposant sur les objets connectés.

métrique zéro, la capacité d'accéder à des objets autrefois réservés à des spécialistes, aujourd'hui supports d'usages multiples et ouverts à tous, dans un monde où le codage et les algorithmes se démocratisent et

(1) Application web, appelée web app, accessible via un navigateur web via un réseau informatique (Internet, intranet, réseau local).

deviennent, grâce aux Apps⁽²⁾, largement accessibles.

Il est donc essentiel de rappeler, je crois, que nous sommes en train de vivre, avec l'avènement de ce paradigme ubiquitaire, une période de rupture technologique très forte – toutes les analyses le soulignent actuellement, et à raison. Grâce à l'utilisation du silicium embarqué, tous les

objets ont aujourd'hui la capacité d'être connectés et communicants. Cette évolution nous pousse à porter un regard nouveau sur les objets que nous utilisons au quotidien, car la technologie leur confère désormais des capacités de communication, de maillage et d'intelligence. Or, on évalue actuellement à 6 milliards le nombre d'objets connectés dans le monde, pour un total de 7 milliards d'habitants et dans une dizaine d'années, ce nombre d'objets connectés sera multiplié au moins par 5 ! Les potentialités technologiques qui s'ouvrent à nous paraissent dès lors quasi infinies.

Mais s'il est important de souligner ces faits, ils ne suffisent cependant pas, d'après moi, à expliquer ce qui fait la spécificité de la révolution ubiquitaire. L'important, je pense, n'est pas que les objets soient devenus des objets technologiques, mais bien qu'ils soient devenus des objets sociaux, faisant naître du même coup, à l'échelle mondiale, une culture de l'homme numérique. Prenons l'exemple des adolescents qui se connectent à leur page Facebook *via* leur portable pour communiquer : ils font de leur téléphone un usage social avant tout, avec un mode de communication nouveau qui transite par les réseaux sociaux. Cette forme d'échange massivement utilisée remplace la conversation téléphonique, prolonge parfois la rencontre physique, mais crée aussi de nouvelles relations, qui transcendent l'objet lui-même.

Les objets du XXI^e siècle intègrent ainsi 3 composantes : technique, de savoir-faire et sociale. C'est ceci qui caractérise, selon moi, la révolution ubiquitaire : tout objet, quelle que soit la façon dont il est connecté, a désormais un usage social.



L'ÉMERGENCE DES NOUVELLES TECHNOLOGIES

> Faut-il engager une prospective sur l'évolution technologique en gendarmerie ?

> Quelle est l'urgence ?

> Des évolutions technologiques qui contribuent essentiellement à la fourniture d'outils ?

○ Cela nécessite pour nos personnels d'être capables d'intégrer une interface entre leur intelligence et celle d'une machine dotée d'un certain niveau d'autonomie et de décision du fait d'algorithmes de programmation de plus en plus complexes.

○ La gendarmerie nationale doit gagner la bataille des savoirs afin de disposer de personnels qualifiés et porter les textes relatifs à l'emploi de ces technologies en interministériel et dans les lieux de débats d'idées. A défaut, elle subira l'expertise de cercles extérieurs.

○ Il faut une grande transversalité entre la prospective, une gouvernance éclairée et le pilotage d'une R&D afin de garantir une cohérence dans la définition de la doctrine d'emploi de la gendarmerie nationale.

Nouvelles technologies

et action des forces de sécurité

par **MARC WATIN-AUGOUARD**

L

Les nouvelles technologies par leur émergence dans toutes les strates fonctionnelles de nos sociétés vont sculpter une nouvelle approche professionnelle des forces de sécurité. Elles portent en elles un questionnement sur la stratégie de leur déclinaison dans l'art de notre métier et la place de l'homme dans cette ingénierie.

Les technologies façonnent le champ de la sécurité

Examiner l'impact de l'émergence des nouvelles technologies sur l'action des



MARC WATIN-AUGOUARD

Directeur du Centre de recherche de l'école des officiers de la gendarmerie nationale

forces de sécurité est un exercice risqué. La démarche prospective que suggère le terme « *émergence* » est incertaine. Elle appelle à l'humilité car nul n'étant

prophète en son pays, chacun peut donner libre cours à une imagination d'autant plus libre que la critique de ses théories s'appuie sur des bases non consolidées. C'est la raison pour laquelle il convient de se limiter à l'examen de ce qui est probable, à l'observation des tendances lourdes dont on peut tirer des lignes de force.

Affirmer que les nouvelles technologies transforment notre société est un truisme. L'histoire nous offre de nombreux exemples de bouleversements liés à une découverte qui change les référentiels : il y a un « *avant* » la découverte de l'imprimerie et un « *après* ». Aujourd'hui, le « *tout numérique* » entraîne une métamorphose de la société dont nous ne mesurons pas encore toutes les implications. Cette mutation profonde a des conséquences immédiates sur la défense et la sécurité. Depuis longtemps, les technologies nouvelles créent des ruptures dans le

domaine de la défense (invention de l'arme à feu, de l'arme nucléaire, *etc.*) ; le duel « canon/cuirasse » est l'illustration de la relation entre les technologies et « *l'art de la guerre* ». Cette relation se manifeste au travers de la stratégie - notamment des armements -, de la tactique, de l'organisation des forces, du statut du combattant, *etc.* S'agissant de la sécurité, le lien est plus récent. L'évolution du profil du héros policier dans les romans ou les films est bien révélatrice de la relation désormais plus étroite entre technologies et sécurité. Les forces de l'ordre en tirent bénéfice, comme les délinquants qui en exploitent eux-mêmes les avantages dans l'exécution matérielle de leurs infractions. La cybercriminalité suffit à s'en convaincre.

Les technologies favorisent l'émergence de nouvelles catégories d'infractions. Un simple regard sur l'évolution de la loi pénale depuis un demi-siècle en offre une parfaite illustration. Les atteintes aux systèmes de traitement automatisés de données ou celles portant atteinte à l'éthique biomédicale n'étaient pas concevables il y a encore quelques années. Les progrès de la science ont conduit le législateur à les intégrer de façon parfois prémonitoire dans le corpus répressif.

D'une manière générale, un parallèle peut être établi entre le développement d'une société et l'évolution de la criminalité qui l'affecte. Avec le seul secteur primaire (le



Robot vigile © Yves Darnin

Demain, l'intelligence artificielle devra rester juridiquement sous la responsabilité du donneur d'ordre.

secteur agricole), les atteintes physiques aux personnes prédominent : on tue, agresse, viole, séquestre, prend en esclavage, *etc.* Le développement du secteur secondaire fait apparaître de nouveaux profits pour les prédateurs : ils volent, détruisent, dégradent, recèlent. Le secteur tertiaire (banques, assurances, services) ouvre le champ de la criminalité en « *col blanc* » : fraudes, escroqueries, abus de confiance, blanchiment, *etc.* A chaque étape, le délinquant opère un arbitrage entre le gain escompté et le risque pénal, ce qui entraîne un glissement des contentieux vers des infractions complexes plus difficiles à mettre en évidence par les enquêteurs et le juge.

Depuis quelques années, un changement profond s'opère sans que les acteurs en prennent pleinement conscience. Le « secteur quaternaire », celui dont le développement est favorisé par les technologies numériques et les découvertes scientifiques associées, ouvre un champ plus opaque, avec un « chiffre noir » d'autant plus élevé que les acteurs traditionnels ne sont pas ou peu préparés à une évolution dont la vitesse dépasse celle de leur prise de conscience. La délinquance diminue – affirme-t-on – mais n'est-elle pas en vérité en migration vers des champs encore mal délimités d'un point de vue conceptuel ? La cybercriminalité est un exemple topique d'un glissement qui aurait été inconcevable sans le développement des technologies numériques. La science au service de la santé est déjà détournée au profit de manipulations qui pourraient ouvrir la voie à des trafics contraires à la protection de l'espèce humaine. L'atteinte à l'immatériel (identité, intimité, réputation, santé, bien être, intégrité psychique, propriété intellectuelle, etc.) caractérise ce secteur quaternaire. Si certaines infractions ne sont pas nouvelles, leur intensité et leur perfidie sont amplifiées par les nouvelles technologies.

Ces technologies peuvent aussi faire « bouger les lignes » s'agissant des territoires. La mer n'est plus seulement un espace ouvert, rythmé par les flux de marchandises. Elle est désormais un

enjeu territorial de souveraineté, en raison des progrès des techniques d'exploration et d'exploitation des fonds marins, de capture des énergies renouvelables,

(1) La « *maritimisation* » est l'une des tendances lourdes qui vont modeler la société, car la mer, avec le cyberspace, est un réservoir de croissance et de progrès considérable. Mais tout Eldorado attire les prédateurs...

(2) La gestion de l'événement, la pression médiatique, l'exigence de résultat conduisent souvent à privilégier le court terme.

du terrorisme, piraterie généralisée, etc.) d'un nouveau genre, ne serait-ce qu'en raison du milieu maritime au sein duquel elles prendront naissance.

Une démarche proactive doit s'appuyer sur la prospective

La veille technologique, l'identification de nouveaux *modi operandi* doivent être intégrés dans les stratégies de sécurité. Celles-ci, il faut le reconnaître, privilégient le court terme⁽²⁾ alors qu'elles devraient s'inscrire dans une perspective temporelle au moins égale à celle qu'autorise la visibilité de la mise en application des

(3) Les retombées de la recherche fondamentale sont souvent imprévisibles. La R&D est protégée par le secret de l'entreprise. La recherche appliquée, en revanche, est plus ouverte et dessine les orientations du moyen terme.

(4) Cette coopération est encore timide, notamment dans le domaine de la lutte contre la cybercriminalité.

technologies du futur⁽³⁾. Cette démarche prospective doit s'inscrire dans un partenariat étroit avec les acteurs privés, car ils sont les principaux porteurs de l'innovation et

etc.⁽¹⁾ Les installations off shore vont se multiplier avec pour corollaire l'apparition de problématiques sécuritaires (ordre public, police judiciaire, prévention

doivent dans un esprit responsable mieux intégrer les impératifs de sécurité dans les produits, procédés ou systèmes qu'ils élaborent et ce, dès leur conception ⁽⁴⁾.

Accuser les nouvelles technologies d'être responsables de tous nos maux serait faire un mauvais procès à la science. Celle-ci ne saurait être tenue pour « *complice* » des formes modernes de l'insécurité ; c'est le mésusage des technologies par l'homme qui peut être contestable. En revanche, elles sont un allié désormais précieux des politiques de sécurité.

Un facteur de sécurité qui renforce l'appropriation territoriale

Les technologies contribuent à la sécurité, notamment parce qu'elles permettent de prévenir ou de limiter les risques accidentels, qu'ils soient naturels ou non. Elles offrent aussi des perspectives nouvelles dans la lutte contre la criminalité et la délinquance lorsqu'elles favorisent la prévention situationnelle. Les dispositifs qui empêchent la commission d'une infraction ou en réduisent les effets se multiplient.

La vidéoprotection n'a pas encore atteint le stade final de son développement. Couplée au numérique, l'intelligence artificielle - c'est-à-dire la capacité donnée aux machines de détecter, de discriminer, d'interpréter à la place de

(5) Aujourd'hui, les Centres de supervision urbains (CSU) sont limités dans leur action par la capacité humaine à traiter de très nombreuses images.

(6) Machines capables de traiter 10 milliards de milliards d'opérations par seconde.

(7) 16232 tués sur les routes de France en 1972, moins de 2000 en 2020, selon les objectifs du gouvernement. A cette date, sauf à les doter de dispositifs particuliers, les piétons seront les dernières victimes de la route.

l'homme⁽⁵⁾ - devrait accroître son efficacité au bénéfice de la sécurité des lieux publics, voire privés. Cette vidéoprotection de seconde génération ne sera qu'une composante de l'architecture de sécurité des « *villes*

intelligentes » (*smart cities*) dotées de nombreux capteurs sans fil, reliés à des calculateurs exafloppiques⁽⁶⁾.

L'automobile du futur sera plus « *intelligente* » que... son conducteur. Dotée de systèmes de détection et d'asservissement, elle évitera les collisions, régulera la vitesse, identifiera les anomalies comportementales (sommeil, alcoolémie, etc.) du conducteur. Un cap décisif sera ainsi franchi dans le domaine de l'insécurité routière⁽⁷⁾, laquelle cessera de mobiliser des effectifs de policiers et de gendarmes, très sollicités par ce contentieux de masse. Ils pourront être redéployés au profit d'autres missions (la sécurité numérique, par exemple). Quant aux vols de véhicules, ils devraient diminuer, sauf si de nouvelles formes d'appropriation apparaissent.

La domotique améliorera considérablement la sécurité de l'habitat, s'agissant en particulier de la prévention

des cambriolages, lesquels contribuent

(8) La domotique peut aussi réduire fortement les accidents domestiques.

fortement au sentiment d'insécurité⁽⁸⁾.

En se projetant dans un futur proche, l'Internet des objets devrait aussi avoir des incidences notables sur la sécurité des biens meubles. Les systèmes RFID donnent aujourd'hui un aperçu de ce qui pourrait être généralisé demain avec des réseaux de capteurs incorporés au sein des objets, voir des personnes (patches, nanotechnologies, etc.). Le passage du

(9) Aujourd'hui, le réseau Internet fonctionne avec un nombre d'adresses limité à 4,29 milliards. IPV6 offrira 340 milliards de milliards de milliards d'adresses IP, soit près de 7x10 puissance 23 adresses IP par m². Chaque grain de sable du désert pourrait être connecté. .

protocole IPV4 à IPV6⁽⁹⁾ devrait autoriser l'entrée dans le cyberspace de la plupart des objets, notamment les plus sensibles.

Selon des estimations, en 2020, 50 milliards d'objets seront connectés. Ainsi pourra-t-on, par exemple, détecter les objets volés, les objets contrefaits, assurer une meilleure traçabilité des produits au profit de la sécurité alimentaire, etc. Les exemples qui précèdent montrent que les technologies vont profondément modifier les domaines traditionnels au sein desquels l'insécurité se manifeste encore aujourd'hui. Elles vont ainsi permettre aux acteurs de la sécurité de libérer des capacités qui pourront être consacrées aux formes émergentes d'atteintes aux personnes et aux biens (la cybercriminalité par

exemple). Il serait, en effet, utopique de parier sur la fin de l'insécurité. Comme cela a été dit précédemment, des transferts vont s'opérer vers des champs que l'on ignore parfois encore, l'imagination des délinquants étant sans limite.

Pour la contrer, les acteurs de la sécurité verront leur pratique professionnelle évoluer sous l'influence des technologies.

Des pratiques professionnelles sous influence

Les technologies ont déjà profondément transformé les pratiques professionnelles depuis une quarantaine d'année. Cette tendance devrait s'accroître : le policier et le gendarme du XXI^e siècle mettront en œuvre de véritables « systèmes d'arme » qui changeront leur « profil professionnel ». Au sein des forces de sécurité, le recours à la technologie trouve son origine dans le développement de la Police technique et scientifique

(10) Parmi les pionniers, le Français Bertillon et le Britannique Galton.

(PTS) à la fin du XIX^e siècle⁽¹⁰⁾. Mais l'apport est encore

modeste et limité aux connaissances d'alors en physique et en chimie. La PTS se développe réellement à partir des années quatre-vingt, notamment grâce à l'ADN, à l'utilisation de lasers, à la spectrographie de masse, etc. Couplées à l'informatique, ces technologies contribuent à la résolution des affaires les plus sensibles. Les fichiers automatisés dits fichiers de police remplacent les

fichiers manuels. Ces fichiers de renseignement administratif ou judiciaire sont accessibles grâce au développement (et notamment à la numérisation et au passage sous protocole IP) des réseaux de télécommunications. Les réseaux

(11) Premier réseau cellulaire numérique crypté, mis en service au sein de la gendarmerie nationale à partir de 1994.

(12) Réseau de la police nationale, analogue au réseau RUBIS, de développement plus récent.

RUBIS⁽¹¹⁾ puis ACROPOL⁽¹²⁾ préfigurent la convergence aujourd'hui observée, en

intégrant la voix, l'image, le texte dans un même vecteur.

L'usage des technologies par les forces de police et de gendarmerie, sous réserve des contraintes budgétaires, devrait connaître une très forte accélération dans les prochaines années. La lutte contre la cybercriminalité est incontestablement le domaine le plus significatif. Cette forme de délinquance appelle, compte tenu des enjeux, une véritable mobilisation des acteurs de la sécurité. Si des progrès ont été accomplis depuis 2005, ils sont aujourd'hui insuffisants. Chaque enquête a désormais une composante « cyber ». Les investigations exigent des moyens d'analyse, d'expertise, etc. qui seront de plus en plus « démocratisés » pour migrer des laboratoires de PTS vers les unités du terrain.

Dans un autre domaine, on imagine les avancées qui pourraient découler d'une convergence de la cartographie, de la géolocalisation, de l'intelligence artificielle

et de l'exploitation des données au profit d'une connaissance instantanée et fiable des manifestations de l'insécurité. L'aide à la décision offrira un concours d'autant plus précieux que les moyens humains et matériels seront comptés. Elle favorisera une appropriation des territoires en allant puiser de manière instantanée dans « *l'informatique en nuage* » des *data centers* les informations utiles à la conduite de l'action.

Autre exemple, celui du contrôle des flux humains et matériels. Ces flux caractérisent une société de plus en plus mobile. Ils sont source de progrès mais sont également un vecteur privilégié par des « *criminels sans frontière* ». La biométrie, la détection et la traçabilité des objets ou des matières (*cf. supra*) pourront être intégrés dans les équipements mobiles pour un usage quasi automatisé, à l'instar de ce qui se pratique déjà pour la lecture automatisée des plaques d'immatriculation.

D'une manière plus générale, l'intégration du policier et du gendarme dans une « *bulle informationnelle* » va radicalement transformer leurs modes d'action. La mise au point d'interfaces « *homme-machine* » sera de nature à créer une interaction avec leur environnement, notamment à l'occasion de leurs patrouilles. Vêtements « *intelligents* »,

(13) Prototype récemment présenté par Google, ces lunettes permettent d'interagir avec l'environnement immédiat pour envoyer des informations contextuelles (GPS, informations sur l'environnement, images, son, vidéo, etc.).

(14) INRIA, Objectif Inria 2020.

(15) Les britanniques ont compris l'intérêt qui s'attache aux réseaux sociaux, notamment lorsqu'il s'agit d'informer la population, traiter un problème d'ordre public, lutter contre la rumeur.

lunettes à « *réalité augmentée* »⁽¹³⁾, interrogation de fichiers à la voix, etc. donnent un aperçu des applications d'un environnement informatique, capable d'intégrer toutes les fonctionnalités aujourd'hui dispersées quand

elles existent. Selon l'INRIA, l'informatique va tisser « *des réseaux de relations inédites et des institutions à l'état naissant, des individus originaux et des collectifs insolites* »⁽¹⁴⁾. Cette « *bulle* » modifiera sans aucun doute la relation avec le citoyen, dans le contact direct (capacité de détection comportementale au travers des gestes et du langage). Elle permettra, en particulier, un dialogue très décentralisé sur les réseaux sociaux, non pour les contrôler mais pour en tirer profit⁽¹⁵⁾. Elle sera une des composantes d'un commissariat ou d'une brigade de gendarmerie virtuelle, dont la pré-plainte en ligne n'est qu'un début de configuration.

Enfin, n'oublions pas la robotique, de plus en plus présente sur le champ de bataille ; elle sera demain mise en œuvre par les forces de sécurité aux fins de prélèvements d'inspection, de neutralisation, de surveillance,

d'assistance, de secours, etc. Le robot n'a d'autre limite physique pour son emploi que celle imposée par sa maintenance. Il peut agir jour et nuit, sans discontinuité. Le recours à des « *humanoïdes* » peut aujourd'hui relever de la science-fiction, mais il entrera demain dans le quotidien de la population et donc des forces appelées à la protéger.

Le recentrage du métier vers sa finalité humaine

Le concours croissant des technologies va donc entraîner une mutation radicale du profil du policier et du gendarme. C'est une évidence qui n'est sans doute pas encore prise en compte s'agissant du recrutement, de la formation, de la gestion des carrières. Les policiers et les gendarmes qui entrent en école devront être les acteurs des transformations qui s'opèreront dans les trois ou quatre décennies de leur activité professionnelle. L'aptitude des générations « Y » et « Z » à mettre en œuvre les technologies de l'information et de la communication ne suffit pas. Il faut dès à présent accentuer davantage la dominante scientifique dans les cursus de carrière, au risque de ne pas pouvoir prendre le virage, faute de compétences internes.

L'emploi des technologies aura de fortes incidences sur l'organisation des forces, sur les relations hiérarchiques internes, dans la mesure où elles vont offrir une plus grande marge d'initiative, voire

(16) Dès lors que l'on admet que le policier ou le gendarme puisse « twitter » en direct, depuis le terrain, entrer dans les réseaux sociaux, avoir son propre blog, la politique de communication institutionnelle, généralement très centralisée, très contrôlée, devra s'adapter à la dispersion des capteurs et des émetteurs.

(17) On peut imaginer la transmission en direct d'images prises par un policier ou un gendarme dans le bureau de son directeur général, voire de son ministre.

d'autonomie aux acteurs de terrain⁽¹⁶⁾, mais aussi une capacité pour les décideurs d'intervenir en direct⁽¹⁷⁾ dans les processus, sans contrainte « *espace-temps* ». La « *bulle informationnelle* » posera à la fois le problème de la

dispersion et de la concentration de la gestion quotidienne des politiques de sécurité. Les technologies auront aussi pour conséquence d'accentuer le contrôle qualité des pratiques professionnelles par le biais de la certification généralisée des processus de l'enquête.

Mais si les découvertes scientifiques semblent sans limite, leur mise en œuvre au sein de la police et de la gendarmerie sera cantonnée par la satisfaction d'un critère finaliste.

Les technologies vont donc être omniprésentes dans l'action quotidienne des policiers et des gendarmes, en suppléant parfois le cerveau humain dans les tâches qu'il ne peut accomplir en raison de leur nombre et de la rapidité de leur traitement. Sans nier ou minimiser l'importance de leur apport, il serait dangereux de s'en remettre uniquement au progrès de sciences en oubliant que la

fonction du policier et du gendarme est d'abord éminemment sociale. Les acteurs de la sécurité doivent se servir des technologies et non les servir. Cette considération peut sembler relever de l'évidence, mais il n'est pas inutile de la rappeler. L'usage de technologies doit s'inscrire dans une approche pluridisciplinaire associant les sciences humaines, notamment le droit, la sociologie. Le droit est déjà un régulateur qui tempère la mise en œuvre de solutions techniques en les subordonnant au principe de finalité, de

(18) La jurisprudence de la Cour européenne des droits de l'homme, celle du Conseil constitutionnel et les décisions de la CNIL illustrent la recherche d'équilibre entre ce qui est techniquement possible et ce qui est souhaitable au regard de la préservation des libertés publiques.

proportionnalité⁽¹⁸⁾. La question est double : quel produit pour tel usage ? quel usage pour tel produit ? La première relève d'un dialogue

avec les industriels et porte sur la réponse technique aux besoins exprimés. La seconde appelle un débat sociétal fixant les lignes d'équilibre entre sécurité et liberté.

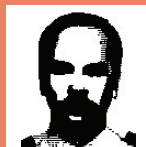
La fin ne justifie pas les moyens, mais l'emploi des moyens doivent répondre à une fin. « *Science sans conscience n'est que ruine de l'âme* » (RABELAIS). Pour les acteurs de la sécurité, il invite à un approfondissement et à une appropriation de règles d'éthique et de déontologie désormais imprégnées par des technologies qui, pour certaines, sont très intrusives dans la sphère privée des

individus. Trop souvent, l'action répond à la question « *comment ?* », alors qu'elle devrait être d'abord inspirée par la question « *pourquoi ?* ». La force publique doit être une « *force humaine* », reposant avant tout sur les hommes et les femmes qui la composent et placée au service de la population. Confiance et transparence seront plus que jamais au cœur de la relation entre les policiers et gendarmes et les citoyens, notamment à l'occasion de l'exploitation des traces que ces derniers vont de plus en plus laisser sur leur passage. L'emploi des technologies doit donc inciter à bien hiérarchiser les valeurs protégées.

Ainsi donc, au gré de l'assimilation des nouvelles technologies, les forces de sécurité devront conduire simultanément une démarche prospective et une démarche introspective. La première nécessite une méthode, une organisation, une coopération qui font aujourd'hui singulièrement défaut, en particulier parce que le temps du politique n'incite pas à la projection dans le futur, sinon immédiat. La seconde est une observation méthodique par les forces elles-mêmes de leurs « *états de conscience et de leur vie intérieure* »⁽¹⁹⁾. On va encore parler de l'Homme dans le futur, voilà qui est de nature à nous rassurer.

(19) Définition du dictionnaire Larousse.

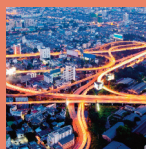
LES TECHNOLOGIES NOUVELLES



Indice de sécurité niveau 0...

p. 33

par "Avatar" d'officier de gendarmerie



La ville : un complexe en pleine mutation

p. 39

par Carlos Moreno



Sécurité et protection des citoyens : accroître la prévention et l'action grâce au numérique

p. 45

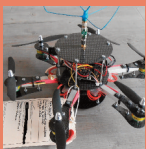
par Jean-Michel Corrieu
et Philippe Sajhau



SPY : la vidéo dans les véhicules pour des décisions plus rapides

p. 51

par Emmanuelle Villot et Éric Munier



Les drones civils, une réglementation émergente

p. 59

par Christophe Masset



Transport ferroviaire et cyberspace

p. 65

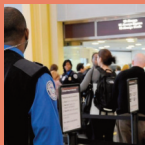
par Patrick Mervent



La sécurité ou des moyens d'action adaptés aux situations critiques

p. 71

par Laurent Denisot



Évaluation comportementale des personnes et sûreté aérienne

p. 75

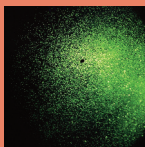
par Mickaël Terosier



Monnaies virtuelles l'exigence du régalien pour créer la confiance

p. 79

par Mickaël Terosier



Les produits de marquage codés

p. 87

par François Heulard



L'ADN rapide à la portée de la gendarmerie

p. 93

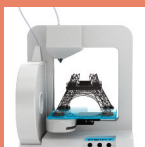
par Emmanuel Pham-Hoai



La filière nationale de sécurité : une opportunité pour la gendarmerie ?

p. 99

par Stéphane Schmolle



L'impression 3D, enjeux et perspectives

p. 105

par Laurent Vidal

Indice de sécurité

niveau 0 ...

par "AVATAR" D'OFFICIER DE GENDARMERIE

Q

Qu'il est bon parfois de donner quelque flamboyance à notre imagination et de se laisser aller à quelques supputations sur notre avenir professionnel et son contexte technologique... Chers lecteurs, laissez-vous enchanter par cette échappée sur un temps à venir... qui est déjà là...

Une journée de 2042 comme une autre

2042, 9 tempus 85 millièmes - heure de l'Union, le gendarme D. est réveillé par le réveil électronique (objet connecté), intégré à sa combinaison de sommeil. Affecté à la brigade de sécurité intérieure du secteur 26 depuis 3 mois, le gendarme D. est

satisfait ce matin. S'il a dormi durant toute son astreinte, c'est que les petits dysfonctionnements du nouveau calculateur national interservice ont été réglés.



AVATAR

code "Project_4210084Z"
d'officier gendarmerie

Il sent depuis sa chambre l'odeur du café et l'odeur du pain grillé, ce qui signifie que l'horloge locale qui avait connu, elle aussi, quelques problèmes de réglage est de nouveau recalée sur le système domotique. Il se dit que sa journée sera peut-être calme, surtout si les cybercriminels détectés hier soir en Allemagne ont pu finalement être interpellés par l'unité d'intervention internationale avant qu'ils ne franchissent les frontières de l'Union. Les réseaux sociaux ont, une fois de plus, largement contribué à la réussite de cette enquête complexe et l'information délivrée par des voisins observateurs s'est révélée particulièrement pertinente.

Le seul message affiché sur le large écran installé désormais dans tous les logements concédés par nécessité absolue de service aux militaires (statut inchangé depuis plusieurs siècles) indique que l'indice de sécurité nationale est satisfaisant ; le niveau 0 sur une

échelle de 10. Avant de faire disparaître ce message et de basculer sur un programme d'actualité, Europe-news, il jette un bref coup d'œil sur la carte de son secteur et s'assure que tous les patrouilleurs sont à l'extérieur conformément au plan électronique de coordination des forces de police communiqué chaque jour par la préfecture.

En effet, en dépit des évolutions technologiques, les gouvernements de l'Union n'ont pas souhaité remettre en cause l'organisation de la sécurité intérieure de certains Etats membres. En particulier, la France a conservé ses deux forces de police ; la gendarmerie exerce sa mission de puissance publique hors des mégapoles pour lesquelles la surveillance est assurée conjointement par la police nationale et les polices d'agglomération. Les périmètres ont été évidemment largement modifiés depuis les redéploiements réalisés au début du siècle. Toutefois, 90%⁽¹⁾ du territoire national reste encore de la responsabilité de la gendarmerie.

(1) Pas de polémique ! ce chiffre est sorti de la tête d'un rédacteur taquin...

Heureusement, le déploiement des capteurs multimédia permet d'avoir une couverture presque parfaite du territoire. Après une réticence inévitable et compréhensible des citoyens, l'omniprésence de ces objets connectés à l'ordinateur central constitue désormais

la clef de voûte de la sécurité passive. Pour les espaces non équipés en raison des coûts élevés de ces équipements, des drones assurent une surveillance depuis le ciel. Les patrouilles à deux ont disparu, mais le gendarme ou le policier en service externe dispose d'éléments pertinents avant toute intervention.

Un accident malgré les progrès du véhicule communicant

Perdu quelques instants dans ses pensées, le gendarme D. est rappelé à la réalité par la plate-forme de surveillance des constructeurs automobiles. Un accident vient d'être signalé automatiquement par le véhicule d'un particulier. Les dispositifs de protection des passagers se sont correctement déclenchés mais l'un des occupants est blessé ... c'est ce que la plate-forme d'appel d'urgence vient de signaler aux trois services qui seront finalement responsables de l'intervention : les pompiers, la gendarmerie et le service des routes car l'infrastructure routière a également subi quelques dommages. L'hologramme documenté disponible en fichier partagé sur le serveur interservices va permettre aux trois intervenants de préparer puis coordonner leur intervention. Alors que la recherche d'un lit d'hôpital disponible est d'ores et déjà enclenchée, le service des routes commande les éléments techniques qui viendront dépanner la pièce défectueuse

sur la route. Dans l'accident, le véhicule a en effet dégradé le système de contrôle de trajectoire et de gestion des flux intégré dans le revêtement de la chaussée. Le patrouilleur de la gendarmerie est, quant à lui, déjà informé et se rend sur les lieux.

Tous les éléments administratifs du véhicule en cause sont déjà intégrés au système d'information et disponibles dans la voiture de service. Les ordinateurs voire PDA ont disparu, toutes les données s'affichent désormais sur le pare-brise et sur les écrans souples présents sur tous les sièges du véhicule. Ils permettent de savoir instantanément quel est le propriétaire de l'engin et, le cas échéant, de préciser si le véhicule est inscrit ou non dans la liste des véhicules volés. Mais ce n'est pas le cas, le gendarme D. le saurait déjà puisque tous les véhicules des particuliers en service depuis 2006 disposent d'un localisateur muni d'un déclencheur automatique en cas de vol ou de conduite par une personne non autorisée (mineur ne détenant pas de permis de conduire ou conducteur non couché sur le contrat d'assurance).

On est bien loin du chronotachygraphe du précédent millénaire présent uniquement sur les transports routiers (fret et passagers) qui nécessitait une intervention manuelle. Désormais, tous les éléments tels que le temps de conduite, la vitesse ou l'état technique de

l'automobile (validité du contrôle technique) sont enregistrés par tous les véhicules y compris ceux des particuliers et peuvent être obtenus en cas d'infraction ou d'accident via les réseaux de communication qui couvrent le territoire national.

