Défis n°7

La revue du département **Intelligence et sécurité économiques**

EXPLORER

L'ENTREPRISE FACE AU TERRORISME
Quels enjeux ? Que peut l'État ?
Impacts et réponses

Entretien avec…

Hélène CAZAUX-CHARLES
Directrice de l'INHESJ

L'ENTREPRISE FACE AU TERRORISME

INHESJ

DÉCEMBRE 2016

Défis

La revue du département
Intelligence et sécurité économiques
de l'INHESJ

INHESJ

INSTITUT NATIONAL DES HAUTES ÉTUDES
DE LA SÉCURITÉ ET DE LA JUSTICE

DIRECTRICE DE LA PUBLICATION
Hélène CAZAUX-CHARLES

DIRECTRICE DE LA REDACTION
Angélique LAFONT

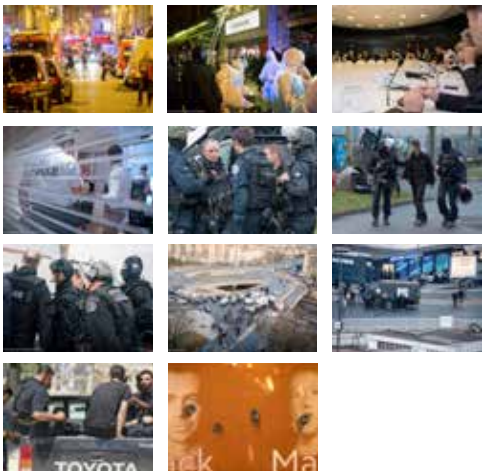
RÉDACTRICE EN CHEF
Diane DE LAUBADÈRE

RÉDACTRICE EN CHEF ADJOINTE
Angélique LE MAZOU

ASSISTANCE À LA RÉDACTION
Manon CHINI, Clémence DESSEILLES

INHESJ
École militaire
1, place Joffre,
75700 PARIS SP 07

ISSN : 2265-4577



Les illustrations de la rubrique *Explorer* sont extraites du Ministère de l'Intérieur / DICOM (F.PELLIER - PIERRE CHABAUD - J.ROCHA - Aurore LEJEUNE) et d'AMARANTE International

ÉDITORIAL

Angélique LAFONT
Chef du département
Intelligence et sécurité économiques, INHESJ

C'est à un moment charnière de la vie de l'Institut, celui d'un changement de direction, que paraît ce nouveau numéro de *Défis*. Directeur de l'Institut depuis 2013, le préfet Cyrille SCHOTT a quitté ses fonctions le 27 octobre dernier. Le département Intelligence et sécurité économiques tient ici à saluer l'engagement et le dynamisme qui ont été les siens dans le développement et la reconnaissance de l'expertise de l'INHESJ et le remercier de son soutien constant dans le déploiement des activités du département. Une nouvelle page de l'Institut est désormais ouverte. Il revient désormais à madame Hélène CAZAUX-CHARLES, magistrate, précédemment conseillère justice au cabinet du Premier ministre, d'en poursuivre l'écriture. Nous l'accueillons chaleureusement et la remercions de nous livrer dans ce numéro ses motivations, son ambition pour l'Institut ainsi que l'état d'esprit dans lequel elle prend ses nouvelles fonctions.

Un an après les attentats du 13 novembre 2015, ce nouveau numéro de *Défis* paraît également à un moment particulièrement douloureux pour notre pays. La mobilisation de l'Institut autour des enjeux soulevés par le terrorisme n'a cessé de se renforcer ces derniers mois. En témoigne à nouveau ce numéro de *Défis*, dont le dossier *Explorer* aborde le terrorisme et ses conséquences sous un angle encore peu traité, à savoir celui de son impact sur les entreprises.