Le réseau interministériel de l'Etat (RIE) mis en service en 2014 est dans la 5^e version. Il répond aujourd'hui à l'ensemble des besoins d'échange de données aussi bien pour les fixes que pour les mobiles. Ses capacités de transport sont quasi-illimitées, tout du moins à l'échelle de la compréhension humaine, et permettent l'interconnexion de l'ensemble des systèmes d'information, dans la limite fixée par la Commission mondiale des libertés électroniques individuelles (ex CNIL).

Avant d'arriver sur les lieux, le patrouilleur télé-questionne les pièces d'identité du conducteur et des passagers. Là-encore, les travaux de l'Agence nationale des titres sécurisés (ANTS) sur la carte nationale d'identité numérique ont bien évolué et ont abouti à l'intégration d'une puce électronique sans contact « grandes elongations ». Ainsi, le boîtier SIGMA du véhicule collecte tous les éléments d'identité et peut, sous réserve de disposer des certificats d'accès, ce qui est évidemment acquis aux forces de police, transmettre ces données à distance *via* la connexion radioélectrique

de l'automobile. Le procès-verbal dématérialisé élaboré sur la base des éléments recueillis automatiquement, auquel s'ajouteront les informations des deux autres services qui concourent à l'intervention, pourra rapidement être complété puis validé par le gendarme.

Comme de nos jours...toujours au mauvais moment...

A peine a-t-il reçu le message de clôture de l'intervention, que le gendarme D. est avisé qu'un braquage se commet sur le secteur 27 contiguë à sa zone de responsabilité. L'effort porté depuis de nombreuses années sur le développement des capacités d'anticipation et de conduite opérationnelle a conduit à la mise en place d'un système d'information spécifique alimenté d'une part par les études de risques conduites sur l'ensemble des établissements commerciaux et au quotidien par le récapitulatif des moyens des unités de police et de gendarmerie. Le système expert a immédiatement interprété l'alerte transmise par le bijoutier et sollicité l'intervention de tous les moyens humains disponibles.

C'est l'occasion pour le personnel d'intervention de s'introduire dans les combinaisons exosquelettes Iron Man qui offrent évidemment une protection à l'épreuve de toutes les armes ordinairement utilisées par les braqueurs

et présentent, dans la version V3 récemment déployée, l'avantage de relever tous les paramètres médicaux du porteur de cette armure intelligente. Désormais, en cas de blessure même légère, toutes les données sont transmises au service hospitalier le plus proche qui pourra à distance proposer éventuellement les premières mesures et, au besoin, projeter une aide médicale d'urgence. Au-delà, ces exosquelettes permettent de décupler la force des policiers et gendarmes qui les revêtent. Le tissu interne présente également la particularité de réguler la température du corps. Si le patrouilleur doit utiliser son arme, la caméra intégrée fournira tous les éléments au service juridique et confirmera probablement que son emploi était justifié. Une fois encore, l'intervention ne pose aucune difficulté, les malfaiteurs interpellés sans heurt sont conduits au centre de garde à vue mutualisé de secteur. Le système de gestion sophistiqué, mis en service opérationnel depuis 2022, se charge d'allouer les chambres de sûreté et de contrôler, via de nombreux capteurs, l'état physique des mis en cause. Désormais, plus de risque de voir une personne attenter à ses jours dans le temps de la garde à vue et de décéder faute d'une surveillance appropriée.

Dur est le réveil ...

...Il fait nuit, le téléphone sonne, le gendarme D. est secoué par son épouse

qui l'invite à décrocher rapidement le téléphone de service avant que toute la maisonnée soit réveillée.

Encore une fois, le gendarme D. va pester ... il a neigé cette nuit, le véhicule de service n'a pas été rentré au garage de l'unité par la patrouille de sortie en 20h00 – 24h00. Il se dirige vers les locaux de service pour récupérer le terminal radio, la tablette tactile et son arme. Sa préoccupation ? Ne pas se tromper d'arme, car il n'y a pas de gestionnaire informatique des moyens qui enregistre toutes les demandes, vérifie plus particulièrement les références de l'arme et accessoirement que le carnet de tir de l'intéressé est à jour ! C'était quand même un beau rêve, se remémore-t-il en grattant le givre sur le pare-brise de la twingo.

Le centre opérationnel lui adresse les éléments ; il s'agit d'un accident corporel de la circulation routière. Il connaît les lieux... heureusement, car il en aurait été quitte pour remonter à son domicile afin de récupérer la carte routière du canton qu'il a trop l'habitude d'oublier chez lui en fin de service !

Et pourtant, ce n'était pas qu'un rêve !

Les directions générales de la police et de la gendarmerie nationales ont en effet renforcé les équipes en charge des études prospectives afin d'adapter les

moyens des forces de sécurité intérieure aux futurs enjeux.

Les objets connectés :

A l'occasion du dernier grand salon de l'électronique grand public (*Consumer Electronics Show*) qui s'est tenu à LAS VEGAS du 7 au 10 janvier 2014, les objets connectés ont été mis sous les feux de la rampe : montres, bracelets, jouets et autres appareils électroménagers communicants sont le marché de demain. Cet Internet des objets s'adresse à des marchés aussi cruciaux que la gestion de l'énergie et des transports. Le maintien des personnes âgées à domicile rendu possible grâce à ces dispositifs intéresse évidemment les forces de l'ordre.

Les réseaux sociaux :

Moins d'une semaine après son lancement, le compte Twitter de la gendarmerie compte déjà près de 13 000 abonnés. Ouvert à l'occasion 6^e édition du Forum international de la cybersécurité qui s'est tenue à LILLE, le mardi 21 janvier 2014, le compte Twitter @Gendarmerie suscite un fort intérêt. Dès à présent, il permet à un large public de suivre l'actualité opérationnelle de l'institution, de recevoir des informations en direct et partager des conseils de prévention. Très remarquée dans les médias, l'ouverture du compte Twitter @Gendarmerie complète la stratégie « réseaux sociaux » engagée pour

s'adapter aux nouveaux usages de communication et se rapprocher de la population en diffusant une information plus réactive et immédiatement utile.

Les drones :

Lors du 18^e salon biennal Milipol qui s'est tenu au parc d'exposition de Paris Nord Villepinte en novembre 2013, le drone à usage civil a été l'une des têtes d'affiche. Le marché de ce type d'appareil est en pleine expansion car ses usages sont très larges. Il permet par exemple de surveiller les frontières, détecter les feux de forêt, surveiller les bâtiments et infrastructures stratégiques.... et pourquoi pas de seconder les patrouilles terrestres des policiers et gendarmes. Plus de 2 000 modèles ont été créés rien que ces derniers mois, preuve d'une véritable effervescence en la matière.

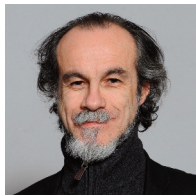
La ville : un complexe

en pleine mutation

par **CARLOS MORENO**

U

Un nouveau monde urbain est en train d' émerger, porté par ces mutations de fond et l' apparition de nouveaux paradigmes de connaissance, issus des quatre révolutions technologiques. Ce contexte fait également naître pour nous des enjeux inédits auxquels il est crucial de réfléchir. Quelles vies souhaitons-nous pour demain, à la lumière des possibilités que nous ouvre le progrès technologique ? Mais avant de s' interroger de la sorte, il convient sans doute de réfléchir à ce qu' est une ville.



CARLOS MORENO

Conseiller Scientifique du
Président de COFELY
INEO.

Membre CSFRS (Conseil
Supérieur de la Formation
et la Recherche
Stratégiques)

Une interaction généralisée

Je dirais tout d'abord que toute ville est, par excellence, un système complexe, au sens étymologique du terme, qui vient du latin *complexus*, entrelacé. Car la ville

est une agrégation d'être humains dont les besoins vitaux, d'épanouissement et de développement se croisent de multiples manières. Cela donne lieu à des ensembles de systèmes et de sous-systèmes, qui viennent s'épouser sous forme de services et d'usages pour se loger, se déplacer, se nourrir, se divertir, se soigner, s'éduquer, etc. Tous ces sous-systèmes sont par ailleurs interdépendants : les individus comme les systèmes, dans une ville, n'existent qu'en lien les uns avec les autres. Au niveau de la métropole, cette complexité est encore renforcée du fait du changement d'échelle.

Ensuite, une ville est un système vivant, qui se développe dans le temps. Comme tous les organismes vivants, elle obéit donc à deux tendances. D'une part, elle doit satisfaire ses besoins pour croître : toute ville a pour fonction de satisfaire les besoins vitaux de ses habitants et leur quête de bien-être. D'autre part, elle est



une ville est un lieu de transversalité des flux et un nœud d'interactions.

soumise à un certain nombre d'aléas qui la rendent fragile : tempêtes, pannes, incendies, attentats, épidémies, *etc.* La ville doit donc être résiliente, c'est-à-dire être capable de surmonter ces aléas.

La ville de demain, une ville citizen-centric

La ville du XXI^e siècle possède ainsi ces deux caractéristiques, mais vient s'en ajouter une troisième qui lui est propre : elle est user-centric ou citizen-centric, c'est-à-dire qu'elle offre toute une gamme de services pour mettre en cohérence les habitants et leur environnement, pour mieux vivre, mieux se loger, se déplacer,

se nourrir, *etc.* Nous sommes ainsi, selon moi, au début d'une tendance profonde, qui va bouleverser la façon dont les villes et les métropoles répondent aux besoins vitaux et de bien-être de leurs habitants et font face aux aléas qu'elles subissent, en créant des usages et des services nouveaux.

L'hybridation entre monde physique et monde numérique, rendue possible par le paradigme du massivement augmenté, porte en effet en elle un potentiel énorme de transformation de la vie urbaine, puisqu'elle permet de partir du monde physique pour le réinventer, par le biais du

monde numérique et de l'usage social qui en est fait, en proposant des usages et des services entièrement nouveaux. L'hybridation n'est pas une chose nouvelle : l'homme s'est toujours approprié son espace de manière créative par le biais de la technique puis de la technologie. Ce qui est nouveau, à l'heure actuelle, c'est que la technologie ouvre des espaces nouveaux en reliant socialement les individus. De même les activités humaines s'ouvrent actuellement à de très nombreuses possibilités à travers les objets connectés, qu'il s'agisse de l'art, de la médecine, des biotechnologies, etc. ou de la vie de tous les jours. Les usages sont ainsi, aujourd'hui, réinventés par l'hybridation.

On voit déjà apparaître aujourd'hui, par exemple, de nouvelles façons de se déplacer qui répondent à nos besoins de consommer moins d'énergie : les systèmes d'information intelligents qui nous renseignent en temps réel pour favoriser le report modal vers les transports en commun, l'auto-partage, le co-voiturage etc. Demain, on peut imaginer par exemple que la carte d'abonnement au système urbain de véhicules électriques servira aussi pour le vélib, les transports en commun, le cinéma, le retrait bancaire.... Des capteurs installés sur les véhicules permettent de créer de l'information en



temps réel pour renseigner sur l'état du trafic, alimenter des bases de données pour calculer des temps moyens de parcours, etc. De même dans le domaine de la santé, notamment en ce qui concerne la lutte contre la dépendance et le maintien de l'autonomie : il y aura sans doute des réseaux sociaux dédiés aux aidants familiaux ou destinés à renforcer les liens de voisinage, de solutions pour désengorger les consultations médicales et de façon générale pour renforcer la prévention ou enrichir le quotidien. On pourra aussi identifier plus facilement les zones de précarité sociale par exemple, en suivant leurs seuils de consommation énergétique ou leurs temps de transport, afin de leur prêter une plus grande attention.

La technologie hackée par la ville

Il est donc tout à fait intéressant de souligner le renversement qui peut finalement s'opérer grâce à la technologie connectée : bien loin d'être simplement hackée par la technologie, la ville se met à son tour à « hacker » la technologie car elle décide de la mettre à son service, en faisant d'elle un outil d'expression sociale.

On observe en effet, à l'heure actuelle, de forts bouleversements sociaux à travers la planète. Il peut s'agir de contestations de l'ordre établi, comme lors des Printemps arabes – au cours desquels la réincarnation du cyber espace dans la vie réelle, via la contestation, a joué un rôle majeur dans le renversement des régimes en place. Mais il s'agit aussi et de plus en plus de manifestations de lutte contre des grands projets lancés sans consultation préalable des citoyens, pour la préservation de vrais espaces de vie, de l'environnement, de la qualité de vie, de l'aménagement urbain. Je citerai quelques exemples: à Istanbul, il y a quelques mois, nous avons vu une forte crise sociale déclenchée par le manque d'acceptabilité d'un grand projet d'aménagement d'infrastructures urbaines. Décidé à ne pas céder, le pouvoir a pourtant été mis en difficulté en quelques jours. De même à Rio, il y a peu, la population est descendue dans la rue pour la première fois depuis 20 ans et a manifesté sous des formes diverses

contre la hausse du prix des transports et le coût, jugé trop important, des grands événements que la ville se prépare à accueillir en 2014 et 2016.

Nous sommes donc également en train d'assister à une révolution des modes d'organisation : les systèmes hiérarchisés et verticalisés sont progressivement remis en question, puisqu'aujourd'hui, avec la diffusion massive et horizontale des informations, chacun peut s'approprier les compétences et prendre les décisions, voire renverser les ordres établis.

La gendarmerie, forces d'intervention et forces de réflexion

Formidable outil d'expression des libertés collectives, la technologie devient donc un outil qui peut aussi faciliter voire accélérer la déstabilisation des ordres établis. Elle nous offre donc plusieurs facettes : outil de communication, d'échange permettant de tisser des liens sociaux dans une grande diversité ; outil captant tous nos mouvements et permettant de surveiller, repérer, contrôler ; source d'apprentissage, de savoir, de culture, de brassage ; nouvelle source de tensions et de mouvements sociaux.

Une ambiguïté qui s'est incarnée sous nos yeux dans quelques événements récents :

– le marathon de Boston : la vidéo-surveillance et les outils associés au

service de forces de l'ordre a permis d'identifier puis de retrouver en quelques heures les terroristes ; mais nous savons aussi que c'est également l'usage de la technologie qui facilite aujourd'hui les actes terroristes et les guerres asymétriques ;

- à Kiev, à l'heure actuelle, les réseaux sociaux et la force des images diffusées par leur biais jouent un rôle majeur dans la pression qui s'est créée – démontrant une nouvelle fois qu'il n'est désormais plus possible, dans ce type de conflit, de ne pas tenir compte de l'opinion publique ;
- en France, la montée médiatique de Dieudonné M'Bala M'Bala – lequel, absent des médias traditionnels, a su habilement utiliser les réseaux sociaux, notamment YouTube – se traduit par la création des tensions sociales sous un angle nouveau, car il ne s'agit plus d'une cybermobilisation mais d'une vraie mobilisation de ses supporteurs, qui se considèrent par ce biais comme des « chantres de l'anti-système » ;
- la justice est de plus en plus fréquemment saisie pour des faits comme le cas de ce légionnaire, arrêté le 18 février, pour avoir fait voler un mini drone depuis la Tour Eiffel ; celui de cette jeune personne, à Nancy, qui a fait objet de poursuites après avoir filmé la ville depuis un drone (ses images ayant été vues en quelques

heures par des milliers de personnes sur les réseaux sociaux) ; mais aussi l'utilisation du laser portable pour reconstruire en quelques heures le terrible accident du train dans les Alpes dû à la chute d'un rocher, la diffusion par la police de la photo d'un

(1) <http://fr.news.yahoo.com/police-diffuse-photo-d-39-cadavre-twitter-l-164700416.html>

cadavre sur Twitter⁽¹⁾ pour l'enquête ou la création récente du compte Twitter de la gendarmerie nationale.

Dans tous les cas, il s'agit pour nous de réfléchir à l'équilibre indispensable entre la démocratie, les nouvelles formes d'expression, la participation citoyenne et la sécurité, qui sont tous des éléments indispensables pour notre développement social.

Face à ces évolutions complexes, je crois que les forces de la gendarmerie française, qui représentent une des composantes visibles et majeures de l'autorité étatique, participent déjà à la profonde transformation que nous voyons s'opérer dans les usages et les comportements sociaux amenés par les nouvelles technologies. Forces d'intervention, elles doivent aussi se faire forces de réflexion, pour être capables d'anticiper les crises avant que celles-ci ne se produisent. En s'appuyant sur le levier de l'analyse sociétale et urbaine, la gendarmerie a la capacité de s'attacher, au travers des révolutions technologiques

en cours également, à l'analyse des « signaux noirs et faibles », ces signes précurseurs qui annoncent, à 5 ou 10 ans, des situations critiques sur lesquelles il est trop tard pour agir. Les réseaux sociaux, par exemple, sont devenus un nouveau terrain de confrontation et de tension (cyberhacking, cyberrévolte) où les interventions sont déjà plus importantes, en termes d'intensité et de confrontation, que celles de la rue.

A l'horizon de quelques années, les nouvelles formes d'hybridation de la technologie dans nos villes et nos vies avec la réalité augmentée, les drones d'usage quasi personnels, les *wearable devices* tels les *Google Glasses* et toutes sortes d'objets connectés, l'impression 3D, la simplicité de la reconstruction des environnements 3D par des appareillages simples, voire embarqués dans les téléphones, la généralisation des systèmes de haut débit en situation de mobilité et l'explosion d'une multiplicité de réseaux sociaux véhiculant images, vidéos, messageries, créeront autant des situations qui, par le phénomène de maillage qui les caractérise, échapperont à un contrôle centralisé et planifié.

Tous ces phénomènes doivent être étudiés et compris dès aujourd'hui par l'analyse prospective car ils sont à la croisée de nouveaux sentiers d'expression sociale, de vie et de tensions de toutes sortes.

Sécurité et protection des citoyens : accroître la prévention et l'action grâce au numérique

par **JEAN-MICHEL CORRIEU** et **PHILIPPE SAJHAU**

L

Les citoyens attendent des opérateurs publics qu'ils assument leurs responsabilités en matière de sécurité. Une ville réputée sûre attirera de nouveaux citoyens, de nouvelles entreprises et augmentera son attractivité touristique et économique. Cet article permettra au lecteur d'appréhender les perspectives et les solutions mises en œuvre par IBM pour concourir à l'avènement d'une ville plus intelligente et sûre.



JEAN-MICHEL CORRIEU

Directeur
Centre mondial de
Solutions Métiers IBM
Nice Sophia-Antipolis



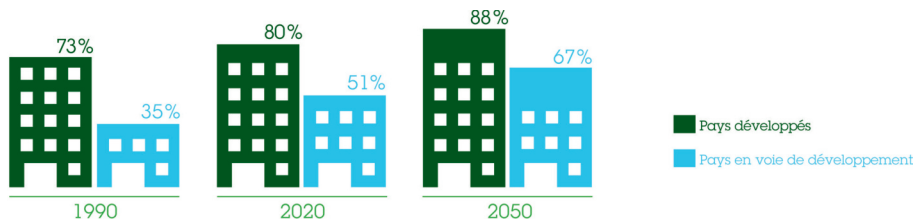
PHILIPPE SAJHAU

Vice-Président IBM
France, Smarter Cities

Bâtir une ville intelligente

Le futur de l'humanité s'écrira-t-il dans les villes ? Il est légitime de le penser. Depuis 2007, plus de la moitié de la population mondiale vit en milieu urbain. Cette tendance, identique dans les pays développés et dans les pays émergents, va se poursuivre : la projection est de 70% en 2050. On estime également que le nombre de personnes vivant dans des villes d'au moins un million d'habitants approchera les 2 milliards en 2025 alors qu'il était de 500 millions en 1975.

Les villes deviennent les moteurs économiques, sociaux, culturels et technologiques d'un monde en pleine transformation. Elles gagnent en influence, mais aussi en responsabilités. La croissance démographique en milieu urbain, la raréfaction des ressources naturelles, les contraintes budgétaires et le vieillissement des infrastructures imposent un changement de modèle de



Source : Analyse des données des Nations Unies de l'IBM Institute for Business Value.

Une concentration humaine préoccupante dans les villes des pays en voie de développement.

pilotage. Mieux contrôler leur fonctionnement et leur développement est une nécessité. Les seuls moyens humains ne peuvent suffire quand il s'agit d'apporter des services de qualité à une population en augmentation constante, de réduire les gaspillages ou encore de concevoir des infrastructures innovantes.

Plus les villes grandissent, plus les systèmes à gérer deviennent complexes et plus la quantité d'informations à traiter est importante. Le défi posé par un avenir durable est lié à la capacité à transformer des milliards de données en connaissances utiles au service des citoyens et de l'écosystème et planifier l'avenir de nos territoires urbains.

Bâtir une ville plus intelligente, c'est être capable de mobiliser tout le potentiel offert par les nouvelles technologies de l'information et de la communication pour répondre aux enjeux économiques,

sociaux et environnementaux en développant des solutions innovantes au service de tous : citoyens, entreprise, collectivités. Pour les citadins, une ville plus intelligente est avant tout une ville qui facilite les déplacements, gère efficacement les ressources énergétiques, assure la sécurité, offre des conditions de formation optimales, simplifie les relations avec l'administration... De plus en plus exigeante, la population attend que l'afflux urbain et la croissance économique qui l'accompagne génère des normes de qualité de vie élevées.

L'interconnexion des objets, des services et des personnes est un fait.

Ce monde
C'est simple.
C'est linéaire.

Les personnes, les objets interagissant et s'échangeant entre eux, se voient offrir des solutions personnalisées de données.

Nous devons de manière et de manière croissante l'exploiter et développer les moyens de les transformer en données et en services.

Le monde est de plus en plus instrumenté.
Le monde est instrumenté et il est basé sur les données. Mais attention car il y a aujourd'hui un milliard de transactions par seconde, milliards de personnes, la téléphonie mobile et 25 milliards d'appareils connectés (MPEC). La génération connectée et le fabricat croît des puces sort à l'origine de ce phénomène.

Le monde est de plus en plus interconnecté.
60 milliards de connectés interconnectés à l'échelle de 2 milliards ! Les réseaux sociaux nous permettent d'usage d'internet. L'industrie cherche à devenir plus. Les personnes, les objets et les processus d'une organisation peuvent être connectés en temps réel. Élargir la quantité d'informations produite par l'interaction entre tous ces éléments.

La ville devient plus intelligente.
Assurer à des coûts d'analyse personnalisés, des modèles prédictifs et des services, les supercalculateurs ou les réseaux sociaux et les outils «Cloud Computing» usage d'internet. Les technologies de l'information sont prêtes à se mettre au service des citoyens. La mise en relation des données issues de ce monde interconnecté permet de générer, les personnes et les infrastructures (transport, santé, éducation, services...) plus efficaces, plus productifs, plus résilients. En un mot, plus intelligents dans le but de servir les populations.

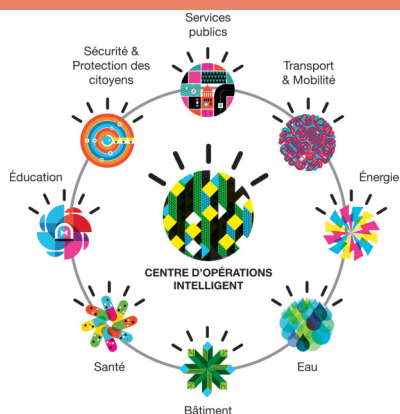
La conception d'un centre d'opération intelligent

En pensant nos villes comme un « tout », comme un ensemble de systèmes au service des citoyens, un Centre d'opérations intelligent propose une solution qui permet aux villes de toutes tailles d'innover grâce à une vision fédératrice et collaborative du fonctionnement de la cité. A travers le Centre d'opérations intelligent, les villes sont capables de collecter, analyser et traiter en temps réel les informations produites par les différentes agences de l'écosystème et les services municipaux, tels que la sécurité publique, les transports, l'eau, les bâtiments, les organismes sociaux, etc. Il permet d'analyser ces informations en temps réel afin de développer des modèles d'analyse qui permettent d'anticiper les problèmes et de réduire l'impact des perturbations sur le quotidien des administrés. Il intègre l'ensemble des données afin de permettre une prise de décision rapide qui réponde aux événements et aux incidents. Enfin, il permet de calculer et simuler l'impact des décisions sur l'avenir et devenir de la cité.

A titre d'exemple, IBM et Rio de Janeiro collaborent pour faire de Rio une ville plus intelligente. Tout a commencé par une initiative du maire de la ville qui a souhaité explorer des pistes d'innovation avec IBM dans la perspective de la Coupe du monde de football de 2014 et des Jeux olympiques d'été de 2016. A Rio de

Janeiro, un Centre d'opérations intelligent permet d'intégrer et d'interconnecter des informations de multiples sources pour aider la ville dans ses opérations quotidiennes ainsi que lors de situations d'urgence. Ce système prévoit très précisément les précipitations et les risques de glissement de terrain pour chaque quartier (1km²) de la ville 48 heures à l'avance contre 6 à 4 heures maximum auparavant, afin de déclencher une évacuation si nécessaire. Les services de distribution d'eau, assainissement, transports urbains, système de santé, sécurité civile, forces de l'ordre, collecte des déchets, éclairage public, logement, tourisme, système éducatif..., s'intègrent au fil du temps sur cette plateforme unique. La bonne gestion du trafic, et l'amélioration donc du temps des interventions d'urgence, sont des éléments majeurs pour la sûreté

urbaine. Tous les services de la ville pourront bénéficier du centre d'opérations pour un fonctionnement collaboratif intégré.



La solution IBM d'un centre d'opération intelligent.

En France, dans le cadre d'un contrat de Recherche et Développement avec Montpellier Agglomération, les universités et ses partenaires, IBM met en place une plateforme collaborative basée sur un Centre d'opérations intelligent qui permettra aux entrepreneurs du territoire d'imaginer de nouveaux services urbains autour de la santé, de la surveillance hydraulique et de la gestion des risques. Cette plate-forme permettra aussi d'optimiser les systèmes et de réduire les coûts.

La ville intelligente au Centre mondial de solutions de Nice – Sophia-

Antipolis

Le Centre mondial de solution métiers IBM situé à La Gaude (Nice) se consacre à l'innovation technologique appliquée aux différents secteurs d'activités. Il héberge notamment le centre d'excellence pour des villes plus Intelligentes. Les architectes informatiques spécialisés développent des solutions métiers innovantes basées sur les meilleures pratiques à travers le monde. Ces solutions répondent aux enjeux des territoires urbains tels que la sécurité et la protection des citoyens, le transport et la mobilité, l'énergie, l'eau, ou encore l'éducation. Elles illustrent aux différents acteurs des villes le potentiel offert par l'utilisation pertinente des nouvelles technologies de l'information pour repenser les modes de fonctionnement, innover et construire un futur durable. Parmi les solutions proposées par IBM, on distingue quatre outils développés au profit des opérateurs et des décideurs. La force de ses solutions provient du fait que les experts mobilisés travaillent avec les organes de sécurité des villes du monde entier pour améliorer la prévention et l'action dans les domaines de la sécurité des citoyens.

En matière d'analyse comportementale et environnementale, une solution concerne la détection d'anomalités. Les systèmes de vidéo protection génèrent un flux croissant d'images qui réduit l'efficacité

des opérateurs dans la détection d'anormalités. L'attention humaine perd en effet jusqu'à 90 % de son efficacité au bout d'une vingtaine de minutes d'analyse. Dans les grandes agglomérations, couvertes par de nombreuses caméras, les opérateurs ne peuvent visualiser en temps réel et en simultané que 10% des vidéos d'où l'importance de s'intéresser aux « yeux virtuels », systèmes de détection automatique d'anormalités. Dans un même temps, les centres de surveillances urbains sont de plus en plus sollicités par les services judiciaires pour la recherche de preuves à partir de l'archivage vidéo. La solution *Intelligent Video Analytics* d'IBM intègre les dernières technologies d'analyse d'images qui apportent une meilleure visibilité dans cette recherche de preuves par l'indexation en temps réel des différents objets qui se déplacent dans le champ de vision des caméras. Chaque objet en mouvement (personne, véhicule, autre) est caractérisé par un jeu d'attributs définissant son profil (classification, couleur, taille, déplacements). Le bénéfice sera tout autant dans la recherche de preuves, afin de retracer l'historique d'une situation précise, que dans l'investigation à court terme d'un événement majeur (ex : recherche d'une personne portant un pull et des baskets verts). Ce type de techniques peut améliorer jusqu'à 30 fois

la rapidité d'une recherche classique à partir de vidéos. Cette innovation technologique est utilisée dans plusieurs grandes villes telles que New York, Chicago ou Rio de Janeiro.

Un deuxième outil est constitué par l'*IBM Crime Management Center*, destiné aux agences et organisations dont la mission première est la lutte contre la criminalité, le maintien de l'ordre et l'amélioration de la sécurité publique. La solution favorise l'intégration et le partage d'informations internes et externes, structurées ou non. Elle intègre des fonctionnalités avancées de collaboration entre les équipes permettant aux différents acteurs de la sécurité publique de se concentrer davantage sur leurs missions de prévention, de prédiction, d'enquête et de déceler des menaces criminelles ou terroristes élaborées. La solution proposée mobilise des outils de visualisation et d'analyse mais également des modèles de prédictions qui permettent d'ajuster les stratégies de maintien de l'ordre et l'allocation de ressources en fonction de l'historique de la criminalité. En fonction des incidents, de leurs fréquences et de leurs situations géographiques, le *IBM Crime Management Center* va suggérer des décisions et points d'attention particuliers. Pour assister les personnes sur le terrain, la solution intègre des fonctionnalités de mobilité telle qu'une

application mobile embarquée et un gestionnaire de cas mais aussi une suite complète d'aide à la décision.

L'analyse du renseignement est une étape essentielle à l'appropriation des faits et un prérequis à la prise de décision. L'*IBM i2 Analyst's Notebook* permet aux analystes de classer, analyser et visualiser rapidement des données provenant de sources disparates. Il réduit le temps nécessaire pour reconnaître l'information essentielle et fournit un renseignement concret et opportun permettant d'identifier, de prévoir, d'empêcher et d'interrompre les activités terroristes, criminelles et frauduleuses. La solution, initialement développée pour les enquêtes judiciaires, se trouve de plus en plus utilisée dans des affaires de fraudes, financières ou aux assurances, afin de mettre en évidence des pratiques difficilement décelables. Par exemple, dans le cadre de fraudes financières, ce ne sont plus nécessairement des transactions de montants élevés qui sont concernés, mais de nombreuses transactions de montants moins importants. Or ces « petites » transactions sont plus difficiles à détecter lors d'une investigation classique.

Enfin, est couverte la gestion des urgences par l'outil *Intelligent Emergency Management Center*. Le changement climatique a enclenché des événements météorologiques majeurs qui ont un impact sur la gestion des territoires par les pouvoirs publics et suscitent une attention particulière des compagnies d'assurance. On estime entre 25 et 35 % de la production de richesse nationale directement influencée par la météorologie. Comme l'illustrent les tempêtes qui ont déferlé cet hiver sur les côtes françaises et britanniques, bénéficier de meilleures capacités de prévision et de réaction pourrait faire gagner plus de 10 milliards d'euros par an à l'économie française (Météo France). L'*Intelligence Emergency Management Center* permet de collecter et d'agréger des informations en temps réel provenant de différentes sources d'informations. Elle permet d'anticiper les risques, zones inondables, incendies, trafic saturés... et de coordonner les actions inter-organisations afin de réduire les impacts. Cette plate-forme opérationnelle et décisionnelle s'utilise aussi bien en temps de crise qu'en administration quotidienne, et permet ainsi de gérer les différentes phases d'une urgence : réduction, prévention, gestion et remise en service.

SPY : la vidéo dans les véhicules pour des décisions plus rapides

par EMMANUELLE VILLOT et ERIC MUNIER

Imaginez un centre ville bondé un samedi soir. Soudain, un incident débute dans une rue adjacente. Un système de surveillance innovant détecte automatiquement le démarrage d'une rixe et alerte instantanément une patrouille de police qui se trouve à proximité. Les policiers interviennent et traitent l'incident avant qu'il ne dégénère. La vidéoprotection intelligente en environnement mobile offre des perspectives séduisantes aux forces de sécurité et de secours pour améliorer leur réactivité et leur

efficacité dans des contextes opérationnels imprévisibles et évolutifs. Les avancées technologiques garantissent qualité, fiabilité, sécurité et intégrité de ces nouveaux systèmes qui révolutionneront demain le quotidien des policiers et des gendarmes.

Coordonné par la société *Airbus Defence and Space* (ex *Cassidian*), le projet européen SPY (*Surveillance imProved sYstem*) préfigure l'arrivée prochaine d'un système de surveillance mobile avec détection automatique d'évènements (identification d'objets et de personnes, détection d'agressions, de comportements anormaux...). Aujourd'hui les caméras de vidéoprotection fixes sont omniprésentes mais leur efficacité est limitée d'une part car elles ne répondent pas aux besoins de mobilité des utilisateurs et d'autre part parce que les personnels des centres de supervision et de contrôle



EMMANUELLE VILLOT

Chef de projet du Pôle Pilote de Sécurité Locale



ERIC MUNIER

Chef de projet Recherche et Technologies au sein d'Airbus Defence and Space

n'ont pas la capacité de traiter les milliers d'images qui arrivent. Les images provenant des caméras fixes sont donc globalement sous exploitées et ne servent souvent qu'à fournir des preuves *a posteriori*.

Le projet SPY a pour but de réaliser de nouveaux systèmes d'assistance et de surveillance, intelligents et automatisés, adaptés à la mobilité des utilisateurs (véhicules de police et de gendarmerie). Cet aspect de mobilité implique le développement de solutions intelligentes utilisables directement sur le terrain, qui doivent donc minimiser la quantité d'informations à transmettre entre le centre de supervision et les opérationnels (optimisation de la bande passante du réseau de télécommunication) et donner à ces derniers les moyens de réagir le plus rapidement et efficacement possible à une situation donnée, grâce à des capacités de détection et d'analyse de l'environnement (objets volés, comportements anormaux, recherche et identification de personnes). Pour ce faire, SPY exploite des applications ainsi que des algorithmes avancés pour fournir aux utilisateurs une représentation de la situation la plus pertinente possible et un support automatisé d'aide à la prise de décision pour s'adapter au contexte changeant et imprévisible de la nouvelle délinquance.

L'appréciation de la situation est en effet un point critique surtout dans des environnements complexes et fortement dynamiques nécessitant des décisions

rapides. Pour les aider dans leurs missions au quotidien, les forces de sécurité et de secours ont besoin de pouvoir s'appuyer sur des informations fiables et pertinentes via des médias tels que la vidéo et la représentation interactive des données. Le démonstrateur développé dans le cadre du projet met en œuvre différentes techniques innovantes pour répondre à ces besoins de partage en temps réel de contenus enrichis (tels que des vidéos associées à des métadonnées comme la zone d'intérêt, la localisation, etc.) entre les salles de contrôle et les agents sur le terrain, pour une action rapide en cas d'incidents.

Un projet de recherche européen

Le projet SPY fait partie du programme de recherche et développement européen ITEA 2 (Information Technology for European Advancement), qui labellise des projets dédiés à la conception et au développement de systèmes et services à base de logiciels. Les partenaires engagés dans les projets ITEA sont financés partiellement par les gouvernements respectifs de leurs pays. Pour la France, ils sont soutenus par le ministère du Redressement productif. SPY s'est déroulé de 2011 à 2013 et 13 partenaires (PME⁽¹⁾, académiques et grands groupes industriels) issus de quatre pays ont participé à sa réalisation, la société *Airbus Defence and Space* assurant la coordination du projet.

(1) Petite et moyenne entreprise.

Partenaire	Type	Pays	Expertise
Arc informatique	PME	France	Systèmes SCADA* et automatisation
Airbus Defence and Space	Grand groupe	France	Systèmes de communications sécurisées et systèmes de surveillance aux frontières.
Ecole Nationale Supérieure de Techniques Avancées	Université	France	Traitement image et vidéo, temps réel et implémentation dans l'embarqué.
Institut d'Electronique Fondamentale	Université	France	Traitement de l'image, optimisation des algorithmes et parallélisation pour des systèmes temps réel embarqués
Institut Mines-Telecom	Université	France	Codage vidéo adaptatif, indexation, tatouage et standardisation ISO/IEC
EOLANE	PME	France	Capteurs audio/vidéo embarquables et systèmes de vidéoprotection embarqués
Pôle Pilote de Sécurité Locale	Association	France	Expérimentation de nouvelles technologies dans le domaine de la sécurité urbaine
ASELSAN .A.S	Grand groupe	Turquie	Systèmes électro-optiques, micro-electroniques et de guidage pour des applications militaires et de sécurité
C2Tech	PME	Turquie	Systèmes d'aide à la décision pour salles de commandement
VTT Technical Research	Centre de Recherche	Finlande	Crédibilité de l'information, fusion de données
Roger-GPS Oy	PME	Finlande	Localisation
Kilosoft	PME	Finlande	Logiciel de monitoring réseau
CogVis software und Consulting GmbH	PME	Autriche	Vidéosurveillance intelligente

*télé-surveillance et acquisition de données

Des innovations technologiques majeures

L'objectif global de SPY est d'améliorer les systèmes de surveillance actuellement mis en œuvre en zone urbaine en mettant à profit les informations visuelles en provenance de systèmes mobiles en temps réel. Or la vidéoprotection en milieu mobile, au regard de sa nature, est dépendante de ses capacités de transmission de données, ce qui peut jouer sur la qualité et le nombre de flux vidéo. Aujourd'hui les réseaux de communications de sécurité publique (RUBIS et ACROPOL en France), sont principalement dédiés pour des services de phonie, et en outre n'offrent pas la bande passante suffisante pour transmettre des flux vidéo. L'arrivée des

(3) 4^e génération.

(4) *Long Term Evolution*

réseaux commerciaux 4G⁽³⁾ offre une alternative

mais ceux-ci ne sont pas assez sécurisés en termes de confidentialité, de qualité de service et de résilience. Une solution radio haut débit sur une base technologique LTE⁽⁴⁾ répondra à ces critères pour déployer des applications haut débit (vidéo, consultation de base de données multimédia...) mais malgré tout, les aspects relatifs à la bande passante restent problématiques et la gestion de celle-ci délicate. L'équipe SPY a su être ingénieuse pour économiser cette denrée précieuse. Les deux concepts permettant cette optimisation sont assez simples dans leur compréhension mais se révèlent

beaucoup plus complexes à mettre en pratique, à savoir ne transmettre que lorsque cela est nécessaire et adapter la qualité de la vidéo en fonction de la disponibilité du réseau et de la situation.

Les aspects légaux et les critères d'acceptabilité ont aussi été pris en considération par le projet d'une part pour garantir la confidentialité et l'intégrité des flux vidéos afin qu'ils soient légalement recevables en tant que preuve, et d'autre part pour fournir un accès simple et rapide à ces vidéos et faciliter la recherche et la corrélation des informations.

Airbus Defence and Space et les partenaires du projet ont travaillé sur des innovations technologiques aussi variées que :

- des algorithmes de détection de situations anormales dans un contexte mobile,
- des caméras intelligentes, permettant d'embarquer des algorithmes, de s'adapter au contexte de la mission et de remonter les informations pertinentes,
- la garantie d'intégrité des flux vidéos grâce à des techniques de tatouage ('watermarking') et de cryptage des données afin de détecter toute modification de ces données sans en altérer le contenu, ni que cela soit visible,
- la compression adaptative des flux vidéo en fonction de la bande passante pour



maintenir le flux vidéo à tout moment et adapter la qualité à la demande de l'opérateur,

- des enregistreurs « *intelligents* » de flux vidéos, en local (véhicule) mais aussi à distance (centre de commandement), dans un but de recherche rapide d'information dans les enregistrements,

- de nouvelles solutions de représentations interactives des informations permettant de présenter à l'utilisateur une vue de situation intuitive,

compréhensible et adaptée pour faciliter la prise de décision. Les flux vidéo affichés par le système de supervision intègrent par exemple des métadonnées telles que la position de la caméra et le type d'événement détecté et un basculement automatique vers des caméras du réseau fixe situées à proximité peut se faire.

Des résultats probants

L'intégration de toutes ces innovations dans un seul et unique système de surveillance a été l'un des enjeux de SPY



Les avancées technologiques sont prometteuses comme la reconnaissance faciale dans des environnements maîtrisés.

et le résultat obtenu est à la hauteur des efforts fournis par *Airbus Defence and Space* et ses partenaires. Pour la revue finale du projet en décembre 2013, il a été mis en œuvre un véhicule équipé de différents capteurs intelligents (caméras optiques et infrarouges) dans lesquels étaient directement intégrés les algorithmes et technologies développés au cours du projet. La démonstration finale organisée par le Pôle pilote de

sécurité locale (PPSL), qui a eu lieu dans les locaux de l'ENSTA à Palaiseau en présence des représentants d'ITEA2, s'est faite sur la base de deux scénarii opérationnels, l'un de gestion de foule lors d'un événement sportif, le second simulant un trafic de stupéfiants dans un hall d'immeuble. Il a ainsi été possible de montrer la capacité du système à détecter des événements anormaux (chute de personne, rixe, fuite d'un

individu, démarrage de feu, détection de visage) dans un contexte mobile et à les remonter en temps réel vers un centre de supervision. Les possibilités offertes par ces avancées technologiques sont donc très prometteuses même si certaines fonctionnalités nécessitent encore des développements complémentaires, comme la reconnaissance faciale qui, si elle est possible avec une caméra fixe dans des environnements maîtrisés comme un hall de gare ou d'aéroport, reste encore complexe en mobilité.

Des contraintes légales

La mise en œuvre d'un système tel que SPY ne peut cependant se faire que dans un cadre légal et il doit donc être tenu compte des règles liées à la protection de la vie privée et au droit à l'image en vigueur dans de nombreux pays. Il peut par exemple être nécessaire de flouter les visages ou cacher les zones privatives comme les jardins. Le droit d'en connaître doit aussi être respecté pour les autorisations d'accès aux flux vidéo. La législation applicable dans les différents pays partenaires du projet a donc été étudiée afin de proposer des solutions compatibles des règles en vigueur ou le cas échéant envisager une évolution des cadres d'emploi légaux préalablement à toute commercialisation.

Cadres d'emploi et nouveaux concepts opérationnels

Un système tel que SPY pose la question de l'emploi futur de ce type de technologies et des répercussions qu'elles auront sur les conditions de mission et les modes opératoires des forces de sécurité et de secours. De nouveaux métiers consacrés à l'exploitation de systèmes de vidéoprotection, comme ceux de responsable de centre de supervision ou d'opérateur vidéo, voient déjà le jour mais l'arrivée de la vidéo intelligente dans un contexte de mobilité laisse entrevoir de nouvelles utilisations et ouvre des perspectives pour l'augmentation de la réactivité et de l'efficacité des policiers et des gendarmes dans leurs missions de surveillance, d'intervention et de contrôle. L'accès en temps réel à des données visuelles de la situation sur le terrain pour les responsables des interventions basés dans les salles de commandement fiabilisera l'interprétation des informations et les décisions qui en découlent. Des missions de surveillance discrète pourront se faire à distance avec détection automatique de personnes et d'incidents à partir d'analyses algorithmiques de visages, de vêtements et de comportement et retransmission de ces informations vers un centre de contrôle distant où une prise de décision pourra se faire très rapidement au vu des images remontées en temps réel. Dans un proche

avenir, une voiture de patrouille équipée d'une caméra intelligente pourra aussi détecter automatiquement un suspect et interagir avec un réseau de caméras fixes pour obtenir des informations supplémentaires et suivre l'individu à distance au travers du réseau. On peut ainsi imaginer le déploiement de quelques véhicules équipés de caméras intelligentes lors d'un prochain sommet du G8 ou du G20 par exemple, qui alerteraient automatiquement le centre de contrôle en cas d'attroupement, de mouvements suspects, ou encore d'identification de personne recherchée. Il y a aussi fort à parier que les policiers et les gendarmes n'auront prochainement plus besoin de passer de longues heures à bord d'un véhicule « en planque » dans le cadre d'une surveillance d'activité terroriste ou de trafic de stupéfiants puisque la caméra intégrée au véhicule enverra elle-même une alerte au centre des opérations en cas de détection d'un individu ou d'un véhicule dans la zone surveillée. Il suffira alors au responsable du centre des opérations de décider d'une action éventuelle au vu de la situation.

ALLER PLUS LOIN

www.itea-2-spy.org

emmanuelle.villot@ppl.asso.fr

eric.munier@cassidian.com

Les drones civils, une réglementation émergente

par **CHRISTOPHE MASSET**

P

Positive et attirante par ses aspects ludiques et économiques, en développement constant et avec des perspectives encore difficiles à cerner, l'arrivée massive des drones civils dans notre environnement génère des menaces et des risques que la gendarmerie intègre, dès leur appropriation, dans l'exécution de sa mission de protection des personnes et des biens.

Des objets volants diversement identifiés pour un marché nouveau

Dans le public et jusqu'à un passé récent, le drone était synonyme d'utilisation militaire. Son usage, répandu dans tous les conflits contemporains, médiatisé par les images de "frappes chirurgicales" par des engins pilotés depuis



CHRISTOPHE MASSET

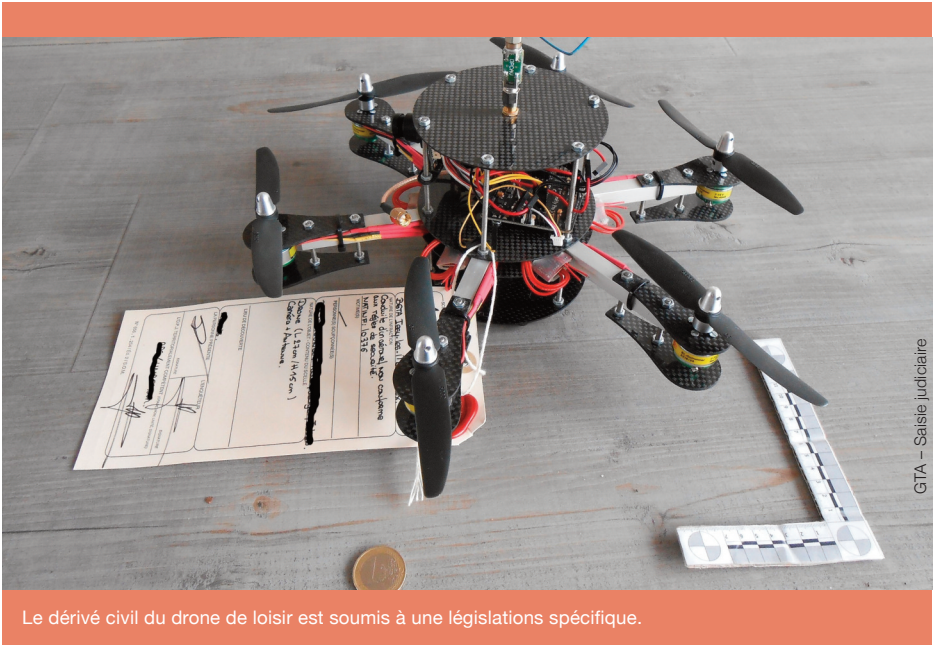
Officier renseignement de la gendarmerie des transports aériens.

des postes de commandement déportés, a marqué les esprits. Mais récemment, l'usage civil des drones s'est développé. La réglementation en cours⁽¹⁾ parle d'aéronef télépiloté.

(1) Deux arrêtés du 11 avril 2012.

Dans l'acception commune, il s'agit de tout objet volant télécommandé de taille réduite.

Ces objets volants s'apercevaient jadis sur les terrains d'aéromodélisme ou privés. Mis en œuvre par de rares spécialistes, ils étaient coûteux et peu performants. Ils se sont peu à peu banalisés. Grâce aux avancées technologiques, notamment la miniaturisation et le développement des aides au pilotage, ils sont devenus accessibles au plus grand nombre. Les progrès réalisés en terme de batteries électriques ont permis d'augmenter de façon significative leur autonomie, ce qui a définitivement conquis le grand public.



GTA – Saisie judiciaire

Le dérivé civil du drone de loisir est soumis à une législations spécifique.

En France, le développement des premières entreprises de drones date seulement d'une dizaine d'années. Aujourd'hui, le marché du drone civil repose sur quelques locomotives : *Delta Drone*, *Delair Tech*, *Infotron*, *Survey Copter* pour les applications professionnelles et *Parrot* pour les loisirs. Aux 25 entreprises concevant des drones s'ajoutent les nombreux opérateurs (345 entreprises) dont la grande majorité est spécialisée dans la réalisation de vidéos aériennes. En juin 2013, une Fédération professionnelle du drone civil (FPDC) a vu le jour. Elle compte désormais 270 membres et les représentants des plus grosses entreprises composent son comité directeur.

À côté des entreprises dont l'enjeu est de développer des applications professionnelles, les particuliers s'équipent également de drones, plus particulièrement pour faire de la vidéo aérienne. Cette utilisation de loisirs offre à tous la possibilité de diffuser des vidéos via les médias sociaux. Il est devenu courant au cours d'une promenade dans les parcs et jardins d'apercevoir ces engins évoluer, suscitant systématiquement la curiosité du public.

Une nouvelle réglementation

Les conséquences de cette évolution ont été rapidement prises en compte par les services de l'Etat puisque la Direction générale de l'aviation civile (DGAC) a permis à la France d'être le premier pays à disposer d'une réglementation nationale

pour les drones civils. Celle-ci repose sur deux arrêtés du 11 avril 2012 et a permis d'offrir à la fois un cadre juridique souple pour les entreprises et de renouveler la réglementation sur l'aéromodélisme qui s'applique aussi à l'utilisation "loisir".

Il convient de retenir que ces deux textes créent quatre scénarios d'emploi (deux en vol à vue et deux en vol hors vue) et sept

(2) Le terme drone n'est jamais cité.

catégories
d'aéronefs

télépilotes⁽²⁾ (deux catégories d'aéronefs télépilotes pour les loisirs et cinq catégories d'aéronefs télépilotes pour le travail aérien). Ces textes prévoient notamment que tout survol d'un rassemblement de personnes dans le cadre d'un travail aérien suppose un agrément spécifique de la DGAC assorti d'une autorisation préfectorale. Cette dernière est aussi requise dans le cadre d'une utilisation de loisirs. Toutefois, l'autorisation préfectorale ne permet pas le vol en surplomb direct des rassemblements de personnes, rigoureusement interdit, tout comme les vols nocturnes, le transport de matières dangereuses et les vols supérieurs à une hauteur de 500 pieds (environ 150 m). Ces différentes interdictions ne peuvent être levées que par une dérogation spéciale et individualisée de la DGAC. Ces règles de sécurité sont parfaitement appliquées par les entreprises les plus importantes et les plus expérimentées. Cependant, certaines entreprises du

CADRE JURIDIQUE

M. ARNAUD GRUT, ingénieur-expert drone au sein du pôle certification/suivi navigabilité et aviation générale de la DGAC, a accepté de nous présenter son analyse sur l'évolution de la communauté des drones :

M. GRUT, après deux ans d'application, quels enseignements tirez-vous de l'application des 2 arrêtés du 11 avril 2012 ?

Avant ces deux arrêtés, cette activité s'était développée sans repères fixes ce qui était préjudiciable d'une part pour les entreprises qui avaient déjà conçu des drones militaires et qui, à partir de 2004-2005, voulaient développer des systèmes de missions civiles, et, d'autre part, pour les aéromodélistes les plus bricoleurs dont certains commençaient à concevoir des aéronefs capables de produire de la vidéo aérienne de qualité. A partir de 2012, un cadre juridique stable a été mis en place permettant le développement économique de cette nouvelle activité auparavant focalisée sur la demande militaire et la demande internationale. Bien sûr, cette réglementation a dans le même temps permis de fixer des règles de sécurité et de bon usage de l'espace aérien pour l'ensemble des utilisateurs.

Après deux ans d'application, la France compte 25 fabricants, 345 opérateurs et une fédération professionnelle regroupant une bonne partie d'entre eux. Aucun accident grave dû à une chute ou à une collision avec un aéronef n'est à déplorer, sachant bien sûr que la multiplication du nombre de drones va multiplier d'autant les risques dans un futur proche.

Quels seront les axes majeurs des prochains arrêtés modificatifs qui devraient entrer en vigueur avant cet été ?

Il ne faut pas attendre de révolution mais des adaptations basées sur les retours d'expérience des nouveaux acteurs et des simplifications favorisant la bonne compréhension des textes. Les discussions restent en cours concernant notamment la modification des scénarios d'emploi et la définition de l'utilisation de loisirs.

secteur ne disposent pas de l'agrément, pourtant obligatoire, pour exercer une activité professionnelle avec un drone. Cette situation conduit les entreprises vertueuses à dénoncer une forme de concurrence déloyale. Depuis septembre 2013, les 18 signalements recueillis par la Gendarmerie des transports aériens (GTA) ont donné lieu à deux enquêtes administratives et seize enquêtes judiciaires qui ont abouti à des rappels à la loi, une COPJ et deux transmissions au parquet en vue de peines d'amende.

Dans ce contexte, la GTA est confrontée à deux problématiques. La première, qui relève du domaine du renseignement, résulte du fait que les militaires de la gendarmerie ne connaissent pas au préalable tous les sites d'emploi des drones. La deuxième tient au fait que l'utilisation "loisir" n'a pas véritablement de statut particulier. Tout utilisateur d'un drone en zone peuplée devrait théoriquement détenir une autorisation préfectorale. Or, quasiment tous les utilisateurs de loisirs ignorent, en toute bonne foi, cette impérieuse nécessité. Sauf cas de mise en danger d'autrui caractérisée, un parquet ne saurait poursuivre ce type de fait. Il existe par conséquent un vide juridique à combler dans un domaine où pour l'instant les abus restent heureusement limités. En l'absence de réglementation et afin d'éviter les procès dans les pays de Common Law, les constructeurs de

drones de loisirs, à l'instar de *Parrot*, se contentent de diffuser quelques conseils de précaution dans leur mode d'emploi.

Des dangers catégorisés

Si aucun accident grave n'a aujourd'hui été recensé en France, il n'en demeure pas moins que les dangers liés au pilotage des drones sont réels. On peut les regrouper en quatre catégories. La première concerne la commission de blessures volontaires et involontaires. Les appareils les plus vendus aujourd'hui sont très majoritairement les multi-rotors. Le danger principal vient d'une perte de contrôle de l'appareil qui peut alors venir heurter une tierce personne. Le risque de blessure peut venir non seulement du choc lui-même mais également des rotors, pouvant briser les os des doigts et lacérer les chairs. Une consultation de la rubrique sécurité du site internet "le dronologue" permet de découvrir quelques illustrations de graves coupures engendrées par des drones. Ce risque s'accroît avec la densité du public (plages, stades, sites extérieurs de spectacles, etc.), sachant que les utilisateurs non-professionnels n'hésitent plus à voler partout, encouragés par la capacité des drones à faire des photos et vidéos aériennes de qualité. Le 11 septembre 2013, la chute d'un drone sur la foule lors d'une fête en Catalogne⁽³⁾, a illustré tous les dangers du survol d'une

(3) <http://www.smartdrones.fr/une-drone-secrase-dans-la-foule-en-catalogne/001381>

foule et la légitimité de l'interdiction en France du vol en surplomb direct. Dans un ordre plus critique, le deuxième point évoqué sera celui d'un usage à des fins de terrorisme. La facilité du pilotage d'un drone en fait un vecteur potentiel d'attaque accessible, dont l'effet réel et surtout médiatique serait particulièrement déstabilisant. La première attaque terroriste avec un ou plusieurs drones ferait très certainement le buzz. La troisième catégorie concerne la sensible atteinte à la vie privée. L'emploi parasite d'un drone au-dessus de propriétés privées risque d'engendrer des conflits de voisinage et d'ouvrir des perspectives à des paparazzi. Enfin, l'utilisation d'un drone aux abords d'une route ou d'un aérodrome pourrait détourner l'attention des automobilistes, motocyclistes, pilotes d'aéronef et perturber leur concentration, indispensable à la maîtrise de leur véhicule.

La souhaitable gestion d'un contrôle des utilisateurs

On peut raisonnablement supposer que le risque majeur n'a pas pour origine l'utilisation professionnelle des drones, cette activité nouvelle étant en quête de crédibilité. Conscients du handicap au développement qu'un accident grave provoqué par un drone engendrerait, les responsables des entreprises fiables sont particulièrement vigilants sur la sécurité. D'ailleurs, soucieuse de préserver la communauté et d'acquérir une vraie

crédibilité, la FPDC annonce vouloir se séparer de ses adhérents qui refusent de se soumettre à la réglementation de la DGAC. Elle reste aussi très attentive à l'encadrement juridique de l'activité et notamment aux prochaines réponses pénales.

Le risque potentiel proviendrait donc plutôt d'une utilisation par des télé-pilotes amateurs pour lesquels aucune formation particulière n'est réglementairement prérequis. Les arrêtés du 11 avril 2012 prévoient en revanche qu'un télé-pilote professionnel de drone ait au minimum réussi l'examen théorique de la licence de pilote privé, de pilote planeur ou de pilote ULM. Cette obligation est assortie d'une déclaration de niveau de compétence délivrée au télé-pilote par l'exploitant après une formation initiale réalisée par lui ou un organisme qu'il a désigné. Les règles de formation des télé-pilotes devraient évoluer vers une professionnalisation accrue dès le printemps 2014 lors de la refonte des deux arrêtés.

L'absence d'accident connu n'a toutefois pas empêché la gendarmerie des transports aériens d'anticiper les conduites à tenir face à de futurs comportements délictueux. Grâce à leurs contacts réguliers avec les services de la DGAC, aux relations nouées avec la FPDC et à la diffusion d'un cadre juridique adapté à la répression, les gendarmes sont prêts à faire face à des utilisations

abusives de drones civils. Ainsi, la DGAC transmet à la GTA l'intégralité des signalements de faits délictueux qui lui sont adressés et la contacte régulièrement pour des échanges relatifs à l'application de la réglementation.

Dans son appropriation progressive de cette problématique nouvelle, la GTA, en concertation avec les services juridiques de la DGAC, centre son action répressive sur l'article 6232-4 du code des transports :

« Est puni d'un an d'emprisonnement et de 75 000 € d'amende le fait pour l'exploitant technique, le propriétaire et, le cas échéant, l'exploitant commercial de :

[...] 4° Faire ou laisser circuler un aéronef dans des conditions d'utilisation non conformes aux règles édictées en vue d'assurer la sécurité par la présente partie ou par les textes pris en application de la présente partie par le ministre chargé de l'aviation civile et relatifs à l'équipement des aéronefs, aux modalités de leur utilisation, à la composition des équipages et à leurs conditions d'emploi. »

Compte tenu de sa formulation assez générale, ce texte est déjà régulièrement utilisé pour les autres aéronefs. Viser exclusivement cet article permettra de créer une jurisprudence favorable à la puissance publique afin de faciliter la répression. La GTA diffusera prochainement à tous les militaires de la

gendarmerie une fiche-guide simplifiée sur la conduite à tenir face à la constatation de visu de l'emploi abusif d'un drone. L'objectif n'est pas de fixer une mission supplémentaire aux militaires des unités territoriales mais de leur donner quelques repères simples pour pouvoir réagir en faisant cesser un vol lorsqu'il présente une dangerosité avérée et mettre en place un traitement juridique adapté.

Le drone alimente beaucoup de fantasmes régulièrement relayés par les médias. Dans le cadre de la protection des personnes et des biens, il est surtout nécessaire de le considérer, de manière pragmatique, comme le support matériel de nouvelles activités qu'il convient de réglementer. A ce titre, le partenariat efficace public-privé soutenu par une répression adaptée permettra à fois un développement économique harmonieux et une utilisation paisible dans le cadre des loisirs.

Transport ferroviaire et cyberspace

par **PATRICK MERVENT**

L

Le trafic ferroviaire a bénéficié de l'évolution générale des technologies. L'implantation, le long des infrastructures et dans les motrices des trains, d'une série de systèmes communicants sécurise les transports de biens et de personnes. La connaissance de ces connexions et des mécanismes correcteurs qu'ils génèrent permet de comprendre la cinématique d'un incident, ce qui peut-être utile aux experts et aux enquêteurs.



PATRICK MERVENT

Dirigeant du groupe télécommunications à Projets-Système-Ingénierie SNCF PACA
Chef d'escadron (rc) GTA
et membre de la réserve citoyenne cyber défense

Le transport ferroviaire réputé sûr

L'histoire mondiale des chemins de fer abonde d'accidents imputables selon le cas à des erreurs humaines, des défaillances

techniques, de mauvaises conditions atmosphériques ou à une combinaison de ces facteurs. L'illustration la plus courante d'un accident ferroviaire est le déraillement ou la collision qui provoquent des dommages souvent importants et graves. Si ces exemples sont en général ceux qui viennent immédiatement à l'esprit, d'autres aléas peuvent entraîner des accidents ne se rattachant pas à ces catégories classiques car un enchaînement de circonstances aboutit parfois à cumuler des faits distincts. Un déraillement peut être causé par un éboulement, suivi d'une collision puis d'une explosion et d'un incendie. En fait, dès l'origine de sa mise en exploitation, le chemin de fer s'est avéré un mode de transport présentant un fort potentiel de risques par les ouvrages qu'il utilise, l'importance et la vitesse des masses qui s'y déplacent. Ils sont souvent découverts empiriquement lorsqu'ils se réalisent.



© oskar_C-

Une connexion machine-infrastructure fiable.

Afin de les diminuer, le risque zéro n'existant pas, les exploitants et les autorités qui les contrôlent se sont efforcés au fil du temps de tirer les leçons des accidents ferroviaires en adoptant les mesures propres à éviter leur renouvellement. C'est pourquoi le chemin de fer est, statistiquement, l'un des moyens parmi les plus sûrs pour se déplacer, bien plus que la voiture individuelle et au même niveau de sécurité que l'avion.

Une signalisation ferroviaire évolutive

Les risques liés à la conception des installations de signalisation sont très

rare. Celles-ci sont conçues pour présenter une situation sécuritaire en cas de défaillance (feu rouge par coupure de courant et feu vert dans le cas inverse). Réglementairement, il est à noter qu'il existe cinq risques ferroviaires : le déraillement, l'obstacle, le nez-à-nez, le rattrapage, la prise en écharpe. Une défaillance humaine ou technique ne suffit pas à elle seule pour aboutir à une situation dangereuse. Des boucles de rattrapage sont prévues : ce sont des dispositifs techniques qui surveillent l'action de l'homme. Afin de le maintenir en état de vigilance, cette surveillance

n'agit qu'en arrière-plan : c'est l'homme qui agit et non l'automatisme. Sur les lignes classiques, hors lignes TGV, les signaux sont implantés à gauche de la voie concernée. Cependant, il peut arriver qu'exceptionnellement les signaux soient implantés à droite de la voie dans le cas par exemple d'Installations Permanentes de contre-sens (IPCS).

Les objectifs de la signalisation sont multiples. On peut cependant les résumer aux points suivants : l'espacement des trains et la protection des circulations dans divers cas comme les croisements de trains ou pour les passages à niveau rail-route. On admet que l'observation correcte des signaux placés latéralement à la voie ne peut être correctement réalisée que si la vitesse n'excède pas 220 km/h. Sur les lignes TGV, il n'est donc plus possible d'implanter des signaux classiques et on a recours à une signalisation en cabine. Tous les engins moteurs qui doivent circuler sur les lignes à grande vitesse et dans le tunnel sous la manche sont équipés de la Transmission Voie Machine (TVM). Les signaux sont remplacés le long des voies par des repères et des jalons et en cabine par des indications de vitesse limite. De même, les indications de sectionnement et de passage pantographe baissé sont reportées en cabine.

Cette signalisation en cabine est réalisée techniquement par l'envoi d'informations

continues au train par les rails et par des balises d'informations ponctuelles. En outre, un contrôle de vitesse est réalisé qui oblige le mécanicien à respecter les indications en cabine et provoque le cas échéant le freinage du train.