Plus que jamais la diffusion de la culture d'intelligence et de sécurité économiques constitue la vocation première du département aujourd'hui. La prise de conscience de l'ensemble des risques et menaces qui pèsent actuellement sur les entreprises est en effet un enjeu majeur pour l'avenir économique et le développement de nos territoires. En cela, les formations du département constituent un levier précieux qui fait l'objet de toute notre attention. Mais il n'est pas le seul. Le département a investi, en effet, depuis le mois de janvier 2016 un groupe de travail au sein de l'AFNOR visant à élaborer un projet de norme internationale sur le management de la sûreté, qui n'existe pas aujourd'hui. C'est un enjeu majeur auquel le département consacrera l'énergie nécessaire pour promouvoir sa vision globale de la sûreté.

De même, le niveau de coopération et de synergie entre les acteurs est également un facteur déterminant dans la diffusion de cette culture. Ainsi, nous nous réjouissons du renforcement des liens qui unissent le département au monde de l'entreprise mais également aux différents services de l'État en charge de ces problématiques de sécurité économique. Nous veillons en effet à associer les uns et les autres à l'ensemble des activités du département. Cette volonté de coopération renforcée s'est illustrée récemment à l'occasion du colloque que le département a organisé conjointement, le 4 octobre 2016, avec le Service de l'information stratégique et de la sécurité économiques dans le but de redynamiser le dispositif *EUCLES* de conférenciers en sécurité économique. Nous connaissons en France, contrairement aux pays anglo-saxons, de véritables difficultés à intégrer cette culture. Nous progressons cependant, la forte augmentation des candidatures pour notre session nationale « Protection des entreprises et Intelligence économique » (reconnu équivalent bac+5 depuis 2012) en témoigne. Cette évolution positive ne peut que nous réjouir et renforcer notre détermination à faire bouger les lignes. ■

SOMMAIRE Défis n°7

EXPLORER

L'ENTREPRISE FACE AU TERRORISME

Dossier coordonné par
Diane de Laubadère, *Rédactrice en chef de* Défis

QUELS ENJEUX ?
QUE PEUT L'ÉTAT ?
IMPACTS ET RÉPONSES

INTRODUCTION

Diane de LAUBADÈRE

Rédactrice en chef de la revue *DéfIS,*
Chargée de mission à l'INHESJ

Le terrorisme a causé la mort de 238 personnes sur le territoire national depuis l'assassinat de la rédaction de Charlie Hebdo, le 7 janvier 2015. Les massacres qui suivirent, des 130 victimes du Bataclan au carnage de Nice, jusqu'au meurtre du père Hamel en juillet dernier, ont suscité l'émoi du monde entier : réseaux sociaux inondés de messages de soutien, bougies et épitaphes sur les lieux des attaques, déclarations des représentants politiques de tous bords, rassemblements et manifestations compassionnelles dans de nombreuses villes Françaises et étrangères.

Mais la France, victime sur son sol du terrorisme islamiste, fut aussi pointée du doigt et reléguée au rang de « pays infecté » responsable, selon Donald Trump, désormais Président élu des États-Unis, d'avoir « laissé ces personnes entrer sur son territoire »[1]. Certaines voix à l'international semblent promptes à accuser les autorités Françaises de n'être plus en mesure de garantir la protection des citoyens. L'affaire du « Burkini », en août dernier, a contribué à brouiller un peu plus les pistes, en déclenchant une vague de critiques d'une toute autre nature. « Cible de la haine »[2], la France est passée du statut de victime à celui, guère plus enviable, de Nation persécutrice tentée par l'islamophobie. De puissants clivages sociétaux sont mis au jour, le labarum des « valeurs républicaines » ne semble plus aussi rassembleur qu'avant, et l'État donne souvent l'impression d'être impuissant à enrayer un phénomène dont l'ampleur le dépasse.

La France est-elle la Nation fracturée que décrivent certains, tétanisée par une menace qu'elle ne comprend pas et n'a pas su détecter à temps ? Il n'appartient pas à *DéfIS* d'en débattre. Mais au moins pouvons-nous tenter de mesurer l'impact « réputationnel » du contexte sécuritaire actuel et son poids sur l'économie et la compétitivité de nos entreprises. Comment éviter la tentation de « la fracture »[3] sociale, identitaire et religieuse ; acte précurseur de la guerre civile ? C'est l'une des questions posées par ce numéro consacré à « L'entreprise face au terrorisme ».