Signalisation ferroviaire et cyberspace

L'avenir en matière de signalisation ferroviaire passe par l'ERTMS/ECTS (*European Rail Traffic Management System/ European Train Control System*) qui est destiné à remplacer les 27 systèmes de signalisation ferroviaire en service en Europe. Lorsqu'on sait que le TGV Thalys, qui relie Paris, Bruxelles, Cologne et Amsterdam, doit être équipé de sept systèmes différents, entraînant un surcoût de 60 % lors de la fabrication de chaque rame, on comprend le besoin de norme unique.

Par ailleurs, la standardisation entraînée par la mise en place d'ERTMS permet d'alléger la formation spécifique des conducteurs conditionnant l'obtention du certificat européen. Cette nouvelle norme permet le contrôle de vitesse en sécurité grâce à un échange d'informations entre le sol et les trains. Il peut se faire

BIBLIOGRAPHIE

www.uic.org
www.synerail.com
www.rff.fr

ponctuellement par balises, il s'agit d'ERTMS niveau 1, ou en continu par radio communications GSM-R (*Global System for Mobile Communications – Railway*). On parle alors d'ERTMS niveau 2.

Outre l'ERTMS, le GSM-R permet de nouveaux services par rapport à l'ancien système de radio sol-train avec une gestion des différents types d'appels par priorité, l'appel d'urgence étant un appel prioritaire sur toutes les autres communications. Le GSM-R a fait l'objet en France d'un partenariat public privé (PPP) entre RFF et SYNERAIL et utilise une infrastructure indépendante du réseau GSM grand public. Ce dernier assure aujourd'hui la gestion et la maintenance du réseau GSMR pour le compte de RFF. En GSM, la carte SIM fournit des informations pour se connecter au réseau. Un utilisateur peut se protéger contre une utilisation piratée en activant le code PIN. Dans un train la carte SIM est associée à un engin moteur et pas à un utilisateur. Plusieurs conducteurs peuvent se succéder dans le train dont ils doivent connaître le code PIN. Cette situation implique un parc avec 2 sortes de cartes SIM en GSM-R : des cartes pour les téléphones portables standards et des cartes pour les engins moteur avec dans ce cas une authentification calculée avec un algorithme pour la clé secrète. Cette phase d'identification n'est pas

nécessaire avec les autres téléphones portables standards. La gestion des cartes SIM doit être faite avec ou sans authentification. Le GSM-R est basé sur la norme GSM 2G /GPRS (*General Packet Radio Service*) avec un algorithme A5/1 et un chiffrement à 64 bits pour crypter les communications, même si les révélations "Snowden" sur les écoutes de la NSA prouvent qu'on peut, sans avoir obtenu les clés de chiffrement, décoder les communications GSM. La vulnérabilité la plus vraisemblable reste le processus de changement des clés de chiffrement car si elles sont chargées sur un support physique pour être transmises aux personnes autorisées, elles pourraient être piratées pour mener une attaque par déni de service. La conséquence d'une telle attaque serait immédiate sur l'exploitation ferroviaire et pourrait entraîner des retards de trains car, en cas de dysfonctionnement de la signalisation, la marche à vue est imposée à 30 km/h maxi. Le palliatif à cette problématique est la mise en place d'un centre de gestion qui prend en charge à distance la création, l'échange et la mise à jour automatique des clés d'authentification pour éliminer toute opération manuelle.

L'ERTMS niveau 1 est conçu pour les lignes classiques déjà équipées de signalisation latérale et de détecteurs de train comme les circuits de voie ou les compteurs d'essieux. Les balises sont installées pour transmettre des

informations vers le centre de commande et le train. Les informations des balises sont utilisées pour calculer la vitesse maximale. En revanche, l'ERTMS niveau 2 ne nécessite pas de signaux latéraux mais toujours l'utilisation d'un système de détection des trains au sol pour localiser un train aval et transmettre l'information au centre radio RBC (*Radio Block Center*) qui gère l'espacement entre deux circulations. Les données de signalisation ne sont plus transmises par balises mais en permanence par le réseau GSMR qui permet une utilisation fonctionnelle sans coupure de communication jusqu'à une vitesse de déplacement théorique du train de 500 km/h. Le train maintient ainsi en permanence une connexion numérique par modem vers le centre. Une connexion du modem perdue, il s'arrête automatiquement. En situation normale, le train suiveur reçoit à n'importe quel moment une nouvelle autorisation de circulation par l'intermédiaire de la liaison GSM-R. Dès que le train aval libère un canton, le poste central de commande reçoit l'information correspondante du sol par liaison radio pour le train suiveur. Le train communique constamment sa position qu'il détermine avec un odomètre au centre de contrôle qui lui communique en retour les actions à effectuer (vitesse, arrêt...). L'ERTMS niveau 2 rend disponible immédiatement l'information libératoire pour le train suiveur et contribue ainsi à augmenter la fluidité.

C'est la différence par rapport à la signalisation conventionnelle où une demi-minute est parfois nécessaire pour libérer un aiguillage alors que le train est déjà loin. Depuis le 17 décembre 2013, la ligne LGV Est-Européenne fonctionne avec l'ERTMS niveau 2 superposé à la TVM entre Vaires en Seine-et-Marne et Baudrecourt en Moselle.

Un système clos et sécurisé

Le GSM-R *via* GPRS peut s'interconnecter avec un réseau IP. Pour le ferroviaire ce réseau basé sur l'IP, appelé INFRANET, n'est pas relié à Internet pour se prémunir des cyberattaques du WEB. Avec un backbone (artère principale) sur fibres optiques posées le long des voies ferrées et 70 routeurs, l'INFRANET offre aux applications un service d'échange fiable de données avec un service de transmission mutualisé MPLS (Multi Protocol Label Switching). La supervision et l'administration de l'ensemble des équipements constitutifs du réseau INFRANET/MLPS sont entièrement centralisées à PARIS. Le protocole MPLS permet la création de réseaux privés virtuels reposant sur des classes de services (CoS) afin de garantir des délais d'acheminement pour que le trafic important soit traité avec la priorité adéquate. INFRANET supporte entre autres les applications de type MISTRAL (Module Informatique de Signalisation, de Transmission et d'Alarme) pour les

nouvelles générations de postes d'aiguillage informatiques nécessaires au projet CCR (Commande Centralisée du Réseau) qui consiste à rassembler la commande-contrôle des 1 500 postes d'aiguillage et la régulation des circulations dans seize centres, supervisés et coordonnés par un centre national.

La migration des systèmes ferroviaires vers l'IP, leur interconnexion ou tout simplement leur connectivité à internet restent prohibées pour le moment. Toutefois, l'évolution technique fait converger les métiers de la signalisation, des télécommunications et de l'informatique. Il importe maintenant d'homogénéiser les analyses de risques cyber avec les analyses de risques classiques pour que le risque cyber soit considéré à sa juste hauteur et soit comparable aux autres.

La sécurité ou des moyens d'actions adaptés aux situations critiques

par LAURENT DENISOT

L

La gestion de crise, l'appropriation de grands événements mobilisant des milliers de participants sur des sites parfois immenses, la nécessité d'assurer l'ordre public lors de manifestations festives ou culturelles suscitent une demande de solutions qui révolutionnent l'approche de la sécurisation de ces rassemblements. Elles doivent fournir une palette d'outils facilitant l'acquisition de l'incident et la mobilisation des ressources humaines et matérielles à affecter tout en permettant d'en reconstituer la cinématique.



LAURENT DENISOT

CEO chez Egidium
Technologies
Réserviste citoyen de la
gendarmerie nationale

Le monde actuel devient de plus en plus incertain. La multiplicité des menaces les rendent de plus en plus difficiles à traiter : terrorisme, cybercriminalité, délinquance urbaine,

trafics illicites, immigration illégale, catastrophes naturelles et industrielles. La prise de décision rapide et efficace est un enjeu majeur dans un contexte où l'information circule de plus en plus en temps réel. Face à ces risques et à ces menaces, la demande de produits, de solutions et de services devient stratégique. Cette problématique globale démontre l'importance d'une convergence « sécurité privée - sécurité électronique » et l'intérêt d'intégrer l'ensemble des moyens disponibles (vidéoprotection, moyens de communication, géolocalisation...)

La convergence sécurité privée et sécurité électronique

La loi de 1983, la première réglementant les activités privées de sécurité en France, donnait au secteur privé un champ d'action bien délimité dont les axes majeurs et valorisants étaient principalement le transport de fonds et l'aéroportuaire. Aujourd'hui le besoin a évolué et ce marché connaît un fort ralentissement.



Société Egilium – Valensi

Un outil intégré pour une supervision intelligente.

En 2011, la structuration de cette profession, la mise en place d'une nouvelle organisation et la création d'une nouvelle image est devenue nécessaire

(1) Le Cnaps est un établissement public administratif placé sous tutelle du ministère de l'Intérieur. Il est chargé de l'agrément, du contrôle et du conseil des professions de sécurité privées.

voire cruciale. Le Cnaps⁽¹⁾, Conseil National des Activités Privées de Sécurité, a été créé. Il est né

d'une volonté commune de l'Etat et des acteurs de ces métiers de moraliser et de professionnaliser ce secteur en accord avec les pouvoirs publics et sous leur contrôle. Certains auteurs estiment que l'on arrive de fait à une privatisation partielle de la sécurité. Il est à noter qu'en France, l'Etat a validé la privatisation d'une partie des missions de sécurité par la loi d'orientation et de programmation sur la sécurité de 1995 en reconnaissant le gardiennage, la vidéoprotection, les audits et les conseils en gestion du risque comme des activités participant à la production de sécurité collective. L'examen des dispositions et des pratiques montre qu'il ne s'agit pas d'un transfert total des fonctions de l'État au secteur privé mais plutôt d'une délégation contrôlée de certaines d'entre elles.

La problématique de l'appropriation des grands événements

La sûreté et la sécurité sont les principales priorités des organisateurs d'un grand événement. Prenons l'exemple d'un grand salon comme celui de l'Aéronautique qui présente des caractéristiques de criticité. Le salon du Bourget à Paris est un événement de l'industrie aérospatiale qui y présente ses plus récentes technologies et du matériel connexe, y compris les moteurs d'avion et la technologie des satellites. C'est une référence du monde aéronautique et spatial. En 2013, il a été inauguré par le Premier ministre M. Jean-Marc Ayrault. Le président de la République l'a visité et onze ministres français ont été présents durant l'événement. Ont aussi participé à ce salon le président de la République du Venezuela, le Premier ministre d'Ukraine, le vice-premier ministre de Roumanie, 51 ministres étrangers et 45 chefs d'état-major.

Ce salon, c'est : 132 000 m², plus de 315 000 visiteurs, 285 délégations venant de 102 pays, 192 000 m² d'exposition des aéronaves, 150 aéronaves présents parmi lesquels 40 en présentation en vol. Il faut ajouter à cet ensemble 340 unités chalets et 2 215 exposants venus de 44 pays. La gestion de la sécurité de cet événement illustre parfaitement la nécessité de la convergence entre la sécurité privée et des offres logicielles dédiées à ce métier. En effet, elle a été confiée par l'organisateur, le Salon international de l'aéronautique et de l'espace, pour la deuxième fois consécutive, à deux sociétés complémentaires. La société Maori, qui avait en charge le dispositif humain et opérationnel, s'est

appuyée sur un des produits informatiques développés par la société « Egidium Technologies ». Cette solution installée au sein du poste de commandement central et de gardiennage, a permis au directeur des opérations de garder une vision globale de la sécurité du site tout au long de l'événement.

Une offre technologique à forte plus-value

Egidium Technologies est une société française qui développe et commercialise des solutions logicielles dédiées à la sûreté et à la sécurité des sites sensibles. Forte de 15 années de recherche menées dans l'industrie de défense, elle demeure à ce jour le seul éditeur logiciel européen indépendant sur le marché du PSIM (*Physical Security Information Management*). Les technologies développées mettent à la disposition des opérateurs un outil intuitif de synthèse d'alarmes, d'aide à la décision et de coordination des interventions lors de grands rassemblements sur un seul poste

de commandement et de supervision⁽²⁾. Cette solution offre un traitement et une traçabilité d'incidents permettant de mieux appréhender les diverses situations et d'assurer la sécurité des visiteurs et participants de manière optimale. En effet, la gestion de la sécurité lors d'un événement recevant du public, des professionnels et ou des autorités politiques est décisive compte tenu des multiples menaces potentielles : le feu, une défaillance structurelle, un mouvement de foule, le vol, une intrusion, une manifestation et même un attentat. Tout incident majeur ou mineur

peut avoir des conséquences sérieuses et dommageables.

Une forte capacité d'acquisition des situations

La solution déployée est constituée d'un ensemble de modules logiciels. Grâce à leur architecture distribuée et à leur capacité d'intégration avec tous les types de capteurs et de systèmes de sécurité, la facilité d'intégration et le temps de déploiement sont considérablement réduits. Cet outil de pilotage, qui agit comme un chef d'orchestre, permet la gestion de plusieurs incidents en simultanément.

Il permet une visualisation en 3D du site à surveiller. Il fournit en temps réel des informations opérationnelles, une localisation automatique d'incidents par les capteurs sur la 3D et une remontée des alertes en temps réel. Une vérification de l'information par les caméras les plus adaptées permet de lever le doute sur une alarme ou un lieu.

Une fonctionnalité recherchée par les clients, satisfaite par le produit mis à sa disposition, est la localisation en temps réel du dispositif déployé (employés, véhicules) par l'intermédiaire de toutes les technologies de géolocalisation indoor et outdoor. Cela autorise une optimisation de la réponse opérationnelle lors de la gestion d'un incident nécessitant la mobilisation de moyens dispersés sur le site ou de nature différente.

Le management de la cinématique de l'incident est soutenu par l'établissement d'une main-courante sur les incidents qui sont horodatés et localisés dans l'espace. Les occurrences sont enregistrées dans une

(1) La solution Egidium port le nom « d' Event Monitor »

de commandement et de supervision⁽²⁾.

base de données, consultable à tout moment qui permet de reconstituer le contexte et assure une traçabilité des phénomènes observés par le système.

Cette solution s'appuyant sur la technologie est un outil qui permet à l'homme derrière ses écrans de gérer intelligemment toutes les situations critiques par sa vision globale et en temps réel. L'outil, facile et intuitif, flexible et évolutif, a été conçu pour répondre aux besoins de ses clients et ne nécessite qu'une courte formation des opérateurs.

Une intégration dans un dispositif général de sécurité

La technologie proposée recherche dès sa phase conceptuelle une réduction du temps de réaction du superviseur, une qualification de l'incident crédible et intelligible, l'affectation aux phases d'analyse et d'intervention d'équipes compétentes. Elle donne également les moyens d'assurer une alerte et la transmission d'informations probantes aux différents organismes concernés par une coproduction de sécurité sur le site : police et gendarmerie nationale, SDIS, protection civile, agents d'intervention, etc. La technologie permet d'avoir l'information en temps réel, d'anticiper les menaces, d'identifier et de suivre des groupes ou un individu à risque pour l'ordre public. C'est aussi un outil de dissuasion et de coordination des actions. Il permet d'avoir une visibilité globale du terrain et de coordonner et calibrer les actions à mettre en œuvre pour des événements qualifiés. Un avantage juridique certain est procuré par la capacité d'assurer une traçabilité

spatio-temporelle optimale des incidents. Les supports numérisés peuvent en cas de besoin servir de base à une expertise judiciaire ou à des organismes techniquement habilités à les analyser.

Cette solution peut être proposée pour les grands salons, mais aussi pour les stades, les festivals, les parcs d'attraction ou tout grand rassemblement. Il est à noter qu'à partir d'une plate-forme logicielle standardisée les évolutions sont possibles. Les grands salons n'ont pas hésité à inclure dans leur demande de prestations le comptage des entrées-sorties, fonctionnalité qui a été intégrée dans le dispositif logiciel.

Les entreprises françaises de petite taille sont reconnues comme des experts de hauts niveaux dans ce domaine et commencent à exporter leurs solutions. Récemment, grâce au soutien apporté par BPIFRANCE et UBIFRANCE, Egidium a signé son premier contrat en Chine pour la mise en place d'un dispositif de sécurité innovant sur le site d'accès à la Cité Interdite, à Pékin. Il est à souligner, que face à ce marché extrêmement fragmenté, a été créé par 4 syndicats, FIEEC, GICAN, GICAT et GIFAS, le conseil des Industries de Confiance de la Sécurité, le CICS.

Ce Conseil a été conçu pour créer une organisation plus étroite entre les grands groupes et les PME, dont l'objectif est de mobiliser les compétences de cette filière pour développer des activités positionnées sur un marché européen et mondial en forte croissance.

Evaluation comportementale

des personnes et sûreté aérienne

par **MICKAËL TEROSIER**

L

La multiplication des actes malveillants perpétrés suivant des modes opératoires toujours plus innovants a entraîné un changement progressif dans la gouvernance de la sûreté aérienne. Aujourd'hui, les Etats se tournent vers de nouvelles mesures de sûreté plus efficaces. L'évaluation comportementale des personnes, principalement des passagers, est l'une d'entre elles.

Une menace protéiforme et mondiale

La sûreté du transport aérien peut être définie comme la protection de l'aviation

civile contre les actes d'intervention illicite.

Cet objectif est réalisé par une combinaison de mesures ainsi que de moyens humains et matériels.



MICKAËL TEROSIER

Officier de gendarmerie enseignant à l'Enac (Ecole nationale de l'aviation civile)

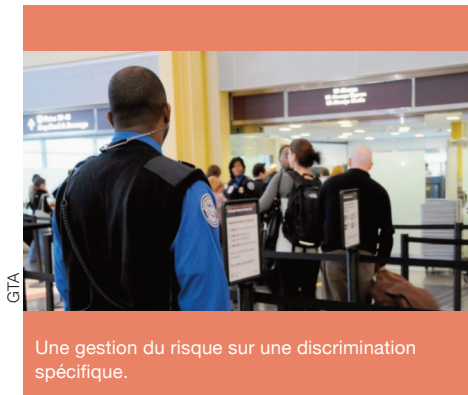
Depuis les événements du 11 septembre 2001, plusieurs autres actes malveillants ont été perpétrés. Ces attaques marquent le début d'une ère nouvelle dans l'histoire de la sûreté du transport aérien caractérisée par la multiplication d'actes pouvant être qualifiés de terroristes au sens de notre

(1) Article 421-1 du Code pénal.

(2) Apparu en 1966, sa portée est faible (3 à 4 km) mais son système de guidage infra rouge et sa très grande mobilité (le système est portable à dos d'homme) en ont fait une arme redoutable et quasiment indétectable avant son lancement.

code pénal⁽¹⁾. A titre d'exemple, le 22 décembre 2001, Richard Reid, un citoyen britannique, tente de détruire un aéronef en vol au moyen d'un engin

explosif dissimulé dans ses chaussures. Le 28 novembre 2002, à Mombasa au Kenya, des individus appartenant à la mouvance Al-Qaïda lancent 2 missiles SAM-7⁽²⁾ en direction d'un avion charter israélien mais les deux missiles manquent leur cible. Le 10 août 2006, les services britanniques de Scotland Yard parviennent à déjouer un projet d'attaques coordonnées de grande



GTA

Une gestion du risque sur une discrimination spécifique.

envergure visant 10 avions de ligne desservant les Etats-Unis. L'attaque devait se faire au moyen d'explosifs liquides. Enfin, le 25 décembre 2009, Umar Farouk Abdulmutallab, un jeune Nigérian, tente sur un vol Amsterdam-Detroit de la compagnie américaine Northwest de déclencher un engin explosif improvisé non métallique dissimulé dans ses sous-vêtements.

Ces actes malveillants rappellent que le transport aérien reste une cible de choix pour les terroristes. De plus, le modus operandi de plus en plus innovant des auteurs de ces actes met en évidence les limites de la gouvernance actuelle de prévention de la malveillance à l'encontre du transport aérien. Comme le souligne le rapport d'information parlementaire présenté par MM. les députés Goldberg et Gonzales en 2011, « *si la diversité et le caractère massif des mesures actuelles d'inspection-filtrage ont un effet dissuasif, celles-ci doivent néanmoins être sensiblement améliorées pour tenir compte des différents niveaux de risque que présentent les passagers* ». Ces préconisations sont à l'opposé du dispositif

actuel de sûreté aéroportuaire. En effet, d'un coût estimé à plusieurs centaines de millions d'euros, la sûreté du transport aérien français est constituée d'une accumulation de strates successives de mesures, souvent prises en réaction à des actes malveillants. A titre d'exemple, les mesures de protection des portes de cockpit ont été prises suite aux attaques kamikazes du 11 septembre 2001. Les mesures de restriction d'emport en cabines des liquides, aérosols et gels ont été adoptées suite aux attentats manqués à l'explosif liquide de 2006, etc. Or, malgré des niveaux de protection de plus en plus nombreux, des actes malveillants sont encore commis. Certains osent même comparer le dispositif de sûreté à une « *ligne Maginot* ».

Les carences révélées par les tentatives successives d'attentats ont conduit les principaux acteurs du transport aérien à repenser le concept global de la sûreté. Les réflexions menées, notamment lors de la Conférence de haut niveau sur la sûreté de l'aviation à Montréal en septembre 2012, ont poussé les gouvernants à promouvoir un système de sûreté plus efficient. La Direction générale l'aviation civile (DGAC), sous l'égide du Secrétariat général de la défense et la sécurité nationale (SGDSN), expérimente de nouvelles techniques pour répondre à cet objectif. L'une des principales mesures est « *l'évaluation comportementale des personnes* » qui concerne aujourd'hui les passagers. Très ambitieuse, elle s'inscrit pleinement dans le concept de « *sûreté du futur* » fondé sur un traitement différencié du passager.

L'origine de la démarche

L'évaluation comportementale est une technique qui consiste à détecter des

passagers potentiellement mal intentionnés, susceptibles de présenter un risque pour la sûreté de l'aviation civile, en s'appuyant sur la détection de signes involontaires de stress, de peur ou de dissimulation. M. Jean-Pierre VEYRAT, expert en morphogestuelle comportementale, parle de gestuelle « *non verbale* », autrement dit l'ensemble des mouvements corporels inconscients, d'où qu'ils proviennent – corps, mains, tête – qui émergent lors d'un échange. Ils sont émis par l'individu à son insu, sans intention signifiante pour lui-même, mais ils s'avèrent extrêmement révélateurs pour l'observateur, surtout dans les moments de tension.

En décembre 2008, sous l'impulsion du SGDSN, la DGAC a démarré le programme expérimental d'analyse comportementale des passagers rebaptisé depuis « *évaluation comportementale des personnes* » dans les projets de textes réglementaires. Cette méthode a pour l'heure été expérimentée en France sur les aéroports parisiens (Paris-Charles de Gaulle et Paris-Orly) en amont des postes d'inspection filtrage pour détecter des passagers présentant des signes anormaux du comportement. Dès l'origine, l'expérimentation a été menée avec le concours des services compétents de l'État, dont la Police aux frontières (PAF) et la Gendarmerie des transports aériens (GTA). Le projet français d'évaluation du comportement des personnes a été élaboré à partir du programme américain SPOT (« *Screening passengers by observation techniques* » – contrôle des passagers au moyen de techniques

d'observation). Après une présentation théorique et pratique du programme

(3) Agence fédérale américaine chargée de la sécurité des transports qui a été créée au lendemain des événements du 11 septembre 2001. Elle est rattachée au ministère de la Sécurité intérieure. Elle est notamment responsable de la sûreté du transport aérien aux États-Unis.

SPOT par des fonctionnaires de la TSA⁽³⁾ (*Transportation Security Agency*), la DGAC et l'Enac (Ecole nationale de l'aviation civile) ont bâti le

programme français d'analyse comportementale des passagers. Les services de l'État, comme la PAF et la gendarmerie des transports aériens, y ont grandement contribué. Les officiers du bureau "sûreté" de l'état-major de la GTA, tous auditeurs "sûreté", ont activement participé aux travaux de cette expérimentation en apportant leur expertise technique, en participant aux jurys d'évaluation des agents chargés de la détection du comportement et en siégeant aux comités de suivi du projet.

Evaluation comportementale des personnes et « profiling »

Il importe de rappeler que l'évaluation comportementale des personnes est différente du « profiling » – ou profilage criminel – méthode qui permet à des enquêteurs spécialistes de la psychologie de déterminer a posteriori le profil psychologique d'un criminel, souvent récidiviste (c'est-à-dire après que des faits ont été commis) à partir d'indices recueillis sur une scène de crime. *A contrario*, l'analyse comportementale des personnes, plus proactive, est une technique visant à repérer et identifier des individus avant que ceux-ci ne commettent des actes d'intervention illicite. Si les mesures de sûreté actuelles ont essentiellement pour

but la recherche et la détection d'articles prohibés, donc la recherche de l'élément matériel des actes malveillants, l'analyse comportementale vise quant à elle la détection de mauvaises intentions (l'élément moral de l'acte malveillant).

La méthode, qui reste confidentielle, se déroule en plusieurs étapes. En substance, cette technique, déployée stratégiquement après une évaluation des risques, permet de cibler des passagers présentant un risque potentiel. Ces derniers subissent alors des mesures de sûreté complémentaires et réglementaires conduites par des agents de sûreté dûment formés. Il convient de rappeler que ces personnels en charge de la détection du comportement sont des agents de sûreté de sociétés privées qui agissent sous le

(4) L'article L. 6342-4 du code des transports dispose que les opérations d'inspection-filtrage des personnes, des objets qu'elles transportent et des bagages ainsi que les opérations d'inspection des véhicules peuvent être réalisées, sous le contrôle des officiers de police judiciaire et des agents des douanes, par des agents de nationalité française ou ressortissant d'un Etat membre de l'Union européenne, désignés par les entreprises ou organismes mentionnés à l'article L. 6341-2 ou les entreprises qui leur sont liées par contrat.

contrôle des services compétents de l'Etat (police ou gendarmerie).⁽⁴⁾ Cette méthode est strictement fondée sur la recherche de signes anormaux du comportement et garantit ainsi toute dérive vers des pratiques

discriminatoires.

Une mesure de sûreté d'avenir

De nombreux États recourent aujourd'hui à l'analyse comportementale des passagers (Etats-Unis, Israël, Grande-Bretagne, Suisse, etc.). En France, la mise en œuvre de l'évaluation comportementale des personnes sur les aéroports de province est

imminente. La police aux frontières et la gendarmerie des transports aériens assureront le contrôle de la mise en œuvre de la mesure et interviendront le cas échéant en cas de doute avéré sur une personne.

Cette technique illustre parfaitement le changement en cours dans la manière de concevoir la sûreté en différenciant les mesures de sûreté appliquées au passager selon le risque qu'il présente. Depuis août 2011, les Etats-Unis expérimentent sur plusieurs aéroports un dispositif de sûreté fondé sur une analyse du risque (« risk-based security ») qui consiste notamment en la mise en place de mesures de sûreté adaptées, ciblées et parfois aléatoires définies grâce à des évaluations de la menace faites en temps réel. L'évaluation comportementale est un des outils utilisés dans le cadre de ce concept.

La nouvelle gouvernance qui se met en place veut concilier sûreté, facilitation et moindre coût. De plus, ce dispositif consacre l'importance du facteur humain dans la lutte contre les actes malveillants visant le transport aérien aux côtés d'équipements de plus en plus perfectionnés. Enfin, convaincus par cette technique, certains États comme les Pays-Bas recourent largement à l'analyse comportementale dans le côté « ville » des aéroports (partie publique et donc librement accessible des plateformes aéroportuaires) afin de détecter non seulement des personnes pouvant potentiellement nuire au transport aérien mais également des auteurs d'infractions de droit commun.

Monnaies virtuelles

l'exigence du régalien pour créer la confiance ?

par JEAN-LUC DELANGLE

L

Le bitcoin restera l'une des vedettes de l'année 2013 avec l'envolée de son taux de change multiplié par près de 100 en 12 mois, suscitant d'ailleurs la multiplication de monnaies virtuelles concurrentes. Ces monnaies virtuelles se légitiment dans la contestation de l'État et de l'imposante réglementation bancaire et financière. Pourtant, c'est cette réglementation qui pourrait devenir indispensable à leur pérennité.

La monnaie, une définition plus économique que juridique

Définir la monnaie semble trivial tant elle fait partie du quotidien. Comme l'écrivait, voilà quelques décennies, l'économiste américain John Kenneth Galbraith, l'argent concerne tout le monde, ceux qui en ont comme



JEAN-LUC DELANGLE

Réserviste citoyen, centre de recherche de l'EOGN.

ceux qui n'en ont pas. Cependant, inutile de feuilleter le Code monétaire et financier : le droit français n'en donne aucune définition. Tout au plus, découvre-t-on que le Traité de Maastricht réserve à

(1) Article 106 du Traité de Maastricht

(2) Cours légal : les billets ou pièces ayant cours légal ne peuvent être refusés par un créancier ; toutefois, les montants pouvant être réglés de cette façon sont limités par la loi (art L 112-6, D 112-3 et D 112-4 du Code monétaire et financier)

(3) Pouvoir libératoire : qui éteint une dette

la Banque centrale européenne le monopole⁽¹⁾ de l'émission des seuls billets de banque à avoir cours légal⁽²⁾. Ces billets ne peuvent donc être refusés en règlement

de dettes libellées en euros. Quoique ... il existe des dispositions juridiques stipulant l'obligation de régler par un moyen traçable au delà d'un seuil déterminé. Le Code monétaire et financier se limite à préciser quel est le pouvoir libératoire⁽³⁾ des formes monétaires exprimées en euros.

Pour les économistes, les choses sont mieux cernées et ce, depuis longtemps.

En effet, dès le IV^e siècle avant notre ère, Aristote dans son « *Éthique à Nicomaque* » avançait que la monnaie était un instrument d'échange, un étalon de valeur et une réserve. Cette vision a certes suscité de nombreux débats, mais sans véritable remise en cause. Le prix

(4) Prix Nobel d'économie en 1976

Nobel d'économie
Milton Friedman⁽⁴⁾

rappelait qu'au final, « *n'importe quel bien susceptible de fournir une garantie provisoire sur le pouvoir d'achat général peut faire office de monnaie* ».

L'histoire de la monnaie est aussi celle de l'innovation pour une plus grande simplification. A l'origine, on a pu se servir de troupeaux. Ainsi le mot « *pecuniaire* » qui désigne ce qui est relatif à l'argent vient-il du latin *pecus* signifiant bétail et le nom de la monnaie indienne, la roupie, provient d'un mot sanskrit ayant la même acception. On leur a préféré rapidement les métaux précieux, qui offrent l'avantage d'être pérennes et divisibles. Ces métaux étaient toutefois lourds et présentaient des risques à être conservés. Se sont

(5) La masse monétaire se mesure avec 3 grandeurs (des agrégats) appelés M1, la monnaie immédiatement disponible, M2 et M3, ces 2 dernières intégrant des dépôts un peu moins disponibles à chaque fois mais restant aisément convertibles sous une forme monétaire. En novembre 2013, les pièces et billets représentaient un peu moins de 17 % du total de M1 (contre 83 % pour les dépôts bancaires) et 9 % du total de M3 (contre 91 % pour les dépôts bancaires).

imposés au fil du temps les billets de banque, d'abord convertibles en or puis inconvertibles puis la monnaie scripturale, de simples écritures dans les livres comptables des

(6) La directive européenne 2009/110/CE du 16 septembre 2009 définit la monnaie électronique comme une « *valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique* ».

banques⁽⁵⁾, et enfin la monnaie électronique⁽⁶⁾, des impulsions numériques, détenues sur des supports *ad hoc* : cartes, clés USB ou disques d'ordinateur.

Mais ces monnaies –

et ce très tôt dans l'histoire – ont une spécificité forte : elles sont devenues la marque, le symbole du souverain. Battre monnaie est la caractéristique du pouvoir régalien.

La création monétaire, un phénomène privé qui devient même contestataire

Ce principe régalien suscite toujours d'importants débats chez les économistes. Dans les faits, la création monétaire est largement privée. En effet, pour l'essentiel, la monnaie naît à l'occasion de l'octroi d'un crédit

(7) La création monétaire résulte d'un simple jeu d'écriture : lorsqu'un client bénéficie d'un crédit, ses disponibilités sur son compte, comptabilisé au passif du bilan de la banque - et donc son pouvoir d'achat - augmentent ; la contrepartie figure à l'actif dans la rubrique « prêts accordés à la clientèle ».

bancaire⁽⁷⁾, principalement par les banques commerciales, le plus souvent privées⁽⁸⁾. De même, l'or et l'argent n'ont jamais été créés par un État, le souverain se limitant à apporter sa marque.

(8) L'article 101 du Traité de Maastricht et sa transcription dans l'article L 141-3 du CMF interdisent respectivement à la BCE et à la Banque de France de prêter à une entité publique.

Le pouvoir régalien s'exprime en fait au travers des actions de contrôle, de

réglementation et de régulation de l'activité monétaire. L'estampille du souverain sur les pièces en métal garantissait le poids et la qualité du métal. On comprend alors que Philippe Le Bel réduisant leur poids de métal précieux ait pu passer pour un faux monnayeur. L'activité bancaire aujourd'hui s'effectue sous la surveillance de la Banque centrale européenne. Celle exécute une mission

(9) Article 108 du Traité de Maastricht et L 141-1 du CMF (pour la Banque de France) ; l'objectif assigné à la BCE par la loi est prioritairement la maîtrise de l'inflation.

(10) La plus ancienne encore utilisée est le *wir suisse*, qui date des années 1930. Le phénomène des monnaies alternatives en France semble démarrer dans les années 90.

définie par la loi⁽⁹⁾, avec des moyens définis par la loi. Elle est ainsi fort proche d'une autorité administrative indépendante. Cette réglementation garantit des droits

aux utilisateurs de la monnaie souveraine.

Cependant fleurissent depuis quelques années⁽¹⁰⁾ des monnaies privées appelées « *alternatives* » ou « *parallèles* ». Limitées à une aire géographique donnée, rejetant le système financier et la mondialisation chargés de tous les maux, voire l'État, elles ont pour vocation de favoriser la consommation locale, au risque d'ailleurs d'un repli sur soi. Les formes en sont multiples mais elles se caractérisent par une convertibilité limitée : les particuliers peuvent acheter la devise locale contre euro à un cours fixe mais, devenant « captifs », ne peuvent s'en défaire qu'en la dépensant chez les commerçants qui l'acceptent⁽¹¹⁾. Ces monnaies locales

(11) Les entreprises peuvent avoir la possibilité de la convertir en monnaie souveraine moyennant le règlement d'une commission.

(12) Ingénieur polytechnicien ; la citation est tirée de « *méditations sur le réel et le virtuel* » L'Harmattan ; 2004 ; le terme « *qualité* » est à prendre dans le sens de « *propriété* ».

restent toutefois émises sous le contrôle des autorités monétaires, les dispositions législatives existantes s'y appliquant.

Toutefois, la monnaie ne pouvait bien évidemment pas passer à coté du phénomène cyber, avec la manifestation en 3 vagues des monnaies virtuelles. Il convient ici de clarifier une terminologie qui n'est pas véritablement fixée. Le terme « virtuel » correspond pleinement à l'acception qu'en donne Denis Berthier⁽¹²⁾ : « *est virtuel ce qui sans être réel, a, avec force et de manière pleinement actuelle, les qualités du réel* ».

A l'origine, elle désigne les simulacres de monnaie utilisés au sein des métavers, ces sites à la fois jeux de rôles multijoueurs et réseaux sociaux, dont l'archétype est le *lindendollar* du site *Second Life*. Les monnaies virtuelles sont cependant très vite sorties de l'univers ludique. Ainsi, le *lindendollar* s'achète-t-il aujourd'hui contre des devises souveraines.

La seconde vague a été constituée par des dispositifs alliant système de paiement centralisé et monnaie. C'est ainsi qu'ont fonctionné *e-gold*, de 1996 à 2006, et *Liberty reserve* de 2006 jusqu'à son démantèlement par les polices de 17 pays en mai 2013. Les sociétés gérant



© fotogestober

Le bitcoin : une facilité, une crédibilité, une convertibilité, mais pas une vraie monnaie.

les systèmes de paiement, domiciliés respectivement à St Christophe-et-Nieves et au Costa-Rica, étaient séparées des clients par un ou deux intermédiaires assurant le change. Il y a eu très manifestement la volonté de ne pas tomber sous le coup d'obligations réglementaires. N'étant pas très regardantes sur l'exactitude des identités des détenteurs de portefeuille, leur intérêt pour les blanchisseurs a été rapidement avéré. Si les avocats de *E-gold* ont fait valoir que le droit US est inapplicable à ce type d'instruments privés, la justice en a décidé autrement et retiendra la qualification pénale de blanchiment.

La troisième vague est celle de la décentralisation, dont le parangon est le bitcoin. Ses promoteurs se réclament très ouvertement d'une philosophie libertarienne et ne cachent pas leur

méfiance, voire leur hostilité, envers l'État. Le *bitcoin* a été inventé en 2009 par un Japonais, Satoshi Nakamoto, vraisemblablement le pseudonyme d'un groupe d'informaticiens sur lequel on sait peu de chose. Il fonctionne en *peer to peer*, c'est à dire en échange direct et décentralisé entre internautes, ce qui lui confère également la dénomination de

(13) « Crypto » signifie « caché »

« crypto-monnaie⁽¹³⁾ ».

Autrement dit, le dispositif *bitcoin* est aussi système de paiement. Les transactions financières se dispensent de banques ou de plate-formes de compensation, ce qui, selon ses partisans réduit très fortement les coûts de fonctionnement. Elles restent traçables mais demeurent anonymes... du moins tant que le détenteur du portefeuille n'est pas identifié.

Il n'existe pas non plus d'autorité gérant le dispositif, l'équivalent d'une banque centrale. Cette dernière est d'autant plus inutile que la création monétaire est programmée pour atteindre un nombre fini de *bitcoins* (environ 21 millions) vers 2040. Les *bitcoins* naissent *ex nihilo* selon un rythme décroissant par l'exécution d'un algorithme complexe. Une masse monétaire indépendante de l'action des États est supposée leur éviter la tentation de jouer avec sa valeur.

Cerise sur le gâteau, le *bitcoin* est convertible en monnaies souveraines. Des plates-formes fonctionnent tels des marchés financiers pour l'achat ou la vente, le taux de change se formant selon l'offre et la demande. A cet égard, l'envolée folle de la fin de l'année 2013, jusqu'à 1200 \$ en novembre - contre 100 en septembre, 15 en janvier 2013 et 0 en 2009 – est notamment imputée à la demande chinoise tout comme la chute de 50 % mi-décembre est prêtée aux mesures restrictives prises alors par la Banque Populaire de Chine.

Le succès du *bitcoin* a attiré de nouvelles offres similaires. Selon François Paget, chercheur en cybermenaces chez MacAfee, une centaine de monnaies similaires aurait été créée depuis 2009 dont quelques unes ont déjà disparu !

En tout état de cause, les monnaies virtuelles traduisent clairement la remise en cause de la mainmise régaliennne sur la monnaie.

Des avantages supposés qui sont autant de risques réels

Le *bitcoin* apparaît comme une belle innovation technologique. Sa masse évolue conformément aux prévisions. Est-ce véritablement un souci qu'il échappe à toute instance de contrôle ? Ses promoteurs font valoir qu'il offre ou offrira à terme plusieurs avantages : la stabilité, un faible coût de transaction et la discrétion des transactions.

En fait, ces avantages avancés sont soit très largement surévalués en raison de risques de nature économique, soit facilitent des comportements déviants qui, à terme, obéreront la confiance que l'on peut placer dans le *bitcoin*, la pire des choses qui puisse arriver à une

monnaie. Les banques centrales⁽¹⁴⁾ n'ont d'ailleurs pas manqué d'émettre des alertes.

La stabilité des prix n'est pas garantie par une masse monétaire fixée. Les promoteurs du *bitcoin* procèdent en effet à une lecture intégriste de la loi de Fisher⁽¹⁵⁾. D'une part, pour que les prix restent stables, il faut, au moins en première approximation, que la masse monétaire

(14) Les banques centrales ont d'une façon générale alerté sur les risques liés aux monnaies virtuelles, allant jusqu'à imposer des mesures restrictives (Inde, Chine) voire à interdire les transactions en *bitcoin* (Thaïlande). En Europe, la BCE a émis une mise en garde en octobre 2012 (*Virtual currency scheme*) ; en décembre 2013, la Banque de France fait part à son tour de ses réserves (Focus n°10 du 5 décembre 2013) relayée quelques jours plus tard par un organisme de contrôle financier européen, l'Autorité Bancaire Européenne. A ce jour, l'Allemagne a reconnu le *bitcoin* comme monnaie privée pour des raisons fiscales. Aux États-Unis, le patron de la FED, Ben Bernanke, a reconnu que le *bitcoin* était « prometteur à long terme ».

(15) Cette loi économique, énoncée par l'économiste Irving Fisher (1867-1947) met en relation la masse monétaire et le niveau des prix ; un accroissement trop rapide de la masse monétaire conduit, dans cette conception, à l'inflation.

croisse au même rythme que l'offre de biens et services, ce que la conception d'une monnaie P2P exclut, en tout cas aujourd'hui. D'autre part, la notion même d'inflation n'a guère de sens pour des monnaies virtuelles. En effet, aucun prix n'est exprimé originellement en *bitcoin* ; ils le sont en monnaies souveraines et ensuite convertis. Les prix en *bitcoin* reflètent avant tout les fluctuations du taux de change.

Cette monnaie présente même des motifs d'instabilité par construction, faute de garde-fous. En premier lieu l'absence de banque centrale pour mener des opérations de régulation du change. En effet, un tel organisme a la possibilité d'intervenir sur la marché des changes pour lisser les cours par des opérations d'achat ou de vente contre devises. Il existe bien une autorité centrale, la

(16) Digital Asset Transfer Authority ; créée au cours de l'année 2013, elle n'a aucun pouvoir légal.

DATA⁽¹⁶⁾, qui est un organisme définissant des

règles de bonne conduite mais n'a en rien les prérogatives d'une banque centrale

Un deuxième facteur d'instabilité vient de l'absence d'économie nationale attachée au bitcoin. S'il advient que le taux de change d'une monnaie souveraine se dégrade de façon excessive, le commerce extérieur du pays concerné s'en trouve favorisé par une amélioration apparente de sa compétitivité, ce qui tend à redresser sa valeur. Rien de tel avec le bitcoin : une variation des cours n'a aucun effet compétitivité. Il est indifférent d'acheter un bien 1 *bitcoin* quand son

(17) Cette remarque vaut pour ceux qui acquièrent des bitcoins ; pour ceux qui en détiennent, les fluctuations du change ont un effet sur le pouvoir d'achat de leur porte-monnaie.

(18) Il est courant d'affirmer que les monnaies fiduciaire et scripturale n'ont pas de valeur intrinsèque ; c'est inexact dans la mesure où la monnaie souveraine représentée de par la loi une créance sur l'économie dont elle émane, ce qui lui confère son pouvoir d'achat.

change est à 500 \$ ou 0,5 bitcoin quand le change est à 1000 \$⁽¹⁷⁾.

Enfin, le troisième facteur d'instabilité vient de l'absence de valeur intrinsèque du bitcoin. En effet, privé de son rôle de monnaie, combien vaudrait un *bitcoin* ? Il est régulièrement comparé à l'or, pour lequel il existe cependant un marché non monétaire et qui assure au métal précieux une valeur intrinsèque, garantissant celle de l'or monétaire. Rien de tel, pour le bitcoin. Sa valeur peut s'effondrer, aucun marché ne lui assure une demande non monétaire et donc un prix ... Autant dire que le *bitcoin* peut chuter dans de grandes profondeurs⁽¹⁸⁾.

Le dernier élément d'instabilité vient de sa parfaite substituabilité par des monnaies

(19) Sauf peut être sur les sites du « darkweb ».

souveraines⁽¹⁹⁾ : malgré sa rareté

programmée, la demande de bitcoin sera extrêmement variable selon que les consommateurs souhaiteront l'utiliser pour leurs achats ou lui préféreront d'autres devises.

Si le taux de change du *bitcoin* est passé de quelques euros aux alentours de 900 en début d'année 2013, cela s'explique certes par la montée en régime de son usage mais aussi par le caractère fortement spéculatif que lui confère son essence volatile. Le risque de change⁽²⁰⁾

est considérable, avec des fluctuations parfois de 10 % en quelques heures, de 20 % en quelques jours ... Des produits dérivés – options ou contrats de différence, avec de forts effets de levier – sont apparus, qui sont tout autant des instruments de couverture que de spéculation. Enfin, la détention des *bitcoins* apparaît très concentrée : moins de 50 personnes possèdent 30 % des bitcoins, moins de 1000 en conservent la moitié. L'étroitesse du marché peut faire craindre des manipulations de cours.

Évoquer des coûts de transactions faibles dans ces conditions est excessif. Certes, le système de paiement *bitcoin* se passe d'intermédiaire. C'est sans la prise en compte des risques, de change comme évoqué précédemment, d'erreurs – par le caractère irréversible des opérations – et de vol ... On ne peut sous estimer l'ampleur du « cyberbrigandage ».

Les cas de vol de porte-monnaie se multiplient en raison de la profitabilité du cybercrime. En 2011, la plateforme d'échanges MtGox annonce le vol de 1000 *bitcoins*. C'est à l'époque une somme limitée... A la même époque, un particulier découvre le piratage de son ordinateur et le vol de 25 000 *bitcoins*, soit à l'époque la bagatelle de 350 000 euro (mais 17 millions d'euros aux cours de janvier 2014).

A l'automne 2013, le site Inputs.io subit un vol de 4 100 *bitcoins* – 1,2 millions de dollars – et la plateforme d'échange danoise est piratée pour un préjudice

d'un million d'euros. Les hackers ont parfaitement compris que les coûts de ces cyber hold-up sont modestes pour des rentabilités fortes. Rappelons que l'une des raisons originelles des banques était la conservation des valeurs de la rapacité des criminels... Le prix Nobel d'économie Paul Krugman évoquait à propos du bitcoin une régression

(21) Le risque de change est le risque de perte due à une évolution défavorable du taux de change d'une devise détenue (ou d'un actif libellé en devise).

monétaire⁽²¹⁾. On peut certes en débattre mais sur ce point précis, c'est effectivement une marche en arrière.

Deux qualités majeures avancées par les promoteurs du *bitcoin* en révèlent néanmoins toute l'ambivalence : la discrétion et la convertibilité. Faire circuler l'argent de façon (presque) anonyme, pouvoir le transformer à tout instant en monnaie souveraine représente le nec plus ultra du système de paiement. Ce sont deux facilités extraordinaires que la criminalité organisée ne pouvait négliger.

Des sites internet offrent des produits totalement illicites de toute nature : numéros de cartes bancaires, stupéfiants, armes, pédopornographie... Ce sont les marchés noirs du « *darkweb* ».

L'anonymat des monnaies virtuelles, doublé du recours à un réseau spécifique qui brouille les traces sur la toile, permet de réaliser des emplettes criminelles dans la plus grande discrétion. Au début du mois d'octobre 2013, le FBI fermait *Silk Road*, site mettant en relation acheteurs et vendeurs, se rémunérant par commission, où les paiements ne

s'effectuaient qu'en *bitcoin*. Ce cyber-supermarché (ou plus exactement cybercourtier) du produit criminel, ouvert en 2011, aurait généré en 2 ans un chiffre d'affaires de 9,5 millions de *bitcoins*, à comparer aux 12 millions actuellement en circulation, pour 600 000 *bitcoins* de commission. Il a été très vite remplacé par d'autres et d'ailleurs un nouveau « *Silk Road* » a ouvert un mois plus tard. Il s'agit ici d'une criminalité pleinement économique : s'il y a une demande et un profit à réaliser, il y aura une offre. L'internet et les monnaies virtuelles sont des moyens d'accroître la rentabilité du crime par des gains de productivité et la réduction des coûts ...

De façon simple, le blanchiment qui consiste à dissimuler l'origine illicite de capitaux en est facilité : les flux criminels sont convertis en monnaie virtuelle, transférés là où on veut les dissimuler et transformés à nouveau en monnaie officielle (propre !). Tracfin décrit ainsi dans son rapport 2011 comment une société en France opérait de multiples transactions vers l'étranger de façon totalement dissimulée. Le site *Liberty Reserve*, autre cyber-supermarché de l'illicite aurait blanchi 6 milliards de dollars en utilisant la monnaie virtuelle éponyme. En janvier 2013, Charlie Shrem, un des pontes du monde du *bitcoin* - vice-président de la *Fondation Bitcoin* - connaissait des démêlés avec la Justice américaine, pour avoir contribué à fournir des *bitcoins* à des acheteurs chez *Silk Road*. Deux éléments peuvent encore freiner l'ardeur des blanchisseurs dans

l'utilisation du *bitcoin* : sa traçabilité et sa forte volatilité. Mais des solutions « correctrices » apparaissent : le *zerocoin* est un avatar du *bitcoin* qui offre un réel anonymat, sous couvert du respect de la vie privée ... Et un Russe vient de lancer le *wishcoin*, dont la valeur est indexée sur le rouble, tout en garantissant l'anonymat.

Traquer les circuits financiers criminels

Faut-il interdire les monnaies virtuelles ? Outre que cela reviendrait à condamner toute forme d'innovation, une telle interdiction risque fort d'être illusoire, le cyberspace étant international. En revanche, il est temps de sortir du brouillard juridique.

Les autorités bancaires françaises imposent désormais aux sociétés effectuant « à titre habituel » des opérations de change avec des *bitcoins*

(22) Je tiens ici à remercier Benjamin Maréchal, jeune « ancien » de la Banque de France et l'un des animateurs du FIC 2014, pour l'éclairage qu'il m'a apporté sur le sujet.

de disposer d'un agrément⁽²²⁾ de prestataire de service de paiement, les soumettant ainsi à la

dense réglementation financière. En tout état de cause, il ne peut y avoir de monnaie qu'avec la confiance et celle-ci exige des actions fortes contre la criminalité. C'est le retour du régalien !

La politique la plus efficace contre le crime reste la confiscation des profits illicites. Il faut donc que les enquêteurs de police et de gendarmerie, au-delà des faits criminels, généralisent la traque des circuits financiers clandestins dans lesquels s'insèrent les monnaies virtuelles.

Les produits de marquage codés

par FRANÇOIS HEULARD

P

Pour lutter contre les vols et les agressions à but crapuleux, les technologies de marquage codé issues de la lutte contre la contrefaçon font aujourd' hui irruption dans le domaine de la sécurité.

La manifestation de la propriété s'exerce souvent par un signe visible, clairement identifié. Le marquage au fer rouge des troupeaux dans l'ouest américain en est une illustration très populaire. Dans le domaine commercial, la mise en avant de la marque et du logo associé fonde souvent le modèle de développement de



FRANÇOIS HEULARD
Lieutenant-colonel, chef de la division criminalistique Physique et Chimie de l'IRCGN.

l'entreprise. La préservation de l'identité devient un enjeu économique que les contrefacteurs mettent en péril.

De nombreuses technologies de

marquage ont donc été développées. Elles garantissent l'authenticité, voire la traçabilité du produit. Initialement réservées aux produits de luxe, ces technologies trouvent des applications multiples allant du marquage des fibres

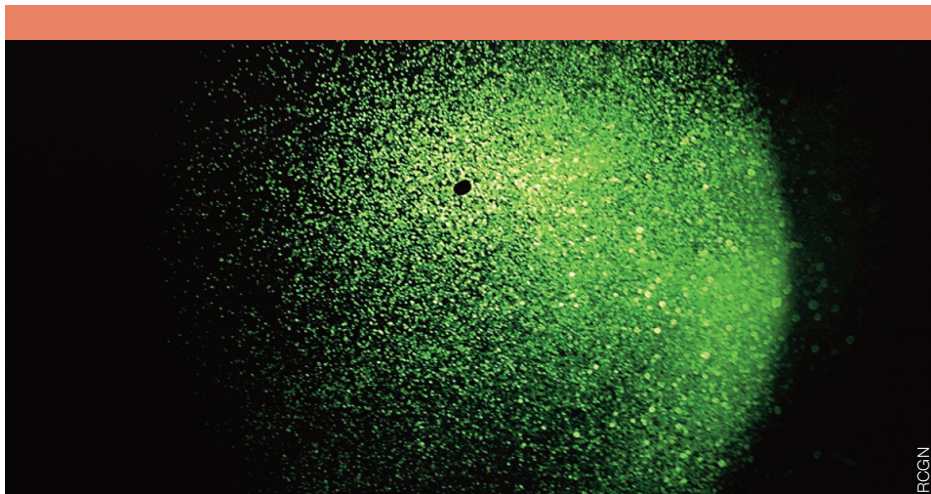
(1) L'actualité chimique - Février-Mars 2012, n° 360-361.
<http://culturesciences.chimie.ens.fr/node/1364>

textiles⁽¹⁾ à celui d'une cargaison de pétrole brut. Le marché de l'Art

s'intéresse aussi de près à ces procédés dont la palette très large s'étend du marquage visible à l'œil nu jusqu'aux techniques de codage les plus pointues nécessitant des analyses poussées dans des laboratoires spécialisés.

Des technologies variées et éprouvées.

Il n'existe presque aucune limite technologique pour réaliser des marquages. La micro-gravure, les encres techniques, les images cachées, les nano-poudres, les codes-barres magnétiques, les micro-étiquettes, les



Une émulsion qui permet une haute traçabilité à la lumière.

terres rares et l'ADN synthétique sont ainsi employés dans de multiples applications commerciales. Les mêmes enjeux économiques et sociétaux ont conduit un glissement de ces technologies vers le domaine de la sécurité privée, à destination des professionnels comme du grand public, pour faire face notamment aux vols. Les produits de marquage codés (PMC) ainsi distribués possèdent la même architecture qui tient en trois composantes : des composés codants, un solvant polymérique ou aqueux, un chromophore qui absorbe la lumière dans l'ultra-violet et émet une lumière visible. Le code, cœur du produit, qui peut être composé de multiples manières, est habituellement constitué de terres rares ou d'une séquence d'ADN synthétique. ADN, le mot magique est lâché...

Merveilleux vecteur de communication, il suscite aussi toutes les craintes et les interrogations les plus irrationnelles. En fait, la réalité est plus triviale : il s'agit d'un court fragment d'ADN monobrin dont le design et l'enchaînement des nucléotides composent un code unique. Il n'y a pas de code génétique, pas d'interaction avec le monde du vivant. Invisible à l'œil nu, déposé ou pulvérisé, le produit peut être visualisé simplement. Il suffit de l'éclairer avec une lampe à ultra-violet et de constater la fluorescence. La lecture du code, plus complexe, impose généralement le passage par un laboratoire de criminalistique.

Marquage d'objets et aspersions d'agresseurs

Pour les particuliers, les produits de marquage codés sont utilisés pour protéger tout type d'objet, de la télévision

à la bicyclette. Il suffit d'appliquer le produit comme un vernis invisible permanent. Chaque petit flacon possède son code propre et n'est attribué qu'à un client. Le particulier indique en retour à la société distributrice la nature des objets marqués à l'aide du PMC.

Si le phénomène est encore marginal en France, l'utilisation de ces PMC se fait depuis de nombreuses années au Royaume-Uni, de façon coordonnée à l'échelle de quartiers entiers, en collaboration étroite avec les forces de l'ordre qui en font la publicité et en favorisent le déploiement. Dans ces conditions, le dispositif se révèle très efficace et possède un effet dissuasif remarquable.

En France, les agressions et vols à répétition posent un problème majeur pour l'exploitation de certains commerces. Dans quelques centres commerciaux, la question de la pérennité de certaines bijouteries s'est posée avec acuité. En dépit des mesures de protection habituelle, comme la vidéosurveillance, elles restent des cibles très attractives. Pour dissuader les délinquants d'agir, certains magasins se sont équipés de dispositifs anti-agression s'appuyant sur ces nouvelles technologies. En cas d'attaque, les assaillants sont aspergés par une solution aqueuse renfermant le produit de marquage codé. Leur présence sur les lieux est ainsi matérialisée, sans

ambiguïté. A ce jour, les dispositifs installés, à grand renfort d'affichages et de publicités, se sont montrés parfaitement dissuasifs.

Durabilité, traçabilité, unicité, innocuité sont garanties par les sociétés qui mettent en avant de nombreux partenariats et certificats comme autant de preuves de sérieux. Pour autant, l'engagement de ces sociétés dans un processus de certification global apparaît comme inéluctable pour renforcer la confiance dans l'utilisation des PMC. L'expérimentation et le suivi(2) du déploiement de ces dispositifs sur plusieurs dizaines de sites sont envisagés en 2014.

Un nécessaire encadrement juridique

Pour que l'effet dissuasif des PMC soit entier, il est nécessaire que les auteurs, quand ils sont passés à l'acte, puissent être effectivement identifiés grâce à ces technologies et qu'ils puissent être déférés devant une juridiction de jugement.

L'identification d'un objet volé ou recélé, marqué avec ces nouvelles technologies, ne pose pas de problème juridique nouveau. Peu importe qu'un véhicule ait ses vitres gravées ou qu'il soit marqué par un vernis codé. La garantie de l'unicité du code et la traçabilité du produit de marquage codé, depuis sa fabrication jusqu'à sa distribution, sont indispensables à la crédibilité du système.



Un processus fortement encadré juridiquement.

De même, le « fichier client » faisant le lien entre l'objet marqué et son propriétaire déclaré est la clé de voûte de l'édifice. Les modalités d'accès à cette base de données nominatives varient selon les législations. Si au Royaume Uni un accès direct est possible, en France, la Commission nationale informatique et liberté (CNIL) veille à la protection de ce type d'informations. Pour les enquêteurs français, l'information utile pour le traitement d'un dossier peut être obtenue, sans difficulté particulière, par voie de réquisition aux sociétés distributrices de ces produits.

L'aspersion et le marquage d'un individu interrogent davantage. Il paraît nécessaire de s'assurer que les moyens utilisés sont bien en adéquation avec les buts

recherchés. Le « *marquage* » d'un individu par aspersion de produit issu d'un dispositif anti-agression n'est ni une atteinte à l'intégrité physique, ni une atteinte à l'image puisque le produit de marquage est habituellement invisible à l'œil nu. Le préjudice peut néanmoins exister pour l'individu dont la peau et les vêtements seraient altérés par l'action du maculage. Si cette contrainte pourrait paraître acceptable vis-à-vis de l'auteur d'une agression, il n'en est pas de même pour les employés et clients des magasins protégés. A défaut d'un cadre réglementaire strict et d'une certification des produits et de leurs conditions d'utilisation, l'engagement des installateurs de ces dispositifs dans une charte de bonnes pratiques pourrait

utilement prévenir les situations conduisant à la mise en jeu de procédures civiles.

Rechercher la lumière

Dès qu'une agression s'est produite et provoque le déclenchement d'un dispositif de marquage, les enquêteurs se mettent en action pour rechercher les malfaiteurs. La question des modalités de la recherche de traces de fluorescence se pose donc. Dans le cadre du flagrant délit, les prélèvements externes en vue de recueillir le produit de marquage codé sont réalisés en vertu de l'article 55-1 du code de procédure pénale. Au Royaume-Uni, des portiques ultraviolet sont utilisés pour rechercher, *a priori* et de façon exhaustive, la fluorescence sur les individus. Cette pratique est exclue en France où seules les personnes soupçonnées, à partir d'autres éléments, peuvent être soumises à la détection à l'aide d'une lampe à rayons ultraviolets et prélevées, généralement par un écouvillonnage externe. En revanche, en l'état actuel du droit français, il n'est pas possible de rechercher des traces de pulvérisation de PMC à la suite d'un contrôle d'identité.

Une véritable force probante

L'administration de la preuve est libre et sa discussion se fait lors des débats contradictoires. L'expert doit être capable de mettre en perspective la réalité scientifique du moment, les résultats obtenus et l'apport de cet élément dans

la réalité du procès. L'acceptation de la preuve scientifique pour les produits de marquage codés ne semble pas devoir poser de difficulté particulière, dès lors que les limites techniques sont posées et expliquées. L'exemple de l'ADN l'illustre bien. Les calculs de probabilité associés aux populations de référence, la maîtrise de la traçabilité depuis les opérations de prélèvement jusqu'à l'analyse au laboratoire sont autant de gages qui font aujourd'hui de l'ADN une preuve peu réfutée et considérée comme étant parfaitement recevable.

Déjà utilisées pour les besoins de certaines enquêtes, ces nouvelles technologies sont, pour les enquêteurs comme pour les magistrats instructeurs, des outils complémentaires, innovants, apportant des éléments importants au dossier. Il s'agit d'indices comme les autres, ni plus, ni moins. Il serait illusoire d'y voir la panacée et la preuve absolue.

Toutefois, en raison de leur forte valeur d'individualisation, les PMC doivent être traités avec une grande rigueur. En amont, la société qui a installé le dispositif doit garantir que le code distribué est bien unique et identifié. La chaîne criminalistique, depuis l'agent de constatation jusqu'au responsable de l'analyse au laboratoire, doit prévenir les contaminations, garantir la bonne réalisation des prélèvements, en assurer la traçabilité et garantir la fiabilité des résultats rendus. Seule cette cohérence

permet d'apporter une preuve solide et fiable. La gendarmerie est prête à faire face à ces nouvelles technologies, par la professionnalisation des acteurs de la police technique et scientifique et les procédures mises en place. La démarche d'accréditation des plateaux départementaux des cellules d'identification criminelles, avec l'appui de l'Institut de recherche criminelle de la gendarmerie nationale s'inscrit pleinement dans cette exigence de traçabilité et de rigueur.

L'arrivée sur le marché de la sécurité privée de nouvelles technologies comme les produits de marquage codés offre pour les enquêteurs de nouvelles possibilités d'établir des liens entre des personnes et des faits, à partir d'éléments matériels. Au même titre que les traces numériques, le recueil et l'exploitation des marquages générés par ces nouvelles technologies impose une grande rigueur. Le respect strict du cadre juridique, la capacité d'adaptation et d'innovation de la chaîne criminalistique pour traiter ces nouveaux objets sont déterminants pour affecter à cet item la valeur probante juste. Au final, la discussion lors des débats autour de cet élément nouveau reste de même nature que celle autour des autres indices habituellement présentés, comme les empreintes digitales ou l'ADN. La jurisprudence ne manquera pas d'en affiner les contours.

L'ADN rapide à la portée de la gendarmerie

par EMMANUEL PHAM-HOAI

L

La capacité des enquêteurs de porter rapidement à la connaissance des magistrats des éléments probants est actuellement confortée par le déploiement de nouvelles technologies. Elles mettent à la portée de l'enquêteur des moyens jusqu'alors distants, onéreux et d'une technicité délicate à mise en œuvre. Le concept de l'ADN rapide fait partie de ces nouveaux protocoles qui auront une incidence forte sur l'exercice de la police judiciaire en général et scientifique en particulier en la démocratisant.



EMMANUEL PHAM-HOAI

Chef d'escadron de gendarmerie. Chef du département biologie de l'IRCGN

Parmi les outils disponibles pour la résolution d'une enquête, les empreintes génétiques sont devenues incontournables. Cependant, les délais de réalisation d'une

analyse génétique et l'éventuelle interrogation du Fichier national automatisé des empreintes génétiques (FNAEG) en résultant se heurtent aux contraintes du temps opérationnel.

Le *Federal Bureau of Investigation* (FBI) américain tente actuellement d'apporter une réponse à cette problématique par le biais du concept dit d'ADN rapide (*Rapid DNA*). Les premiers résultats, en tenant compte de l'architecture des forces de l'ordre françaises, semblent transposables au système judiciaire hexagonal et plus particulièrement au sein de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN).

Avant d'aborder la possibilité d'une éventuelle adaptation, il est nécessaire de revenir sur le travail entrepris à ce sujet par l'agence américaine.

L'ADN rapide, un concept

Le *Combined DNA Index System* (Codis)⁽¹⁾, fichier des empreintes



© Lonely

L'ADN rapide est une technologie accessible et projetable.

(1) <http://www.fbi.gov/about-us/lab/biometric-analysis/codis>

génétiq ues américain géré par le FBI, a pour finalité la comparaison entre profils génétiques inconnus issus de scènes d'infraction (traces) et profils identifiés issus de suspects (individus). Sa mise en place tient compte de l'organisation fédérale des États-Unis ainsi que de l'autonomie législative de ses états. Ce fichier s'articule ainsi sur trois niveaux : local, étatique et fédéral. Une empreinte génétique déterminée par un laboratoire local agréé par le FBI devra être transmise aux niveaux successifs. Dans cette architecture, le facteur limitant est le délai de réalisation des analyses : l'enquêteur doit trouver un laboratoire disposant d'un plan de charge lui permettant de réaliser les travaux dans des délais raisonnables. De cette façon, en cas de résultat positif, la réponse peut s'inscrire dans le temps

de l'action. Pour satisfaire à cette contrainte de temps opérationnel, via des partenaires privés, le FBI cherche à développer un analyseur génétique portable. Simple d'utilisation pour un non-biologiste, il permettrait à l'enquêteur d'alimenter le Codis en profils individus en moins de deux heures. Les contraintes de temps et de logistique imposées par le recours à un laboratoire seraient ainsi éliminées.

L'utilisation de ces appareils s'appliquerait tant au domaine judiciaire (détermination d'un profil génétique d'un suspect et comparaison au sein du Codis lors de sa mesure de garde à vue), qu'administratif (identification de candidats à l'immigration) ou encore militaire (identification sur un théâtre de guerre de soldats tués en opération).

(2) <http://intengenx.wpengine.com/>

(3) <http://netbio.com/>

Deux sociétés, IntegenX⁽²⁾ et NetBio⁽³⁾, travaillent

actuellement sous l'égide du FBI au développement d'un tel matériel, dont les premières versions sont désormais disponibles. Les machines se veulent simples d'accès de sorte que l'intervention humaine soit réduite à son strict minimum (insertion des échantillons et mise en route de l'analyse).

Techniquement, ces appareils profitent des dernières avancées en termes de miniaturisation. Ils sont donc la version réduite d'un laboratoire réalisant les mêmes opérations. Leur point fort est la réalisation en 90 minutes d'une analyse génétique de 5 à 8 échantillons selon le modèle.

Les premiers résultats publiés dans des revues criminalistiques reconnues, telles

(4) Schumm J.W. et al., *A 27-Locus STR assay to meet all United States and European law Enforcement agency standards*, Journal of Forensic Sciences (2013)

(5) S. Verheij, et al., *RapidHIT 200, a promising system for rapid DNA analysis*, Forensic Sci. Int. Gene. Suppl. (2013)

que *Journal of Forensic Sciences*⁽⁴⁾ et *Forensic Science Genetics*⁽⁵⁾, attestent du succès de ces machines sur des supports riches en

ADN (cellules buccales). Cependant, pour des échantillons dits pauvres (traces de contact plus spécifiquement), les résultats sont mitigés. Le protocole concernant ce type de support nécessite de plus amples études qui sont actuellement menées par les deux sociétés.

Sur l'aspect légal, ces machines nécessitent de remplir les conditions imposées par les lois des différents états et surtout les règlements imposés par le FBI quant à la bonne exécution des analyses afin que les profils génétiques obtenus puissent être exploités dans le Codis. Pour l'heure, ces appareils n'ont pas encore été approuvés.

Enfin, l'enjeu économique est majeur pour les deux sociétés précitées. Le marché nord-américain, de par la multiplicité de ses forces de l'ordre, représente un conséquent vivier de clients. Le marché européen n'est pas en reste compte tenu du nombre important de pays membres de l'Union disposant d'un fichier des empreintes génétiques. Dans le prolongement de ce constat, la France pourrait trouver une application stratégique à ces machines.

Une possible application en France

De par son organisation nationale, le système français ne dispose que d'un seul niveau de centralisation des données génétiques. Ses laboratoires, publics et privés, sont disséminés sur l'ensemble du territoire métropolitain, engendrant les mêmes problématiques que celles de leurs homologues américains. Le déploiement des analyseurs portatifs semble donc trouver un cadre d'action tant sur un plan général que particulier. En effet, des services tels que l'Unité d'investigation et d'identification (U2I) de l'IRCGN, seule entité française

criminalistique projetable sur une scène de crime, disposeraient ainsi d'un outil permettant d'apporter une réponse dans le temps de l'action. Conjuguées à la chaîne criminalistique de la gendarmerie, les chances d'obtention de résultats exploitables en seraient nettement accentuées.

Pour illustrer cette approche, il convient d'envisager le scénario (fictif) d'un fait criminel constaté dans un temps proche de sa commission et nécessitant l'engagement de l'IRCGN. Dans ce cas, l'U21 se projetterait au plus près de la scène de crime, permettant un lien direct laboratoire-groupe d'enquête. Les prélèvements seraient effectués sur le lieu des faits par les techniciens en identification criminelle. En lien avec le directeur d'enquête, l'expert déplacé ainsi que le coordinateur criminalistique établiraient un ordre de priorité des éléments les plus intéressants en termes d'enquête policière pour ensuite ne retenir que les plus susceptibles de donner un résultat positif en ayant recours à la machine. Les traces sélectionnées seraient alors analysées *in situ*, tout comme le profil génétique des suspects identifiés en parallèle. L'expert déplacé effectuerait alors la comparaison des différentes empreintes génétiques déterminées, permettant le renseignement en temps réel des enquêteurs. Les prélèvements les plus complexes seraient pour leur part traités

en laboratoire, permettant ainsi d'employer au mieux les savoir-faire détenus par ce dernier à la façon d'une boîte à outils.

Ce scénario est séduisant dans le sens où il permet de répondre à la demande urgente engendrée par l'enquête, d'assurer le déploiement de moyens conséquents justifiés par la sensibilité des faits et de mettre en relation directe les militaires pouvant avoir un impact significatif sur la résolution de l'affaire. Cette vue de l'esprit doit cependant être confrontée à la réalité.

L'intégration de ces appareils dans un dispositif de police technique et scientifique doit tenir compte de plusieurs paramètres : le coût actuel d'une machine se situe aux alentours de 200 000 € et le prix par écouvillon analysé est de l'ordre de 300 € contre 30 € au sein de

(6) Extrait du cahier de tarification 2014 de l'IRCGN, page 41

l'IRCGN⁽⁶⁾. On peut déplorer leurs résultats mitigés sur

des traces dites pauvres : les traces de contact peuvent constituer l'essentiel des prélèvements dans une affaire. Enfin, quant à l'aspect légal, compte tenu de la nécessité française de disposer d'un agrément aux fins d'analyse génétique et de l'obligation de l'accréditation des laboratoires par le Comité français d'accréditation (Cofrac), il est indispensable que ces machines soient reconnues comme un laboratoire miniaturisé, répondant aux mêmes

exigences qu'un laboratoire installé dans un bâtiment.

Les aspects techniques et réglementaires font actuellement l'objet d'études complémentaires. Les sociétés travaillent entre autres à l'obtention d'une certification ISO (organisation internationale de normalisation) de leurs machines, nécessaire pour franchir une première étape réglementaire.

Sans attendre leurs conclusions, ces travaux permettent d'ores et déjà de se projeter quant à la future utilisation de ces analyseurs en France.

Perspectives

Les caractéristiques de ces appareils permettent de distinguer deux créneaux d'utilisation dans le temps. Le premier, à brève échéance, s'inscrirait dans le cadre de moyens supplémentaires de haut niveau mis à disposition pour des affaires à la sensibilité avérée et nécessitant une réponse rapide au plus près des enquêteurs. Le second, à moyenne et longue échéance, résulterait d'une démocratisation de la machine. Les cadres d'action sous-jacents à ces deux cas de figure doivent cependant être définis.

Sur le court terme, l'implantation de ces appareils semble possible en respectant certains critères d'emploi. Il faut inscrire l'usage de l'appareil dans le temps de l'action judiciaire. La rapidité de traitement

par cette technologie doit permettre au laboratoire mobile de s'adapter au mieux aux soubresauts de l'enquête. La proportionnalité de la réponse mise en œuvre en termes de police technique et scientifique doit être respectée. Les homicides sont visés plus particulièrement de par leur sensibilité qui justifie la pertinence d'un tel déploiement. Il paraît opportun de définir une stratégie analytique en fonction de la pertinence du scellé en utilisant la complémentarité des moyens de police technique et scientifique en matière d'empreintes génétiques. Le succès de la mise en œuvre de ces technologies repose sur la capacité de projection *ad hoc*. Comme évoqué supra, l'U2I dispose d'experts projetables et des moyens nécessaires pour assurer l'autonomie logistique d'un laboratoire déplacé. Enfin, et cela n'est pas la moindre restriction, il faut obtenir la reconnaissance juridique de ce type de moyen par la démonstration de résultats reproductibles et identiques à ceux d'un laboratoire traditionnel.

Sur le moyen et long terme, une fois que la machine aura été largement éprouvée, envisager son implantation au sein des Cellules d'identification criminelle (Cic), présentes dans chaque groupement de gendarmerie, semble réaliste mais sous certaines conditions. En effet, ces entités ne disposent pas d'experts inscrits et agréés *in situ*. Il n'en demeure pas moins qu'à l'instar du concept nord-américain,

ces appareils pourraient être dédiés à l'analyse des individus et des traces prélevées sur les scènes d'infraction relevant de la délinquance de masse. Une analogie avec l'évolution des empreintes digitales peut être effectuée. Si initialement le recueil des relevés décadactylaires était centralisé, les évolutions techniques ont permis de délocaliser cette collecte d'informations via des terminaux locaux dédiés à cet effet.

Les suspects prélevés et les traces issues de la délinquance de masse pourraient ainsi suivre la même évolution, permettant d'élargir davantage l'accès aux empreintes génétiques et plus particulièrement au FNAEG. Se poserait cependant la question de la nouvelle place de l'expert en empreintes génétiques dans cette nouvelle configuration. Acteur indispensable quant à la validité du profil génétique, son nouveau positionnement devrait alors concilier la remontée sans délai de l'information (le profil génétique établi localement) et sa garantie scientifique.

Disposer d'un analyseur génétique projetable au plus près de l'enquête est désormais une réalité. Si des obstacles techniques et réglementaires restent à franchir, il n'en demeure pas moins que le déploiement de ce matériel est désormais possible. La gendarmerie, via l'U2I, dispose déjà de l'expérience opérationnelle criminalistique permettant d'embarquer ce nouveau moyen. La disponibilité à court terme de ces technologies milite pour que soit définie une doctrine d'emploi tenant compte des spécificités de l'enquête et des moyens de police scientifique existants. L'analyseur portable s'inscrirait ainsi en tant que nouvel outil « génétique » à vocation clairement opérationnelle sur le court terme. On pourrait s'appuyer sur l'exemple des Pays-Bas. Ces derniers ont en effet développé cette approche projetable au sein de leur *National Crime Squad*. Un analyseur portable a ainsi été intégré au sein d'un mini-van et éprouvé dans différentes situations tests.

Au delà du défi technique, il s'agit toujours d'améliorer les outils de la criminalistique mis à la disposition de la communauté judiciaire. Dans cette perspective, l'ADN rapide offre une capacité à répondre différemment en matière d'empreintes génétiques.

La filière nationale de sécurité : une opportunité pour la gendarmerie ?

par **STÉPHANE SCHMOLL**

L

À la fin de l'année 2013, le gouvernement, les industriels et des opérateurs d'importance vitale ont créé une filière nationale de la sécurité, comme préconisé par le Livre blanc sur la défense et la sécurité nationale (LBDSN). Face à ses ambitions, la filière, dont la gendarmerie nationale est un des acteurs, est confrontée à des défis inédits.

La gestation de la filière nationale de sécurité



STÉPHANE SCHMOLL

Directeur général de Deveryware, Colonel dans la réserve citoyenne de la gendarmerie nationale, Président de la commission stratégique du CICS (Conseil des industries de la confiance et de la sécurité)

La filière est née d'une volonté de démontrer la capacité des acteurs français de la sécurité de pouvoir coopérer pour une meilleure efficacité. Les groupements professionnels de défense pour les trois armées, GIFAS,

GICAT et GICAN⁽¹⁾, avaient préalablement étendu leurs activités à la sécurité dans le

(1) GIFAS : Groupement des Industries Françaises Aéronautiques et Spatiales. GICAN : le Groupement des Industries de Construction et Activités Navales. GICAT : Groupement des Industries Françaises de Défense Terrestre et Aéroterrestre.

domaine civil. Sous l'égide du SGDSN, des membres de ces groupements ont pendant deux ans travaillé avec des services de l'Etat à définir les feuilles de route de certains systèmes du domaine de la sécurité. Elles comportaient des propositions de démonstrateurs des capacités conjuguées des industriels français.

Le dernier livre blanc de la défense et la sécurité nationale a confirmé l'intérêt de ces coopérations en préconisant la création d'une filière nationale spécifique à la sécurité, en liaison avec la politique européenne de sécurité. Son intérêt a été publiquement affirmé par le président de la République. Les objectifs de la filière sont clairs. Il s'agit de prioriser et

LES DÉMONSTRATEURS IDENTIFIÉS

- Communications haut débit sécurisées
- Protection du transport aérien et des aéroports
- Vidéo protection
- Bâtiment intelligent et sûr
- Equipements de protection des primo-intervenants
- Sécurité et sûreté de la chaîne logistique
- Protection des voies TGV
- Plate-forme off-shore
- Protection des zones portuaires

satisfaire les besoins capacitaires stratégiques de l'Etat, des Opérateurs d'importance vitale (OIV) et des entreprises. L'optimisation pour les secteurs public et privé des coûts de développement, d'acquisition et d'exploitation des solutions est recherchée. Enfin, il s'agit de créer de la valeur exportable et de l'emploi. Onze ministères étant concernés, c'est le premier ministre qui anime les travaux du comité de la filière de sécurité (COFIS).

Le COFIS se compose de quatre collèges. Le premier rassemble des représentants des ministères concernés ainsi que d'organismes tels que la banque publique d'investissement, le commissariat général aux investissements, les délégations interministérielles à l'intelligence économique et à la sécurité privée, UBI

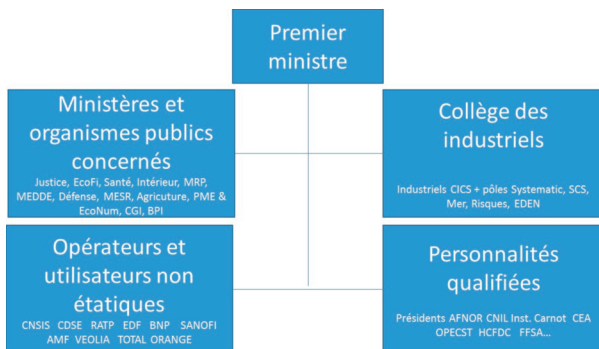
France, l'AFNOR, la DGA, l'ANSSI... Le deuxième mobilise des opérateurs et des utilisateurs non étatiques dans les transports, l'énergie, l'eau, ainsi que des associations et collectivités territoriales, utilisateurs de sécurité. La troisième entité réunit des personnalités qualifiées de divers organismes : haut comité français pour la défense civile, fédération des sociétés d'assurances, instituts de recherche, impliqués dans les volets juridique, normatif et organisationnel de la sécurité. Enfin, des industriels du Conseil des industriels de la confiance et de la sécurité (CICS) et des pôles de compétitivité complètent ce dispositif au sein du quatrième collège.

Le CICS a été créé en septembre 2013 par ses 4 groupements fondateurs :

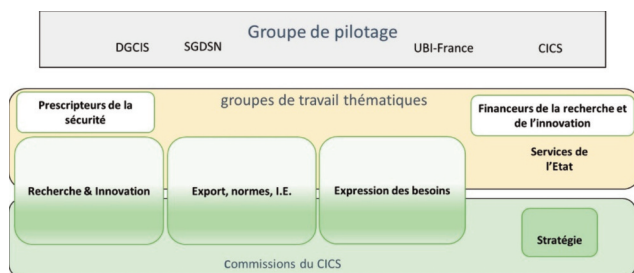
(2) FIEEC : Fédération des industries électriques, électroniques et de communication.

GIFAS, GICAT, GICAN et la FIEEC⁽²⁾ pour fournir au

COFIS un interlocuteur unique représentant les producteurs de solutions de sécurité. Il pourra accueillir d'autres groupements professionnels concernés par la sécurité, tels que la Fédération des



métiers de l'incendie, le Syntec numérique, etc. A ce jour, l'industrie de la sécurité française représente 10 milliards d'euros de chiffre d'affaires, dont 55% à l'export, et 50.000 emplois très qualifiés.



Le groupe de pilotage du COFIS est co-animé par le SGDSN et la DGCS⁽³⁾, assistés de UBI-

France et du CICS. Il s'appuie sur 5 groupes de travail : deux groupes sont purement étatiques, regroupant respectivement les prescripteurs de sécurité et les financeurs de la R&D. Les trois autres groupes sont paritaires avec des représentants des secteurs public et privé : expression des besoins - export, normes et intelligence économique, recherche & Innovation.

Au sein du CICS, les industriels analysent ensemble leurs convergences et bâtissent leurs propositions dans trois commissions miroirs des 3 groupes paritaires du COFIS.

Une commission stratégique, présidée par l'auteur du présent article, a également été créée pour assurer la cohérence des autres commissions, tracer le périmètre industriel de la filière, développer la convergence des stratégies industrielles et des politiques publiques, illustrer les bonnes pratiques de coopération public-privé, explorer les sujets transverses tels que les

coopérations avec l'Europe (institutions et organismes connexes), la protection des données personnelles ou celle du patrimoine immatériel des acteurs de la filière, et explorer le moyen terme.

A court terme, le COFIS a défini 7 axes de travail qui visent à connaître la filière nationale, exprimer le besoin, développer les solutions de demain (démonstrateurs), identifier les technologies de sécurité critiques, soutenir les entreprises françaises à l'export, utiliser le levier européen et enfin mettre en réseau les acteurs.

Une liste d'une dizaine de chantiers de solutions de sécurité a été arrêtée pour démontrer la capacité des acteurs à définir ensemble des solutions, à les financer et à les réaliser dans une coopération précompétitive.

L'ensemble de cette organisation est assez complexe, avec de multiples groupes, commissions et comités thématiques ou transversaux. Comme souvent, c'est souvent le même groupe de personnes motivées qui participe activement à ces instances. Dans la mesure où ces travaux sont chronophages et bénévoles, leur

motivation se fonde sur la volonté de contribuer à l'intérêt général tout en retirant une visibilité et un fléchage des actions prioritaires pour leur propre entité. La camaraderie et la relative confiance qui se sont instaurées dans cette petite troupe sont également des facteurs d'efficacité.

Les défis de la filière de sécurité

Bâtir une filière sous-entend une modification profonde des pratiques des acteurs, ainsi que des changements culturels qui peuvent être assez importants. En premier lieu, la notion même de travail en commun entre le public et le privé pour un même objectif, sans qu'un bord ne commande à l'autre, n'est pas toujours naturelle dans notre pays. Malgré la réduction de sa puissance, l'Etat et ses organismes ont généralement une posture d'administration, les industriels étant traités comme des administrés. Or, ces derniers considèrent qu'ils sont contributeurs du budget de l'Etat, qu'ils investissent et prennent des risques, créent des emplois, exportent, et sont donc fondés à construire avec l'État une politique industrielle, avec une définition et un pilotage partagés. Les acteurs publics et privés de la filière constituent « *l'équipe de France de la sécurité* ».

Le jeu collectif est donc indispensable pour construire des réponses capacitaires efficaces sur notre sol et à l'export. La participation active des administrations aux indispensables efforts d'exportation doit rompre largement avec les pratiques passées et aligner les modes d'actions

sur ceux de nos concurrents internationaux.

La coproduction de solutions avec les quelques grands groupes nationaux proposant des solutions de sécurité a toujours existé sur l'échiquier national et géopolitique, mais une telle coopération intense est encore très marginale avec les PME, qui sont pourtant la clef de l'emploi et de la création de valeur.

La plupart des ministres et hauts fonctionnaires ont compris la nécessité de ce changement culturel, mais les échelons intermédiaires des administrations prorogent encore les dogmes de séparation auxquels ils ont été formés. Le changement doit donc leur être enseigné. Ceci suppose que soient modifiés les objectifs des missions et les indicateurs qui devraient servir de référentiels communs. Actuellement, il ne s'agit que de simples indicateurs de gestion, justifiés par la recherche d'économies, qui ne coïncident pas nécessairement avec l'intérêt général. A l'instar des entreprises, la prise de risque doit être encouragée, l'échec ponctuel ne devant pas être prétexte à sanction mais plutôt un facteur de compréhension des recettes qui fonctionnent ou pas, donc de perfectionnement. La pratique du code des marchés publics doit être affinée pour favoriser l'anticipation des besoins, par exemple dans les projets coopératifs de R&D de l'ANR⁽⁴⁾, des pôles de compétitivité, de l'Europe, et par un lotissement plus favorable aux PME. Enfin, l'expérimentation et les dialogues

(4) ANR : Agence Nationale pour la Recherche.

précompétitifs doivent être développés. En bref, la filière peut constituer un référentiel commun d'objectifs, de moyens et de pratiques, propice à satisfaire l'intérêt général, mesuré sur l'ensemble de l'écosystème de la sécurité : utilisateurs prescripteurs, chercheurs, industriels, politique, etc.

La gendarmerie et la filière de sécurité

L'étendue de sa présence géographique et la variété de ses missions et moyens ont développé une culture du pragmatisme et de la recherche d'efficacité, bien plus que dans d'autres administrations. La mobilité géographique et fonctionnelle des gendarmes ainsi que leur formation continue ont également permis de développer chez eux une compréhension des systèmes et de leurs interactions complexes. Leur connaissance et leur pratique du droit au contact du terrain constituent un autre atout notable, de même que leur esprit de corps. Enfin, la longue et riche histoire de la gendarmerie et la qualité de réflexion des hommes et des femmes qui composent le corps ont doté l'institution d'une culture de la prospective très utile pour anticiper les réponses capacitaires. C'est d'autant plus précieux que son ministère de tutelle n'est guère équipé pour la prospective.

Quelle contribution pour la gendarmerie nationale ?

Une partie des avantages évoqués précédemment constituent paradoxalement un handicap. Son statut militaire semble davantage propice à

l'exécution de doctrines et d'objectifs traditionnels. Les nouvelles impulsions données par son directeur général actuel et ses cadres visent cependant à transformer progressivement ce handicap en un atout, à travers un système de remontées de suggestions et propositions qui favorise la prise de d'initiatives innovantes.

En ce qui concerne le choix de ses matériels, logiciels et méthodes, la gendarmerie, à l'instar des armées et d'autres administrations, a longtemps privilégié la recherche de solutions de haute performance, avec des impératifs de qualité et de maîtrise élevés non compatibles avec des contraintes économiques de plus en plus prégnantes. La présence souvent consanguine des grands groupes nationaux écarte de nombreuses velléités de PME qui proposent pourtant des solutions innovantes et plus efficaces. Les nombreuses PME membres du GICAT le soulignent souvent et le regrettent. De ce fait, les débouchés de leurs recherches et innovations peinent à trouver leur place dans les marchés publics dont les spécifications sont parfois alignées soit sur les suggestions des grands groupes, soit sur le plus grand commun diviseur des PME. On est là assez loin de l'esprit que la filière nationale de sécurité veut développer et pratiquer. Pour cette même raison, on ne peut que suggérer que les militaires de la gendarmerie de tous rangs développent leur contribution à la défense contre les pressions d'autres administrations et de grands groupes⁽⁵⁾

(5) Les exemples sont nombreux, comme la plateforme nationale d'interceptions judiciaires, les gilets pare-balles, etc.

des outils pointus qu'ils ont fait patiemment développer par des

PME. La légitimité absolue n'est plus toujours là où elle semblait évidente. L'impérative nécessité de l'innovation et la recherche de la performance valent que l'on se positionne avec conviction au regard des pratiques traditionnelles de l'État. Pour modifier progressivement cette culture traditionnelle, la gendarmerie gagnerait à être davantage représentée dans les divers organismes et commissions qui construisent la filière. Quelle que soit la qualité de son représentant, la seule coprésidence du groupe d'expression des besoins de la filière est insuffisante. La structure et l'action du ST(SI)² peuvent se développer dans ce sens avec une présence plus forte au sein de ces instances. Une ressource humaine insuffisante peut être palliée par un recours aux réservistes pour l'épauler dans cette tâche chronophage, parfois frustrante mais indispensable.

Par ailleurs, au niveau national comme au niveau européen, la politique générale redessine les missions prioritaires en fléchissant davantage la gestion des crises et la résilience. Dans ce domaine, le maintien de l'ordre, la gestion des foules et les nouvelles technologies souvent duales se conjuguent avec de nombreuses innovations en termes de doctrine tout comme de solutions. Comme le démontre l'exemple des flottes

aériennes (avions, hélicoptères et bientôt drones), la mutualisation de moyens et de solutions opérationnelles s'impose progressivement. Il est donc indispensable de rapprocher davantage les réflexions et les choix des forces de sécurité tout en intégrant dans la réflexion la sécurité civile, les douanes ou des services du Ministère de l'écologie, du développement durable et de l'énergie. L'intérêt général y prévaudrait bien que cela requière quelque souplesse dans la définition de ses critères spécifiques traditionnels.

La filière nationale de sécurité englobe un ensemble de défis. Les relever avec succès est une nécessité impérieuse pour l'intérêt général du pays, de ses administrations et de ses entreprises.

L'évolution rapide des technologies et leur intégration motivent une adaptation et la mobilisation des initiatives. La gendarmerie possède pour cela de nombreux atouts mais elle doit rapidement s'adapter et prendre des initiatives. A défaut, comme tous les opérateurs majeurs de l'état, elle encourt le risque d'être ostracisée et de voir régresser la satisfaction de ses propres besoins et de ses intérêts. On ne peut que se féliciter que la haute hiérarchie donne l'exemple et impulse les nécessaires ajustements culturels et comportementaux. Pour y contribuer, les réservistes citoyens et opérationnels constituent une ressource d'appoint, de dissémination et de support à sa disposition.

L'impression 3D, enjeux et perspectives

par LAURENT VIDAL

L

La technologie des impressions 3D ou prototypage rapide connaît actuellement des avancées qui la rendent de plus en plus accessible et engendrent espoirs et fantasmes. Les progrès à venir s'agissant des techniques, des matériaux et des prix rendent difficile une juste évaluation de l'impact réel à court terme de cette nouvelle technologie. Pour autant, cette dernière intéresse déjà certains prestataires de services et offre un champ de réflexion sur les notions de propriété intellectuelle et de droits de reproduction.



LAURENT VIDAL

Colonel de gendarmerie,
chargé de mission au
CREOGN.

Des technologies différentes

Les appareils d'impression 3D utilisent différentes technologies. La plus répandue est le dépôt de filament. Les brevets de cette

technologie sont tombés dans le domaine public en 2009, ce qui a contribué à son développement. Il s'agit d'un filament de plastique, chauffé et distribué par une buse, qui est déposé sur un support. La buse est positionnée en abscisses et ordonnées par un bras, la troisième dimension étant assurée par le déplacement vertical du plateau support. Passage après passage, les dépôts se superposent et donnent son volume à l'objet. La résolution de ce type de machine est de l'ordre de 100 microns. Quelques 60 000 machines de ce type sont actuellement utilisées dans le monde.

La seconde technologie est celle de la stéréolithographie. Il s'agit dans ce cas de déposer, selon le même principe, des couches successives de résine. Le procédé permet d'atteindre une définition de 30 à 15 microns. Enfin, certaines machines utilisent des poudres agglomérées avec des encres et une



© doornu

Un marché privé réservé à la décoration et aux objets personnels.

résine faisant office de liant. Il est ainsi possible de créer des objets composés majoritairement d'un métal (titane, or, argent, bronze...) ou d'un autre matériau (plus de 200 matériaux actuellement disponibles pour cette technologie).

Dès aujourd'hui, certains fabricants de machines proposent la technologie DMLS (*Direct Metal Laser Sintering* – frittage direct du métal par laser). Il s'agit de déposer le métal en poudre sur un support et de le fondre sous l'action d'un laser, les couches successives aboutissant à la création d'un objet final en métal pur. Il y a tout lieu de penser que les méthodes de création vont aller en se diversifiant, explorant toutes les possibilités techniques. Pour autant, certaines technologies ne sont pour le moment accessibles qu'aux industriels et

laboratoires, du fait de leur coût et de leur encombrement.

A la recherche d'un modèle économique

Le phénomène de l'impression 3D n'a pas échappé aux entreprises. La Poste a pris une position délibérément novatrice en la matière. Depuis décembre, un service « numérique et impression 3D »

(1) Bureaux de poste de Paris-Bonne Nouvelle, Paris-La Boétie et Boulogne-Billancourt-Hôtel de ville. Voir le site de la Poste (<http://www.laposte.fr/Particulier/Actualites/L-impression-3D-avec-La-Poste>)

est proposé dans trois bureaux de la région parisienne⁽¹⁾.

Confrontée à une baisse de son activité courrier, l'entreprise a en effet engagé une réflexion sur le service qu'elle pourrait proposer dans ses 17 000 points de vente afin de faire venir un nouveau public. Dans ce cadre, la mise à disposition de machines d'impression en

3D dans les bureaux de poste, comme il existe déjà des photocopieuses, a émergé. Cette technologie semble offrir des potentiels intéressants sur le plan commercial mais l'entreprise fait face à une grande inconnue : aucune offre équivalente n'existe et on ne peut préjuger de l'accueil que recevra le nouveau service. Fidèle à sa tradition de démocratisation des technologies, la Poste s'engage néanmoins dans une expérimentation sur un nombre limité de bureaux et pour une durée réduite. Il s'agit de vérifier que le marché existe bien auprès du public et que cette initiative est réellement solvable. La Poste permet dans les bureaux témoins de produire sur place un objet sur une imprimante à filament plastique. Il peut s'agir d'un objet à choisir dans un catalogue de produits existants et personnalisables (coque de téléphone par exemple) ou alors d'un article issu d'un fichier apporté par le client. Une action de conseil est également proposée pour un projet entièrement nouveau. Six salariés, anciens facteurs sans expérience dans le domaine de l'impression 3D, ont suivi une formation pour pouvoir utilement conseiller les clients. Ils ont par la suite rapidement gagné en compétence (intérêt pour la technologie, expérience pratique).

Si l'objectif initial d'augmenter la

(2) Dans les bureaux concernés, une hausse de l'ordre de 1,5 % de la fréquentation a été constatée.

fréquentation semble en partie atteint⁽²⁾, il reste à affiner le dispositif, tant dans

sa forme que dans son principe. La question de la présence physique d'une imprimante dans le bureau se pose. Ne serait-il pas préférable de centraliser la fabrication puisque le principe même du système permet l'envoi de l'ensemble des données de manière immédiate ? Il suffirait alors d'adresser par courrier l'objet à son propriétaire. La contrepartie de cette option est la perte du bénéfice de la rapidité (l'entre avec mon fichier, je ressors avec un objet). S'agissant du prix, l'expérience actuelle a permis de constater qu'il n'est pas un frein pour le client. Les personnes intéressées sont

(3) Le panier moyen est de l'ordre de 100€, les prix s'établissant à partir de 7€ pour les objets basiques.

prêtes à payer pour le service⁽³⁾. C'est l'originalité du

LE PROTOTYPAGE RAPIDE INTÈGRE TROIS NOTIONS ESSENTIELLES : LE TEMPS, LE COÛT ET LA COMPLEXITÉ DES FORMES.

Temps : l'objectif du prototypage rapide est de réaliser rapidement les modèles, dans un but de réduction des temps de développement des produits.

Coût : le prototypage rapide permet de réaliser des prototypes sans qu'il soit nécessaire de recourir à des outillages coûteux, tout en garantissant les performances du produit final. On est donc en mesure d'explorer différentes variantes du produit en cours d'élaboration afin de retenir la solution la plus appropriée.

Complexité des formes : les machines procédant par ajout de matière sont capables de réaliser des formes extrêmement complexes (inclusion, cavité...), irréalisables par des procédés tels que l'usinage par exemple.

produit, son côté unique qui séduisent le consommateur non professionnel. Les professionnels constituent quant à eux une part importante de la clientèle. Il s'agit pour eux de produire à moindre coût un prototype.

S'agissant du produit lui-même, compte-tenu du mode de fabrication par dépôt de filament plastique, la Poste précise bien qu'il ne s'agit que d'objets de décoration. Tant le matériau que le procédé de fabrication ne répondent pas à un usage fonctionnel. Il est actuellement irréaliste, par exemple, d'aller faire fabriquer une pièce de remplacement pour un appareil électroménager. On risquerait en effet des avaries ou accidents plus graves que la panne initiale.

Quant au service proposé, il n'inclut pas de scanner 3D. L'entreprise, dans un premier temps, a en effet souhaité éviter de tomber sous le coup des textes réprimant la contrefaçon. Il ne saurait être question qu'un client réalise lui-même une copie d'un article original avec les machines proposées en libre service. En revanche, un débouché pourrait exister avec la fabrication d'emballages sur mesure pour objets fragiles (l'objet à poster serait scanné puis un moule en « négatif » serait imprimé pour assurer la bonne protection de cet objet). La question de la mise à disposition d'un outil de modélisation en 3D d'un modèle physique reste cependant posée, la Poste approfondissant sa réflexion sur ce sujet. De même, la vente de machines d'impression pourrait à terme être

proposée par la Poste. L'entreprise a décidé de prolonger l'expérimentation de six mois pour continuer son exploration du potentiel commercial de la technologie 3D.

Une effervescence créative et économique

Une génération d'entrepreneurs novateurs et de particuliers créatifs est en train de s'emparer de l'impression 3D car cette technologie offre des possibilités jusqu'alors inaccessibles en termes de production d'objets complexes. Le mouvement des « Makers », aux États-Unis, s'exprime désormais en France où se tiendra les 21 et 22 juin prochains le

(4) Une édition 2013 réduite de cette manifestation a eu lieu à St Malo les 11 et 12 octobre 2013

premier Maker Faire de Paris⁽⁴⁾. Il s'agit de regroupement de personnes adeptes du *Do it yourself* (DIY) et du *Do it with others* (DIWO), à savoir d'individus créatifs et férus de technologie qui partagent leurs compétences avec d'autres pour produire des objets innovants, originaux ou simplement esthétiques. Fonctionnant en dehors de tout système économique, ils mettent en général leurs productions en accès libre, à la disposition de toute personne intéressée pour les utiliser ou les améliorer.

Le Fabshop, *start-up* de Saint-Malo, s'efforce de développer en France l'impression 3D (en vendant des imprimantes et en proposant des services associés). Deux gros constructeurs tiennent pour l'instant la majeure partie du marché. Pour autant, il faut admettre que

la généralisation de cette technologie pour le grand public n'est pas forcément imminente. Il convient de noter que la presse vante des capacités qui n'existent pas encore, du moins pour les machines financièrement accessibles. L'expérience montre que les actuels possesseurs d'imprimantes sous-utilisent systématiquement leur matériel et que les logiciels restent complexes à utiliser. Enfin, les produits finis ne répondent à aucune norme de fabrication ce qui limite fortement l'usage des objets créés.

Le potentiel industriel, en revanche, est extrêmement prometteur et intéresse les professionnels. Le procédé permet d'envisager la fabrication distribuée qui génère une source d'économies substantielles et une solution aux problèmes de flux tendus car au lieu de stocker et d'envoyer des pièces, on les fabrique à la demande, sur place. De manière paradoxale, cette technologie de pointe pourrait se développer efficacement dans certains pays économiquement sous-développés. Elle permettrait par exemple, pour les victimes des pays en guerre ou infestés de munitions non explosées, de produire des prothèses à bas coût, adaptées à la morphologie exacte du patient et renouvelables en cas d'usure ou de croissance de l'intéressé. Dans le domaine médical encore, la presse a récemment illustré les capacités nouvelles

offertes aux chirurgiens⁽⁵⁾. Les nouvelles

(5) <http://www.sciencesetavenir.fr/sante/20140227.OBS7957/le-c-ur-d-un-bebe-opere-grace-a-une-impression-3d.html>

technologies d'impression, utilisant des métaux, des matériaux biodégradables et différents produits susceptibles d'être intégrés dans les résines servant à l'impression, ouvrent des perspectives quasiment infinies. On peut envisager à très court terme la production de pièces industrielles et fonctionnelles en matériaux composites mais aussi en métal. Sur le plan économique, plus la pièce à produire est complexe et plus le procédé est rentable car les économies réalisées sur la création du moule ou l'usinage sont plus importantes. La technologie de la construction par dépôts successifs offre également la possibilité de créer des structures alvéolaires et, par conséquent, d'économiser sur la matière première.

Pour aller encore plus loin, les chercheurs travaillent actuellement à une impression 4D qui donne à l'objet dès sa fabrication des fonctionnalités précises. Ce peut être par l'utilisation d'un matériau à mémoire de forme qui, sollicité par les conditions de chaleur ou de luminosité, modifiera la configuration de l'objet. Lors de l'impression, l'inclusion dans le produit de composants électroniques donnera immédiatement à ce dernier une capacité de connexion.

Un dispositif juridique suffisant

Le risque principal de la technologie des impressions en 3D a d'ores et déjà été identifié tant par les grandes marques que par les créateurs et certaines administrations, notamment les douanes : il s'agit de la contrefaçon. La grande prudence de la Poste, déjà évoquée, se

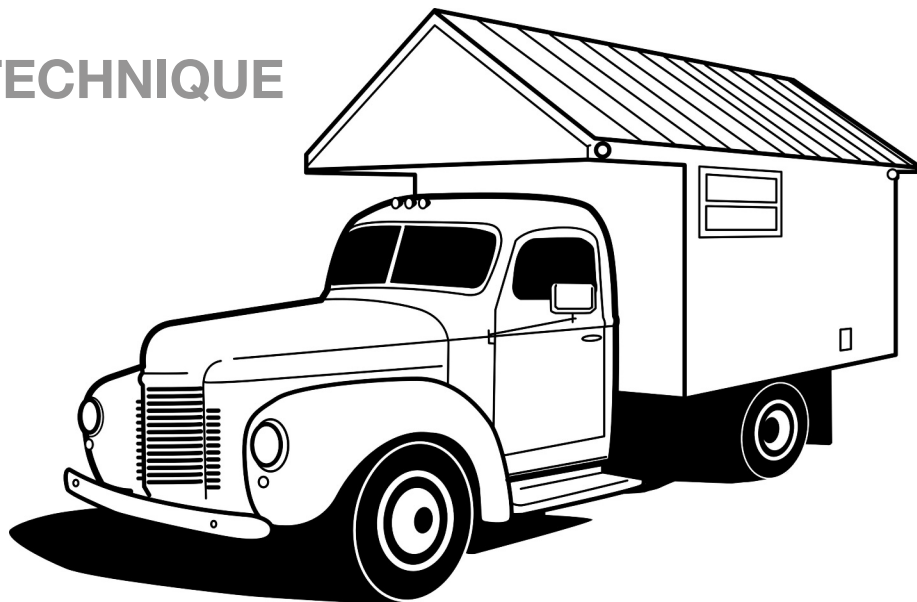
justifie par la facilité théorique de reproduction d'objets de tous types.

Le problème qui se pose est principalement celui de la propriété intellectuelle. Plus que d'objets, on parle de fichiers servant à créer des objets. A l'analyse cependant, il apparaît que si la technologie est nouvelle, la question est déjà traitée dans notre législation pour d'autres formes de duplication et de copie. Comme la reproduction en deux dimensions, la création d'objets en trois dimensions est régie par le droit au nom, le droit des marques et celui des brevets. En conséquence, il ne semble pas nécessaire de légiférer spécifiquement pour la 3D. En revanche, il faut vraisemblablement s'attendre à un contentieux en hausse tant il semble évident que des délinquants astucieux tenteront rapidement, notamment par le biais d'internet, de vendre des objets copiés ou contrefaits. Le marché florissant des figurines de héros de BD ou de film, par exemple, se prête déjà à ce genre de détournements. Lorsqu'il s'agira de pièces détachées pour l'automobile, l'électroménager ou le bâtiment, les risques pour la sécurité publique seront bien réels.

Pour autant, les activités délinquantes utilisant la technologie de l'impression 3D ne se limiteront pas aux atteintes à la propriété intellectuelle. Les médias ont donné un large écho à la mise en ligne des fichiers permettant de construire une

arme à feu. L'intérêt réside dans le fait de produire une arme qui ne ressemble pas à un pistolet classique et qui, sans pièce métallique, peut passer un contrôle par détecteurs de métaux. Si des munitions parviennent à être produites selon les mêmes critères, il y a un risque notamment en matière de sécurité aérienne mais aussi pour l'ensemble des enceintes sensibles nécessitant une sécurité importante. Enfin, notons que la possibilité d'inclure dans la matière utilisée pour l'impression des substances stupéfiantes ouvre *a priori* aux trafiquants de nouvelles possibilités pour l'exportation de leurs produits. Néanmoins, s'agissant des armes comme des stupéfiants, l'arsenal juridique existant suffit et il n'est nul besoin de nouvelles incriminations.

La technologie de l'impression 3D offre à l'imagination des entrepreneurs, des créateurs et des délinquants des perspectives inédites. Dans un domaine en évolution rapide, il importe d'être attentif à toutes les déviances potentielles. Pour autant, il convient également d'être imaginatif pour saisir toutes les opportunités qui ne manqueront pas de se présenter aux services de prévention et de répression de la délinquance.



L'UTILITÉ SOCIALE DE LA VOITURE ?

- > Son devenir ?
- > Le véhicule sera un lieu de vie ?
- > Nouvelle forme de sociabilisation ?

- Conçu comme un moyen de transport de biens puis de personnes, la voiture évoluera vers le concept d'un vecteur régulé par les dispositifs d'une ville "intelligente" aux infrastructures interactives.
- Libéré des contraintes du pilotage, le véhicule automatique, sera un lieu de vie confortable, moyen de déplacement automatisé sûr. Il constituera, moyennant un équipement adéquat, une nouvelle forme domiciliaire.
- Le véhicule automatique modifiera les rapports sociaux. Il réinsérera les personnes âgées ou handicapées qui étaient privées d'un moyen de locomotion et simplifiera les approvisionnements des foyers et les migrations quotidiennes : accompagnement des enfants lors de leurs activités, livraison, trajets domicile-travail, liaisons hôpital-domicile, etc.

Les évolutions majeures des véhicules de demain

Interview de **THIERRY ARCHAMBAULT**

P

La revue : pourriez-vous nous donner votre sentiment sur les évolutions technologiques majeures qui caractériseront les véhicules de demain ?

M. Thierry ARCHAMBAULT : l'ensemble des recherches effectuées par les constructeurs porte sur toujours plus de sécurité, plus de confort, plus d'information et plus d'écologie, ces grandes mutations étant rassemblées aujourd'hui sous le terme de « *véhicule intelligent* ».



THIERRY ARCHAMBAULT

Président du CSIAM, forte expertise du monde automobile et de ses usagers

L. R. : s'agit-il d'une rupture entre le véhicule d'aujourd'hui et le véhicule de demain ?

T.A. : Oui et non. Oui, si l'on compare un véhicule des années 1960 avec ce que

sera celui des années 2020. Pour résumer, schématiquement, le conducteur des années 1960 devait piloter sa voiture, celui des années 2020 la conduira avec un co-pilote embarqué, la voiture elle-même.

Mais ce résultat s'inscrit dans une évolution continue du produit automobile vers toujours plus d'assistance aux usagers. Prenons un exemple particulièrement parlant, celui du freinage. Les études d'accidentologie ont mis en lumière que bon nombre d'accidents auraient pu être évités si le conducteur avait réduit sa distance de freinage d'un mètre, chose possible s'il avait su particulièrement bien freiner. Les mêmes études ont également mis en évidence qu'apprendre à très bien freiner à tous les conducteurs relevait de la mission impossible. C'est pourquoi est née très vite l'idée que la solution passait par la dotation sur le véhicule de

dispositifs d'assistance permettant d'atteindre un niveau d'excellence au freinage sans pareil. Ainsi est né l'ABS qui évite de bloquer les roues et permet de freiner tout en gardant la possibilité de changer la trajectoire du véhicule.

Le système s'est perfectionné avec l'apparition des dispositifs de freinage intelligents : selon la façon dont le pied du conducteur attaque la pédale de frein, le véhicule « *comprend* » qu'il y a situation d'urgence et il engage un freinage maximum immédiatement. Enfin, il existe aujourd'hui sur certains véhicules, couplés à ces précédents systèmes, des radars embarqués qui détectent des obstacles sur la route, par exemple dans le brouillard, et qui déclenchent le freinage du véhicule indépendamment du conducteur dès lors que la situation l'exige.

L.R. : comment ces dispositifs arrivent-ils dans l'automobile ?

T.A. : ils trouvent souvent leur origine dans l'aéronautique. Leurs premières applications routières sont déployées successivement dans les camions, les voitures puis les deux-roues à moteur, une fois la miniaturisation rendue possible par les services de recherche et développement. L'ABS mais également les correcteurs de trajectoire (ESP) en sont deux exemples marquants.

L.R. : dans quels domaines les constructeurs travaillent-ils à l'avènement du véhicule intelligent ?

T.A. : le premier domaine qui a été largement investi concerne la sécurité des usagers. Dès ses débuts, l'automobile n'a eu de cesse d'apporter davantage de sécurité à ses utilisateurs. Je pense ici à tous les dispositifs que l'on rassemble sous le vocable de sécurité active. Alors que la sécurité passive concerne ceux qui interviennent au moment du choc, par exemple l'airbag, la sécurité active caractérise ceux qui interviennent avant l'accident, pour l'éviter ou en limiter les conséquences, par exemple les dispositifs d'assistance au freinage, de contrôle de l'accélération, de maintien de la trajectoire, mais aussi le pré-tensionneur de ceinture, l'avertisseur sonore d'endormissement du conducteur, les systèmes vibratoires en cas de franchissement de la ligne continue, les radars détecteurs d'obstacles, les caméras de recul, etc. Le véhicule de demain ira plus loin encore par son interconnexion avec les autres véhicules en circulation et l'environnement routier.

L.R. : quels sont les dispositifs qui verront le jour à très brève échéance ?

T.A. : d'ores et déjà, roulent des véhicules qui reçoivent des informations sur les conditions de trafic et qui lisent les panneaux routiers. Demain, les véhicules et les routes échangeront des

informations sur les conditions de circulation et les éventuels dangers de la route dans le but d'optimiser la fluidité du trafic et d'offrir davantage de confort pour les usagers et d'écologie pour tous.

Les véhicules recevront également toutes les applications smartphones d'aide à la mobilité. Plus encore, ils communiqueront également avec leur réseau de marque sur les opérations de maintenance à effectuer. Ainsi avant même de se rendre chez le concessionnaire, celui-ci aura été informé des pièces à commander permettant un gain de temps considérable pour l'utilisateur. Ce point intéresse en premier lieu les utilisateurs de camions.

Le véhicule intelligent aura aussi les ressources embarquées nécessaires pour optimiser son rendement moteur en fonction du profil géographique du trajet pour toujours plus d'écologie.

L.R. : jusqu'où peut-on envisager d'aller dans ce domaine ?

T.A. : techniquement le véhicule automatisé sans conducteur est possible. Les principaux obstacles à son avènement relèvent beaucoup plus d'aspects d'acceptation sociale ou de difficultés juridiques complexes à résoudre, notamment en termes de responsabilité.

Peut-on envisager des applications au niveau judiciaire ?

T.A. : ce point n'est pas la préoccupation première des constructeurs dont la mission consiste à mettre sur le marché des véhicules toujours plus sûrs correspondant aux attentes de leurs clients. Il est toutefois très vraisemblable que l'ensemble de ces évolutions trouvera des applications concrètes pour les forces de l'ordre, notamment la possibilité pour chaque véhicule d'avoir une puce électronique permettant de l'identifier. Mais là aussi des obstacles juridiques doivent être levés par le législateur avant d'envisager tout développement industriel.



CHANGEMENT DE STATUT POUR LE VÉHICULE DU FUTUR

> Le véhicule peut-il devenir un moyen
de tracabilité judiciaire ?

> Le véhicule perdra-t-il son statut maté-
riel ?

> Un véhicule connecté sera-t-il
l'objet de nouvelles infractions ?

● L'emploi de ses moyens de communication, mixant des médias différents, fixe une mémoire de l'activité de son occupant : déplacements, appels téléphoniques, échanges d'images et de vidéos, etc. Les anciennes techniques de marquage sont obsolètes.

● Le véhicule étant immatriculé, quasiment inexpugnable sauf autorisation du propriétaire ou réquisition de justice, le mode probatoire se portera lentement sur la valeur des informations dématérialisées qu' il détient et émet.

● Ouvert sur le monde numérique, il sera « hacké » par des spécialistes, générant de nouveaux moyens d' attentats, accident provoqué, etc.

Véhicule communicant

intelligent ou autonome

par **STÉPHANE MILET** et **Pascal CHEYLAN**



Il y a exactement 50 ans, l'écrivain Isaac ASIMOV déclarait : « *Beaucoup d'efforts seront mis dans la conception de véhicules avec "robot-cerveau" — des véhicules qui peuvent être paramétrés pour des destinations particulières et qui s'y rendront ensuite sans l'interférence des réflexes lents d'un conducteur humain* »⁽¹⁾.

(1) Tribune publiée le 16 août 1964 dans le *New York Times* et traitant « des merveilles technologiques qui seraient [un jour] à disposition des hommes »

Force est de constater que ce maître de la science-fiction avait finalement vu juste.



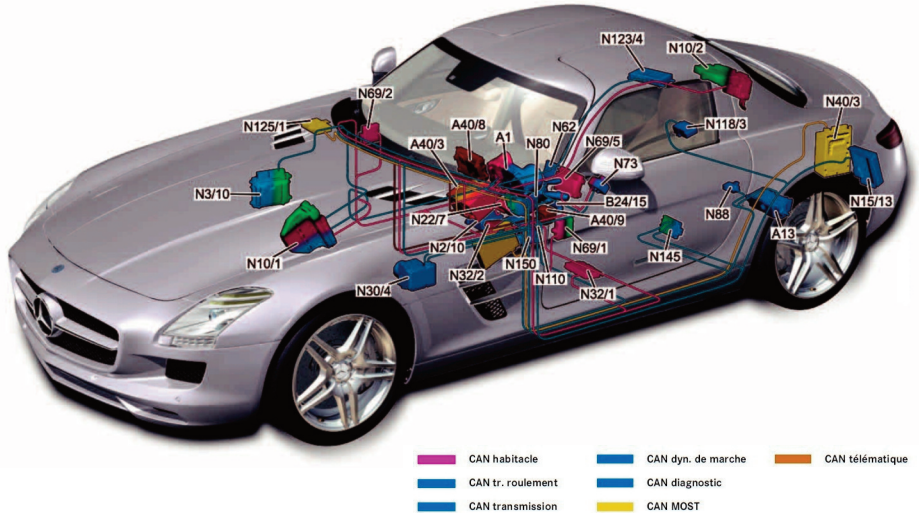
STÉPHANE MILET
officier de gendarmerie,
chef du département
véhicule de la division
criminalistique ingénierie
et numérique,



PASCAL CHEYLAN
officier de gendarmerie,
chef de la division
criminalistique ingénierie
et numérique de l'IRCGN.

Ainsi, depuis plus de 10 ans maintenant, le véhicule, objet technologique de pointe, a entamé une mutation sans précédent. De simple moyen de transport mécanique, il devient résolument un objet communicant, intelligent voire autonome. Freinage automatique d'urgence chez Volvo et notamment Volvo-Trucks, fonctions activables par smartphone chez BMW, stationnement automatique, jusqu'à la conduite sans intervention humaine dont la *Google-car* est le meilleur exemple mais non le seul.

Ces nouvelles technologies, qui ont pour objectif le plus avouable de rendre plus sûre la route (objectif 0 mort en 2050 nous annonce l'Europe), ont dans le même temps créé tout un cortège de fantasmes liés aux possibilités qu'elles offriraient potentiellement aux hackers de tout bord. Ainsi, puisqu'un ordinateur domestique peut faire l'objet de cyber-



Réseaux CAN & MOST sur un véhicule Mercedes haut de gamme.

attaque (cf. le précédent numéro de La revue de la gendarmerie nationale), qu'en est-il de cet ordinateur roulant que tend à devenir le véhicule ? D'ailleurs tout le monde à entendu ces témoignages d'automobilistes déclarant avoir perdu le contrôle de leur régulateur de vitesse. Et s'il s'agissait d'expériences de prise de contrôle extérieur ? L'apothéose a pour l'instant été atteinte en juin 2013, quand le journaliste Michael Hastings s'est tué dans un accident de la route, alors qu'il venait d'annoncer quelques heures auparavant la divulgation très prochaine d'un scoop qui ferait l'effet d'une bombe. Accident bizarre, s'il en est, nous dit-on là aussi : au volant de sa Mercedes C250

dernier cri, et donc bardée d'électronique, il vient percuter tout seul un arbre. *Quid* d'une intervention malveillante externe ?⁽²⁾

(2) Voir à ce sujet l'article de Carl Gibson paru le 26 octobre 2013 sur le site Global Research (<http://www.globalresearch.ca/who-killed-michael-hastings/5355606>)

Bien entendu, aujourd'hui, tout cela peut prêter à sourire. Mais demain...

Une communication fonctionnellement différenciée

Un questionnement subsiste quant à l'objectif du concepteur du véhicule. En effet, en prenant les caractéristiques de communication, d'intelligence et d'autonomie, on peut considérer que le danger potentiel va croissant.

Ainsi, le véhicule communicant ne fait qu'échanger des informations. Il importe d'ailleurs de distinguer sa communication interne et sa communication externe. La révolution de la communication interne est déjà largement dépassée, puisque la plupart des véhicules commercialisés actuellement contiennent un très grand nombre de calculateurs (plus d'une soixantaine pour certains modèles haut de gamme) gérant une grande partie des fonctionnalités du véhicule (airbags, gestion moteur, suspension, ABS, toit ouvrant, boîte de vitesses automatique, réfrigération...). Ces calculateurs

(3) Les réseaux CAN (Controller Area Network – développé par BOSCH) ou VAN (Vehicle Area network – développé par PSA et Renault mais qui tend à disparaître au profit du premier) permettent les échanges d'information entre calculateurs à bas débit.

(4) Notamment grâce au développement du réseau MOST ou *Media Oriented System Transport* dont la vitesse de transfert de donnée est de 22 Mbit/s

communiquent via le réseau CAN ou VAN⁽³⁾, encore limité par la vitesse d'échange de donnée (500 kBits/s maximum).

La communication vers l'extérieur est en revanche en plein

essor⁽⁴⁾. Sous cette expression se cache tout simplement la capacité du véhicule à échanger des données avec une infrastructure dédiée (V2I ou *Vehicle to Infrastructure*) mais aussi avec les autres véhicules situés dans son environnement proche (V2V ou *Vehicle to Vehicle*). Les informations émises sont principalement liées à la dynamique du véhicule (vitesse, position) tandis que celles reçues porteront sur les conditions de trafic, la

présence d'un danger imminent, etc. L'objectif premier est de diminuer les accidents, le deuxième de fluidifier le trafic routier mais bien d'autres existent, comme la création de nouveaux services

(5) Voir à ce sujet l'article de S. Darracq paru dans l'édition électronique du Monde du 14 janvier 2014

commerciaux à grande valeur ajoutée.⁽⁵⁾

Les projets concernant le véhicule communicant sont divers et nombreux. Ainsi, Google a annoncé début janvier 2014 la création de « *Open Automotive Alliance* », alliance regroupant Google, Audi, Hyundai, Honda et General Motors. L'idée est d'uniformiser les systèmes d'exploitation internes à la voiture avec ceux des portables ou des ordinateurs personnels. Le prolongement logique de cette alliance serait de développer un langage universel en V2V. Microsoft coopère, pour sa part, avec Ford, dans le même sens.

Partout dans le monde, on parle de développer des axes routiers équipés de bornes wifi assurant ainsi une parfaite communication V2I. En France, le premier axe équipé pourrait aller de Bordeaux à Vienne en passant par Paris, Strasbourg, Rotterdam et Francfort et ce à l'horizon 2016.

Le véhicule intelligent, quant à lui, va nettement plus loin. En effet, même s'il n'est pas question ici d'intelligence artificielle, ce véhicule possède par définition la capacité à agir et réagir,

notamment en palliant à une absence de réaction du conducteur. Aujourd'hui plusieurs constructeurs proposent des fonctions intelligentes sur leur véhicule parmi lesquelles le freinage d'urgence en cas de danger identifié et d'absence de réaction du conducteur, le maintien des distances de sécurité lorsque le régulateur de vitesse est enclenché, la correction de trajectoire en cas de franchissement de ligne blanche et enfin le pilotage de la direction pour garer le véhicule.

La somme de ces deux qualités, la communication et « *l'intelligence* », ouvrira de nouvelles perspectives et des progrès certains. En matière d'accidentologie, elle permettra d'éviter un grand nombre d'accident ou de minimiser les dégâts par une réaction adaptée du véhicule qui reçoit l'information de danger immédiat. Ainsi par exemple, si l'infrastructure à un carrefour détermine qu'un véhicule, en raison de sa vitesse élevée, va griller le feu rouge, le stop ou la priorité, alors ce véhicule pourra prévenir ce danger et alerter son propre conducteur voir freiner si celui-ci ne réagit pas. Elle participera à la fluidification du trafic en adaptant d'une part la vitesse du véhicule au trafic mais aussi en optimisant les déclenchements des feux rouges.

Le véhicule autonome, enfin est une voiture capable de rouler automatiquement en toute autonomie dans le trafic réel et sur une infrastructure

non spécifique sans l'intervention d'un être humain. C'est une application typique du domaine de la robotique mobile. On a déjà évoqué en début d'article le google-car, mais d'autres exemples existent, tout aussi époustoufflants. Ainsi, au dernier *Consumer Electronical Show* qui s'est déroulé du 7 au 10 janvier dernier à Las Vegas (USA), on a pu voir une présentation dynamique de la BMW M235i, capable de rouler à grande vitesse et d'éviter toute sorte d'obstacle sans aucune intervention humaine, et qui se montre même capable de rattraper un

(6) film à l'adresse suivante : http://www.youtube.com/watch?feature=player_embedded&v=ILmMPWT7s

dérapiage dans un virage sur route mouillée (6).

A terme le véhicule devrait pouvoir circuler en totale autonomie à basse vitesse puis plus tard quelque soit sa vitesse.

Source potentielle de risques ou de dangers pour ses utilisateurs...

Comme indiqué précédemment, le véhicule simplement communicant est en principe peu vulnérable. Toutes les données, internes ou externes, qu'il reçoit ou qu'il émet, ne sont pas sensées influencer directement la bonne marche du véhicule. Le conducteur demeure le point de passage obligé entre l'information reçue et l'action qu'elle entraîne. Il faut noter cependant que le réseau interne au véhicule, (passant notamment par l'émergence des clés électroniques et des anti-démarrage codé sensée assurer une diminution des vols)

a fait l'objet dès son apparition de multiples attaques physiques. Ainsi, le piratage de ces systèmes a provoqué l'émergence sur internet de sites qui commercialisent des outils électroniques pour inhiber l'anti-démarrage ou programmer une nouvelle clé sur le véhicule. Ils sont d'un usage simpliste à l'extrême et vendus à des prix très compétitifs. Ces systèmes ont aussi grandement facilité le trafic des compteurs électroniques. Là encore l'outillage est simple d'utilisation, en vente sur internet et la manipulation est très difficilement détectable. On notera toutefois qu'il est nécessaire pour le malfaiteur de se connecter au véhicule via la prise OBDII (*On Board Diagnostic 2^e génération*) ou au moins en se branchant au circuit.

Alors que les principales violations électroniques de véhicules simplement communicant ont pour but aujourd'hui de dérober ce dernier, il n'est pas incongru de penser que demain la finalité sera de prendre le contrôle à distance du véhicule intelligent. Cette action pourrait avoir pour but de le voler beaucoup plus facilement (en déverrouillant à distance les portes par exemple), mais surtout de l'arrêter voire le conduire dans un lieu isolé pour mieux s'en prendre à ses occupants, voire de provoquer son accident ou encore pire de l'utiliser pour créer un carambolage. Tout est imaginable si l'on considère que

l'occupant peut ne plus être maître de son véhicule. Lors de la dernière DEFCON⁽⁷⁾, plusieurs présentations portaient sur le piratage de voiture. L'une d'entre elles fut grandement médiatisée. En effet, deux chercheurs en sécurité ont réussi à l'aide d'un ordinateur portable et via une connexion filaire, à prendre le contrôle d'un véhicule Toyota plus particulièrement au travers de ses fonctions de direction, de freinage et d'accélération entre autres.

Nul doute que ce qui a été réalisé via une connexion filaire pourrait l'être aussi via une connexion sans fil. En effet, on peut raisonnablement penser qu'il existera à terme une passerelle entre le réseau qui supporte les différents calculateurs électronique de gestion du véhicule et celui qui supporte les fonctions dites de confort accessible via une connexion sans fil de type GSM aujourd'hui et wi-fi demain. En effet, il s'agit d'une condition *sine qua non* de l'existence du véhicule autonome.

En fait, sur certains véhicules, il semble bien que cette passerelle existe déjà, en témoigne le logiciel « *Connected drive* » de BMW qui permet avec son smartphone et sans limite de distance d'allumer les feux, d'enclencher le klaxon, mais aussi les GPS embarqués qui récupèrent une information de vitesse via un capteur interne au véhicule.

... et de nouvelles opportunités pour les forces de l'ordre

Bien entendu, l'implémentation de ces nouvelles technologies laisse entrevoir une multitude de possibilités pour aider les forces de l'ordre dans leur travail quotidien.

Ainsi, la multiplication de ces calculateurs rend le maquillage du véhicule plus difficile, puisqu'il est possible de lire chaque numéro indépendamment. Malheureusement cette lecture n'est encore réservée qu'aux seuls spécialistes qui ont accès à des outils spécifiques et coûteux. L'avenir réside donc dans la création de mallettes de diagnostic universelles.

En matière d'accidentologie, certains de ces calculateurs devraient aussi permettre de retrouver des données liées à la dynamique du véhicule quelques millisecondes avant l'accident. Actuellement ces données sont extraites par le constructeur ou l'équipementier pour le compte de l'expert. La recherche va dans la sens d'une création de mallettes de diagnostic permettant de lire toutes les données intéressant l'expert mais pas forcément le constructeur du véhicule et/ou son réseau interne.

En matière de réseau externe du véhicule communicant, une des fonctionnalités les plus précieuses est à n'en pas douter l'utilisation des données de géolocalisation. En effet, pour

communiquer sur le réseau le véhicule devra s'authentifier vraisemblablement à l'aide d'un certificat numérique. Si ces messages sont stockés sur un serveur et si les forces de l'ordre sont autorisées à faire des requêtes sur ce serveur alors les possibilités sont nombreuses : géolocalisation d'un véhicule volé (déjà réalisable actuellement sur certains véhicules), recensement de tous les véhicules présent dans une zone où a eu lieu un accident avec délit de fuite, suivi en temps réel d'un véhicule suspect et à distance et identification du cheminement d'un véhicule sur une période donnée...

Bien évidemment, ces données sensibles présentes sur les réseaux auront tôt fait d'être « hackées ». Il importe donc dès à présent d'envisager les possibilités de les protéger ou à minima de mettre en évidence toute manipulation. Au delà du GPS, c'est l'ensemble de la télématique et même de l'électronique embarquée qui pourra faire l'objet d'attaques.

Enfin, on peut noter que le contrôle routinier de véhicule s'en trouverait facilité puis qu'avec un simple lecteur il serait possible de vérifier si il y a adéquation entre l'identité numérique du véhicule et son identité physique représentée par son numéro de série frappé. Le maquillage du véhicule serait alors beaucoup plus compliqué.

Dans le même ordre d'idée, en équipant les radars automatiques d'une balise,

l'identité d'un véhicule « flashé » pourrait être vérifiée avant de valider l'infraction. D'ailleurs, en allant encore plus loin, il serait possible de supprimer tous les radars automatiques, puisque en permanence le véhicule communiquerait sa vitesse à l'infrastructure (environ 10 fois par seconde), qui pourrait ainsi en permanence transmettre aux autorités des signalements d'excès de vitesse ! Même Isaac Asimov n'y aurait pas pensé mais nous n'en sommes pas encore là.

La directive 2010/40/UE du parlement européen et du conseil du 7 juillet 2010 est venue fixer le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres

(8) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:fr:PDF>

modes de transport⁽⁸⁾. La gendarmerie, en

charge notamment de la police des flux, y est naturellement partie prenante. Afin de se préparer aux nombreux défis que représentent le véhicule intelligent et le véhicule autonome, elle se doit donc de poursuivre ses efforts pour anticiper toutes les évolutions prévisibles. Il est ainsi important qu'elle soit représentée dans les groupes de travail, essentiellement constitués de constructeurs, qui discutent aujourd'hui des normes et standards de demain entrant dans le cadre de la directive. C'est à cette condition seulement qu'elle pourra, au plus tôt, essayer de faire

prendre en compte les impératifs et besoins des forces de l'ordre dans l'architecture future de ce qui sera le « *Big Data* » du transport.



LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (TIC) ET LES VECTEURS DE TRANSPORTS

> Quels sont les enjeux ?

> Peut-on créer une interface mondiale ?

> Vers quoi tendent les nouvelles technologies ?

● Chaque fournisseur de technologies numériques cherche une hégémonie mondiale mais seules les normes permettent le partage des fréquences d'utilisation, les interopérabilités entre produits et un dialogue entre les acteurs (*car to car et car to infrastructures*)

● Les TIC doivent contenir une interface homme-système embarquée intuitive et intelligible à la clientèle mondiale notamment entre les sensibilités européennes et asiatiques.

● Les TIC provoquent une généralisation des services qui doivent coexister de manière cohérente (systèmes de guidage, gestion des trajets, services de communication, couplage avec la téléphonie mobile, capacité de paiement, gestion des flux vidéos, etc.). Un nouveau défi pour les constructeurs automobiles.

Les TIC

s'emparent du volant

par **CAROLE LEMBEZAT**

P

Poussée par les progrès technologiques et la pression croissante des utilisateurs, la voiture connectée entre en scène. Avec elle se dessinent de nouveaux enjeux, de nouveaux usages, mais aussi un écosystème en pleine mutation. En toile de fond, elle préfigure un modèle économique qui reste à accompagner et à normaliser.

« Hier, les rois de la voiture étaient mécaniciens. Aujourd'hui, ce sont des geeks. ». Si cette formule – qui commence à circuler ! – n'est pas une vérité absolue, on ne doit pas pour autant la prendre à la



CAROLE LEMBEZAT

Journaliste spécialisée en économie et industrie
Alliancy le mag

légère. L'entrée dans l'ère de la connectivité implique un véritable changement de paradigme dans de nombreux secteurs, en particulier pour les constructeurs automobiles. « Cela

fait dix ans que l'on nous dit que les services de télématique embarquée vont décoller », constate Rémi Cornubert, directeur au cabinet de conseil en stratégie Oliver Wyman. « *La différence, aujourd'hui, c'est que les réseaux de télécommunications ont considérablement progressé.* » A cela s'ajoute l'habitude que nous avons prise d'être connectés en permanence.

« *C'est le croisement entre la technologie et la demande client qui tire le marché »,* souligne-t-il.

Pour une conduite plus sûre

L'automobile devient une composante d'un monde où 24 milliards d'objets seront connectés en 2020, selon la GSMA (Association des opérateurs mobiles à l'échelle internationale), contre 9 milliards en 2011. « *Or, il s'agit d'un appareil particulier dans un contexte particulier »,* insiste Julien Clause, directeur marketing d'*Intelligent Systems* (Altran Group). Avec leurs différents



© charmillev

L'enjeu des normes de connexion et des mises à jour des logiciels.

partenaires, les constructeurs s'attachent à développer des fonctionnalités compatibles avec la sécurité routière, comme la reconnaissance vocale, et améliorent l'interface homme-machine avec des boutons plus gros et un fonctionnement plus intuitif. Il s'agit en effet de bien prendre en compte ces spécificités afin que la connectivité à bord garantisse la sécurité des passagers, voire l'améliore ! Certains imaginent déjà des services allant dans ce sens. Marc Pajon, en charge des projets avancés pour la vie à bord, la sécurité et la performance dynamique chez Renault développe : « *Si une voiture dérape sur une plaque de verglas, elle pourrait transmettre l'information*

géolocalisée. Une zone à risques pourrait être signalée aux autres usagers, un peu sur le même principe que le système Coyote. » Cela nécessite d'agréger les données ainsi récoltées. « *Il va falloir mettre en place un modèle probabiliste pour identifier la source du danger* », complète Marc Pajon, « *mais aussi un algorithme suffisamment puissant pour que le véhicule comprenne son environnement et le retranscrive de façon fiable.* »

Incitations réglementaires

Les évolutions réglementaires pourraient aussi contribuer à accroître le taux de pénétration des appareils connectés, comme la voiture. A titre d'exemple, la Commission européenne travaille à la mise

en place, d'ici à 2015, de l'eCall, un système d'appel d'urgence automatique en cas d'accident grave. Les nouvelles voitures devront être dotées d'un module de communication avec carte SIM intégrée. La Commission exhorte les États membres à garantir que les opérateurs de téléphonie mobile traitent ces appels de façon prioritaire et gratuite. « *Mais on ne s'est toujours pas mis d'accord sur qui paie quoi, du constructeur, de l'opérateur ou du client...* », déplore Jacques Garcin, directeur automobile et télématique chez Orange, qui estime que l'opérateur ne peut assumer seul les coûts imposés par ce système. « *Il faudrait des fonds européens pour amorcer la pompe* », avance-t-il. En attendant, certaines marques proposent déjà des solutions de ce type. C'est le cas de Peugeot, notamment, ou de Ford qui, lui, a choisi d'utiliser les téléphones du conducteur, ou des passagers connectés en bluetooth avec le véhicule, pour passer ces appels. Depuis quelque temps, la « *voiture connectée* » suscite une grande effervescence. Les derniers salons internationaux du secteur, à Paris ou Genève, regorgeaient de démonstrateurs. Les tables rondes sur le sujet se multiplient et la « *Journée mondiale des Télécommunications* », le 17 mai 2013, l'avait mise à l'honneur. Renault vient de lancer, en partenariat avec la SSII (ESN, pardon !) Atos et l'Université Pierre et Marie Curie (UPMC), la chaire « *Smart & Connected Mobility* », consacrée à la voiture connectée. Même l'IT Challenge d'Atos lui était dédié cette année.

Un monde en ébullition

Ce bouillonnement reflète l'intérêt que l'ensemble des acteurs de l'industrie traditionnelle de l'automobile et celle de l'IT portent à la voiture connectée et à son nouvel écosystème. « *Il y a la connectivité entre la voiture et les appareils nomades du client ; la connectivité par réseau téléphonique ou par Internet. Nous allons aussi utiliser beaucoup de canaux comme la radio et la télévision numériques et, plus tard, la connexion car-to-car et car-to-infrastructure* », énumère Thierry LeHay, responsable des innovations dans le domaine IHM (interface homme-machine), connectivité chez PSA Peugeot-Citroën. « *Les usages et les canaux sont très variables d'un pays à l'autre* », poursuit-il. « *Nous devons être capables d'être connectés par tous les canaux possibles.* » Avec tous ces modes de communication se profilent de nouveaux usages et de nouveaux services associés, en plus de l'infotainment (information et divertissement) dont tout le monde parle. Votre voiture pourrait, par exemple, faire remonter à votre assureur des informations sur la façon dont vous conduisez et le nombre de kilomètres que vous parcourez. Ce dernier pourrait alors vous proposer un mode « *Payd* » (pour *Pay as you drive*). « *Techniquement, c'est possible. Cela existe déjà aux Etats-Unis et en Italie* », affirme Patrick Pelata, responsable du secteur automobile chez l'éditeur Salesforce.

Examens de conduite

En France, certains assureurs offrent déjà le paiement au kilomètre, basé sur du

déclaratif. D'autres, comme Amaguiz, la filiale de vente d'assurance en ligne de Groupama, proposent des solutions aux kilomètres réellement parcourus, moyennant l'installation d'un boîtier dans votre véhicule. En revanche, les informations liées à votre comportement au volant (type de trajets, respect des limitations de vitesse, utilisation des rapports de vitesse, etc.) ne font pas partie des données remontées à l'assureur. La maintenance préventive, exploitant là encore des données transmises du véhicule à des centres de traitement, fait partie des possibilités envisagées. Bouygues Telecom, en partenariat avec PSA Peugeot-Citroën et Via Michelin, propose un outil qui calcule en temps réel un itinéraire de délestage lorsqu'une congestion du trafic a été identifiée par le ralentissement de la voiture. « *On apporte une vraie dimension de temps réel par rapport aux solutions basées sur le TMC véhiculé par la bande FM* », assure Jean-Luc Gonzalez, directeur projet voiture connectée chez Bouygues Télécom.

Une myriade de nouveaux services

C'est ainsi qu'émerge une myriade de nouveaux services, allant du covoiturage à l'optimisation du carburant. La voiture connectée pourrait même contribuer à la progression du véhicule électrique. « *Avec l'un de nos partenaires, nous avons conçu un système pour optimiser la recharge en fonction du trafic* », dévoile Luc Barthélémy, responsable du projet de véhicule électrique autonome Link&Go chez Akka Technologies. Ce

foisonnement implique de nouveaux acteurs. Renault, par exemple, en partenariat avec la Ville de Paris, soutient plusieurs *start-up* qui devraient lui permettre de proposer rapidement des services liés à la voiture connectée. Au-delà, ce sont les opérateurs de téléphonie, les fournisseurs de solutions de cloud computing, les éditeurs de logiciels, les acteurs du *big data*, les spécialistes réseaux ou encore les experts en sécurité des données, qui sont mobilisés. « *Nous sommes amenés à travailler de plus en plus avec des partenaires qui ne sont pas habituels pour l'automobile* », reconnaît Marc Pajon de Renault.

Compétences multiples

Pour tous, il s'agit de s'accorder sur les protocoles d'échanges de données, sur les systèmes d'exploitation à utiliser et de prendre en compte des cycles de développement très différents selon qu'il s'agit d'une application ou d'un véhicule. « *Une voiture commercialisée en 2011 a été développée à une époque où l'iPhone n'existait pas* », rappelle Julien Clausse d'Altran. Bien sûr, les constructeurs ne peuvent pas prévoir toutes les évolutions. « *Mais ils doivent garantir la maintenance de la connexion au cloud et aux différents services pour la durée de vie du véhicule ainsi que des capacités de mise à jour des équipements embarqués* », prévient Frédéric Bourcier, responsable de projets automobiles chez Wind River, un éditeur et intégrateur de logiciels pour systèmes embarqués, filiale d'Intel Corporation. Il faut, en outre, pouvoir gérer le parc de

cartes SIM. « *La volumétrie ne nous fait pas peur. Nous pouvons les remplacer ou les réallouer si un véhicule est immobilisé par exemple, et ce simplement en un clic* », affirme Marc Avril, responsable marketing Machine to Machine chez SFR Business Team. A cela s'ajoute la nécessité de s'assurer qu'il n'y a pas de zone d'ombre, pas de saturation du réseau. « *C'est là que nous entrons en ligne de compte* », précise Eric Sèle, vice-président et directeur général Europe Sud, Centrale, Moyen Orient et Afrique de Ciena, un spécialiste en matière de réseaux. « *On va vers une nouvelle architecture du réseau qui augmente sa capacité de reconfiguration et assure une absolue fiabilité* », explique-t-il.

La cyber sécurité fait son entrée

Autre point clé : disposer de technologies qui permettent de mieux « maîtriser » le débit. Est-il utilisé pour envoyer de la vidéo ou une information relevant d'un élément critique du véhicule, comme la gestion des freins ? Il s'agit de hiérarchiser les données afin de prioriser celles qui sont cruciales à la conduite. « *Il va falloir protéger les données et éviter que l'on puisse, à partir de la connexion, atteindre les organes de sûreté* », explique un expert en sécurité des données d'un grand groupe industriel. En plus de protéger la vie privée de leurs clients, les constructeurs devront aussi se prémunir contre d'éventuels hackers. Un marché de la surveillance en temps réel et de l'intervention va donc probablement voir le jour en marge du véhicule connecté. « *Il faut intégrer la sécurité dès l'origine des*

projets » recommande l'expert. « *Personne ne pourra travailler seul* ». Se pose alors la question de savoir si la sécurité est un élément de différenciation pour les constructeurs ou un bien commun ? En d'autres termes, qui va payer ? De même, lequel de ces acteurs prendra en charge les coûts de communication, l'augmentation de la capacité du réseau, le développement de tels services ? Hubert Tardieu, conseiller du président d'Atos, tient un élément de réponse : « *Nous avons étudié plus de quarante business cases pour en trouver un qui fonctionne. L'équation tient la route en injectant des partenaires business, comme les assureurs ou les loueurs.* » Pour autant, « *nous sommes dans une phase où aucun business model n'a émergé* », conclut Rémi Cornubert, du cabinet Oliver Wyman. « *Ce sujet n'est pas encore mûr.* »

ALLER PLUS LOIN

Diffusé à 14 000 exemplaires, *Alliancy*, le mag s'adresse aux TOP décideurs (des entreprises, collectivités, institutions publiques et privées) qui souhaitent comprendre comment s'appuyer sur l'innovation pour transformer leur organisation, qu'ils soient issus de filières technologiques ou non.
01 42 66 04 77 de 9h à 18h du lundi au vendredi
courriel : redaction@alliancy.fr



LA GÉOLOCALISATION

> Quels en sont les enjeux fondamentaux en matière de libertés publiques ?

> Quel est son cadre juridique ?

> Que est le cadre légal pour les opérateurs du renseignement utilisant la géolocalisation ?

- Les données géolocalisées peuvent être détournées commercialement. La commission des libertés civiles du Parlement européen, le 21 octobre 2013, a voté un texte renforçant la protection des données (consentement au traitement des données personnelles et transfert de données en dehors de l'UE).
- L'Assemblée nationale et le Sénat ont adopté définitivement le 24 février 2014, une loi relative à la géolocalisation et son utilisation.
- La loi de programmation militaire 2014/2019 autorise les opérateurs du renseignement à employer certains outils comme la géolocalisation. Malgré des réserves, il règle la question de la sécurité juridique de l'opérateur et donne un cadre légal à cette pratique.

La géolocalisation, mode d'emploi.

par **JOËL FERRY**

D

Deux lois viennent de régler le sort de l'usage de la géolocalisation par les administrations chargées de la sécurité et de la défense. Le recours à cette technique est désormais clair et précis et le contrôle destiné à interdire les abus éventuels par des autorités garantes des libertés est assuré. On peut regretter toutefois l'absence d'un traitement global de la problématique. Il faudra sans aucun doute y revenir mais cette fois en traitant la question au niveau européen.

La loi n° 2013-1168 du 18 décembre 2013, relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la



JOËL FERRY

Colonel, réserviste de la gendarmerie nationale.

sécurité nationale, dans son article 20, traite de l'usage de ce moyen en écho au livre blanc de la défense nationale. Par ailleurs, deux arrêts d'application immédiate de la chambre criminelle de la cour de cassation, du 22 octobre 2013, définissent les principes qui devraient s'imposer aux magistrats et enquêteurs pour l'usage de la géolocalisation. En réponse, le législateur vient de s'atteler à la rédaction d'un projet de loi destiné à clarifier le dispositif juridique pénal en fixant des règles claires et précises concernant la saisie des opérateurs ainsi que les circonstances et les conditions d'habilitation de la puissance publique à recourir à cette technique. Il faut dire que, déjà dans un arrêt Uzun contre l'Allemagne du 2 septembre 2010, la Cour européenne des droits de l'Homme a estimé qu'en matière de géolocalisation par un moyen technique, type balise, le droit devait être particulièrement précis, clair et prévoir des garanties adaptées et

XXXXXXXXXX

suffisantes pour interdire les abus.

Le législateur aurait certainement dû regarder la géolocalisation d'une manière globale et non pas segmentée puisque la convergence des technologies du monde numérique et le développement des objets connectés qui dialoguent entre eux produisent de plus en plus de données techniques, certaines pouvant être considérées comme intrusives et attentatoires aux libertés, notamment celles relatives à la localisation des instruments terminaux. Mais l'actualité en a décidé autrement, influencée probablement par les dispositions contenues dans la loi de programmation militaire. Dès lors, on peut regretter l'indolence des pouvoirs publics et celle

de l'Union européenne à un moment où les technologies convergent et où les Etats-Unis s'imposent dans la gouvernance du net malgré des pratiques inquiétantes.

La géolocalisation étant désormais partout et il existe d'indéniables risques pour les libertés publiques. En revanche pour les services de l'Etat, elle se justifie par la nécessité d'assurer la sécurité de la nation et la protection des personnes et des biens. C'est l'objet des différentes lois traitant du sujet mais qui dans ces conditions ne sont pas pérennes. C'est un mal utile pour le développement économique mais il convient d'encadrer son usage d'autant plus que les collectes de données techniques se généralisent

mais sans connaître exactement leur usage.

La géolocalisation : entre sécurité et libertés

L'article 20 de la loi de programmation militaire 2014/2019 répond aux questions de fond abordées dans le rapport sur l'évaluation du cadre juridique applicable aux services de renseignement. Il règle notamment la question de la sécurité juridique du personnel et en même temps donne un cadre légal à l'utilisateur de certains outils ou solutions techniques jusqu'à présent oubliés comme la géolocalisation conduite à l'initiative des agents des services de renseignement ou d'enquête.

Il est indéniable que la géolocalisation d'un téléphone constitue une technique efficace pour apporter des éléments appréciables dans le traitement d'un dossier relevant du renseignement ou de la police judiciaire. Cette solution peut intervenir pour regarder le passé. Dans ce cas il est demandé a posteriori aux opérateurs de téléphonie de communiquer aux services autorisés les informations relatives au positionnement des téléphones sur une période donnée. Il est peut-être également utile d'obtenir ces informations en temps réel pour suivre les mouvements d'une personne ou d'un objet dans le cadre d'une enquête administrative ou d'une enquête judiciaire sur fond, par exemple de

terrorisme ou de criminalité organisée. Cette technique s'appuie sur l'usage certes des téléphones portables mais aussi de balises spéciales. En écho à la Cour européenne des droits de l'Homme dans l'arrêt Uzun⁽¹⁾, le président de la commission des lois de l'assemblée nationale rappelle

(1) CEDH 2 septembre 2010 (Uzun contre Allemagne)
« La surveillance par GPS doit être considérée comme moins attentatoire à la vie privée d'une personne que, par exemple, des écoutes téléphoniques ».

que la géolocalisation est bien moins attentatoire que d'autres moyens spéciaux aujourd'hui utilisés comme par exemple les interceptions de communication. En l'espèce, la surveillance avait été réalisée par des enquêteurs allemands au moyen d'une balise fixée sur un véhicule selon un cadre légal que la haute cour n'a pas contesté. Les juges de la CEDH ont relevé que le droit interne fournissait des garanties suffisantes et effectives contre les abus et notamment qu'il existait une proportionnalité des mesures puisqu'il s'agissait de pallier d'autres techniques de localisation qui avaient moins de chance d'aboutir ou qui étaient plus difficiles à appliquer, que la durée de mise en œuvre de celle-ci était limitée et enfin que la mesure était légitime s'agissant de la poursuite d'une infraction grave. En outre, la mesure décidée faisait l'objet a posteriori d'un contrôle des juridictions internes. En conséquence les protections contre l'arbitraire étaient réunies puisqu'il n'existait pas de surveillance totale et

exhaustive des personnes concernées.

Dans le domaine de la police judiciaire, les deux arrêts de la cour de cassation du 22 octobre 2013 s'inscrivent finalement dans le prolongement de ces réflexions. Les enquêtes portaient sur des trafics de stupéfiants en bande organisée et du blanchiment d'argent dans une cité de La Courneuve. Afin de déterminer le rôle des suspects, le magistrat instructeur avait prescrit la mise en place d'un dispositif technique de géolocalisation sur un véhicule. La pose avait eu lieu dans le parking privé d'une résidence d'habitation. L'interpellation d'un des protagonistes avait été rendue possible et 111 kg de cannabis avaient été découverts dans le véhicule. Après une procédure d'appel, l'affaire avait été portée devant la cour de cassation.

Les juges français, s'appuyant a priori sur le regard porté par la CEDH sur la géolocalisation, ont constaté qu'en France, en matière de police judiciaire, il n'existait dans ce domaine aucun texte spécifique, clair et précis en ce qui concerne la saisie des opérateurs, les circonstances et les conditions d'habilitation de la puissance publique à recourir à ces mesures. Ils insistaient en outre sur le principe de proportionnalité et la nécessité de la mesure dont le contrôle devait être assuré par l'autorité judiciaire.

Si la question s'est souvent posée de savoir s'il était nécessaire de faire mention

en procédure des techniques utilisées, on peut dire que le droit aujourd'hui vient de rattraper les magistrats qui assurent la direction des enquêtes judiciaires et les enquêteurs qui les mènent. Désormais, pour respecter le principe de la procédure contradictoire, toute mesure de géolocalisation sera mentionnée dans la procédure et les enregistrements des localisations placés sous scellés fermés seront joints au dossier. Une seule exception, soumise à l'avis des sages du conseil constitutionnel, a concerné dans le domaine de la criminalité organisée, le cas des informateurs.

Un dispositif encadré mais parfois discutable

Une demande de géolocalisation dans le cadre des interceptions de sécurité ne doit pas interférer avec une enquête de police judiciaire. Ainsi, il ne saurait y avoir interférence entre les deux dispositions d'autant plus qu'une autorité administrative indépendante est chargée d'y veiller.

On remarquera que dans le nouveau dispositif issu de la loi de programmation militaire, la localisation des équipements terminaux fait partie intégrante des données techniques mentionnées à l'article nouveau L 246-2-1 du code de la sécurité intérieure permettant l'accès administratif aux données de connexion. Les services du ministère de la sécurité intérieure, de la défense, de l'économie et

du budget peuvent solliciter cette information lorsque sont concernés la sécurité nationale, la sauvegarde du potentiel scientifique et économique de la France et le maintien de lignes dissoutes.

Lorsqu'à la suite d'un renseignement un service habilité sollicite de l'autorité administrative l'autorisation de recueillir des données de géolocalisation détenues par un opérateur de communication électronique, il lui appartient de motiver la demande qui est exclusivement écrite. Cette autorité représentant le Premier ministre est garante du respect des libertés publiques. Cette autorisation, qu'elle accorde pour une durée de 30 jours et qui peut être renouvelée dans des conditions de durée et de forme identiques, est soumise au contrôle de la commission nationale de contrôle des interceptions de sécurité, l'équivalent de la commission nationale informatique et libertés pour la protection des données personnelles.

Conformément aux vœux de la cour de cassation, le dispositif de géolocalisation judiciaire répond désormais à des règles d'usage claires et précises. C'est un outil de portée générale qui n'est pas réservé à des formes particulières de criminalité telle que la criminalité organisée. Ainsi, elle peut être décidée pour un crime ou un délit puni d'un emprisonnement d'au moins trois ans pour ce qui concerne les atteintes aux personnes et les entraves à

la justice et cinq ans pour les autres domaines, ainsi qu'à l'occasion d'une enquête pour recherche des causes de la mort, de personne en fuite et disparition inquiétante. Cet encadrement répond totalement à la réalité actuelle des infractions justifiant un besoin de géolocalisation.

Le recours à la géolocalisation par le juge d'instruction a fait l'objet d'un encadrement qui n'est pas contraignant puisqu'il peut décider de la mesure pour une durée de 4 mois renouvelable. Cette disposition est identique à celle de l'article 100-2 du code de procédure pénale portant sur les interceptions de correspondances émises par la voie des télécommunications. L'autorisation donnée aux enquêteurs par le procureur de la République pour utiliser cette technique durant la phase police judiciaire a fait l'objet d'un aménagement plus contraignant puisque la mesure peut être décidée pour une durée continue de quinze jours mais autorisée ensuite par le juge des libertés pour une durée d'un mois renouvelable. La contrainte est désormais beaucoup plus forte car au-delà du terme des quinze jours il appartiendra à l'enquêteur et au procureur de se montrer convaincant pour justifier l'importance de la mesure. Le législateur a par ailleurs fait preuve d'une grande compréhension en autorisant l'action d'initiative en cas de risque de dépérissement de preuves ou

d'atteintes graves aux personnes et aux biens par les enquêteurs confrontés à la réalité du terrain à charge d'en rendre compte rapidement au procureur ou au juge d'instruction qui devra statuer sur la pérennité de la mesure sous vingt-quatre heures. On doit s'interroger sur les autorisations laissées à la seule initiative du procureur de la République. Si, selon la cour de cassation, celui-ci n'est pas jugé comme indépendant, alors pourquoi lui laisser cette possibilité d'autoriser une mesure de géolocalisation durant 15 jours sans l'intervention déjà à ce stade, du juge des libertés ? Comment la cour européenne des droits de l'homme appréciera-t-elle cette mesure, qu'elle n'a pas au demeurant soulevé, si un recours lui est présenté.

La géolocalisation n'est pas traitée dans sa globalité

On peut regretter pour l'avenir, que le législateur n'ait pas souhaité s'engager sur une approche globale de la géolocalisation en examinant les technicités d'un futur proche.

(2) GPS signifie *global positioning system*. Il s'agit d'un système de localisation américain qui depuis 1994 utilise une grappe de 24 satellites.

(3) Depuis 1999, le Wifi est un système de transmission de données sans fil utilisant la fréquence 2,4 mhz d'une portée pouvant atteindre une centaine de mètre.

(4) Internet protocole.

La géolocalisation repose en effet sur plusieurs techniques comme le GPS⁽²⁾ pour les balises et le GSM/Cell.id (identifiant de la cellule radio) et même le WIFI⁽³⁾ pour

les smartphones et bientôt les liaisons au standard Wave. Avec Internet, la géolocalisation s'effectue au moyen de l'adresse IP⁽⁴⁾. Un ordinateur ou n'importe quel terminal connecté à Internet peut être géolocalisé en se basant sur cette adresse IP avec un niveau de précision de l'ordre de la ville. Avec le protocole IPV6 chaque objet aura sa plaque d'immatriculation définitive dès sa création, les objets dialogueront entre eux et la géolocalisation deviendra un instrument de l'économie sauf à supprimer le commerce et envisager la régression sociale.

Le législateur a, dans sa réflexion, davantage lié la géolocalisation au cas particulier de l'usage de balises GPS qui constitue par certains cotés une forme de filature moderne numérique. Il n'a pas en revanche souhaité approfondir le cas des autres moyens de communication et notamment de l'internet des objets.

Des opérateurs ignorés du dispositif

On fera néanmoins observer que la protection des libertés individuelles s'exerce sur l'ensemble de la chaîne police judiciaire et durant l'instruction, depuis la collecte par les opérateurs et les transmetteurs de cette information, jusqu'au traitement des données par les services d'enquêtes.

Sans qu'il en soit fait mention dans le texte législatif, le respect de la vie privée s'impose aussi à ces opérateurs qui sont

soumis à la loi informatique et libertés lorsqu'ils traitent des données techniques et notamment des données de géolocalisation dont les références associées comme un numéro de téléphone constituent une donnée indirectement nominative. Pour cela, ils devraient avoir déclaré leur traitement auprès de la commission nationale de l'informatique et des libertés et mis en place d'une part des procédures et des garanties de sécurité physique en sanctuarisant leurs services et d'autre part des moyens de sécurité informatique protégeant les systèmes contre les intrusions. Des normes ISO garantissant la qualité de service de ces entreprises pourraient être envisagées. Or, la loi reste muette sur ce point considérant sans doute que le lien avec la loi du 6 janvier 1978 est naturel.

L'oubli des données stockées à l'étranger

En éludant cette question le législateur balaye également notamment le cas de la collecte quotidienne des données techniques par certains opérateurs étrangers. On est en effet esclave de certaines machines, tablettes ou smartphones équipés de logiciels étrangers capables de géolocaliser nos appareils pour fournir par exemple la météo locale. Ces mêmes appareils dialoguent en permanence avec leur concepteur et on ignore parfois le périmètre total des données collectées. Il

y a lieu de se montrer inquiet car ces données, recueillies en France, sont stockées en dehors du territoire national par des opérateurs étrangers sans que l'on sache le véritable usage des informations collectées. Les techniques de *cloud computing* amplifient le phénomène puisque leur emplacement n'est pas forcément connu et qu'en raison de leur déplacement possible il n'existe aucune certitude sur leur niveau de sécurité. On doit donc se montrer prudent car ce sont nos libertés qui à terme risqueront d'être limitées.

Un enjeu de pouvoir

Il n'est pas surprenant que le législateur ait pris en compte la problématique de la géolocalisation si l'on considère que cette mesure est appliquée depuis de longues années. Les textes répondent aux besoins des services de renseignement et des enquêteurs dirigés par le procureur de la République dans la phase de police judiciaire ou le juge d'instruction dans la phase de l'instruction. Les textes restent muets cependant sur les pratiques des opérateurs notamment étrangers qui pour des objectifs équivoques collectent ce type de données souvent sans véritable information préalable des utilisateurs. Cette question qui intéresse tous les États devra pour le moins faire l'objet d'une réflexion au sein des instances européennes *ad hoc* car désormais, ce n'est plus celui qui détient l'information qui tient le pouvoir, mais bien celui qui sait

Centre de recherche de l'école des officiers de la gendarmerie nationale



DIRECTEUR DE LA PUBLICATION

Général de brigade **Didier BOLOT**

Rédaction

Directeur de la rédaction :
général d'armée (2S) **Marc WATIN-AUGOUARD**,
directeur du centre de recherche de l'EOGN

Rédacteur en chef : colonel **Philippe DURAND**

Rédacteur : **Maquettiste PAO :**
Colonel **Alain Kik** Major **Carl GILLOT**
Colonel **LAURENT VIDAL**

COMITÉ DE RÉDACTION

Général de corps d'armée **Richard LIZUREY**,
major général de la gendarmerie nationale
Général de corps d'armée **Alain GIORGIS**,
commandant des écoles de la gendarmerie nationale
Général de brigade **Didier BOLOT**,
conseiller communication du directeur général
de la gendarmerie nationale - chef du Sirpa-gendarmerie
Colonel **Bernard CLOUZOT**, cabinet
Colonel **Laurent VIDAL**,
chargé de mission à l'EOGN

COMITÉ DE LECTURE

Général d'armée **Laurent MULLER**,
inspecteur général des armées – gendarmerie
Général de corps d'armée **Richard LIZUREY**
major général de la gendarmerie nationale
Général de corps d'armée **Alain GIORGIS**,
commandant des écoles de la gendarmerie nationale
Général de corps d'armée **Bertrand SOUBELET**,
directeur des opérations et de l'emploi
Général de brigade **Didier BOLOT**,
conseiller communication du directeur général
de la gendarmerie nationale - chef du Sirpa-gendarmerie
Colonel **Jean-Louis SALVADOR**,
chef du département gendarmerie
au sein du service historique de la Défense
Colonel **Bernard CLOUZOT**, cabinet

Message aux abonnés

La veille juridique de la gendarmerie nationale et la revue du centre de recherche de l'EOGN sont maintenant consultables sur le site internet du CREOGN - rubrique publications WWW/



LPC - GAV Lannery

THÈME DU PROCHAIN DOSSIER

Investigations criminelles

Un large spectre de dispositions européennes en matière de politiques de sécurité, des technologies favorisant un droit émergent et une culture de la preuve scientifique militent pour que nous fassions le point dans notre prochain numéro sur l'état de l'art des investigations criminelles