DéfIS 7 donne la parole aux acteurs et aux « sachants », universitaires et experts, opérationnels du secteur privé, responsables politiques en charge de la mise en œuvre de stratégies de gestion du risque, à l'Intérieur comme à l'International. **Louis Gautier**, Secrétaire général de la Sécurité et de la Défense Nationale, dresse un panorama complet des mesures prises par le gouvernement, et dévoile le nouveau schéma d'intervention des forces de sécurité sur des zones de compétence territoriale redéfinies. **Gilles Kepel**[4] lance pour sa part un appel aux gouvernants, les invitant à s'appuyer sur l'analyse universitaire pour éclairer l'action publique, dans une tentative de refondation d'un « gouvernement éclairé[5] ». Une réponse aux discours idéologiques et à toute forme de radicalisation ou de totalitarisme dont rêvent les déchus d'une société en mal d'État fort. Cette perspective ambitieuse de réconcilier « le savant et le politique » s'est concrétisée le 16 novembre dernier à l'ENS, lors de sa rencontre avec le ministre de l'Intérieur. La création du Conseil de la stratégie et de la prospective, dont la première réunion a eu lieu le 18 octobre 2016, illustre cette volonté. Il devrait réunir deux fois par an les experts, chercheurs et universitaires qui y siègent sous la présidence du ministre de l'Intérieur.

Comprendre les deux années meurtrières que nous venons de traverser, aveuglément frappés par le « terrorisme de troisième génération », nous impose de resituer la menace dans le temps long : « Nous sommes donc tenus de considérer l'ensemble, l'articulation du système pour comprendre l'événement. »[6] L'analyse rétrospective montre que la menace n'a pas surgi *ex-nihilo* dans l'Hexagone, qu'elle ne se réduit pas à la simple expression

(1) Déclaration de Donald Trump, le 20 juillet 2016 sur NBC.
(2) « Vu de l'étranger. Attentats à Nice : la France, cible de la haine », Courier International, le 15 juillet 2016.
(3) KEPEL Gilles. *La fracture*, Gallimard, Paris 2016.
(4) *Ibid.*
(5) MONTESQUIEU, *De l'esprit des lois* (1748) sur la séparation des pouvoirs et d'un gouvernement éclairé, VOLTAIRE *Candide ou l'Optimisme*, janvier 1759 - *Le philosophe roi*, le livre V de La République.
(6) KEPEL Gilles, *La fracture*, Gallimard, Paris 2016.

d'un malaise social, mais qu'elle est l'« aboutissement d'un processus simultanément à l'oeuvre dans deux contextes : le Moyen-Orient et l'Afrique du Nord d'un côté, la société française et ses quartiers populaires de l'autre. »[7] Elle n'est pas non plus spontanée. Avant de passer à l'acte, les « Loups solitaires » sont « connectés », organisés en réseaux. Leur action relève d'une stratégie.

Deux territoires très spécifiques jouent un rôle fondamental dans le rapprochement de ces contextes : les prisons, sas de décompression des djihadistes de retour des théâtres Irako-syriens, et le Web, territoire virtuel où les réseaux sociaux servent de caisse de résonnance aux prosélytes du « djihad spontané ». En association avec la CNIL et les unités spécialisées de police et de gendarmerie, des entreprises de l'Internet contribuent à surveiller et démanteler ces réseaux, et à fermer les sites les plus toxiques. **Thierry Delville**, chargé de la lutte contre les cyber menaces pour le ministère de l'Intérieur, nous met face à une évidence : « Le combat contre le terrorisme se livre également dans le cyberespace ».

L'entreprise constitue un troisième territoire propice à la radicalisation. Elle fait parfois face à une menace endogène dont les signaux faibles annonciateurs sont les revendications de certains salariés visant à obtenir le droit à des pratiques comportementales et religieuses spécifiques (horaires aménagés pour la prière, menus spécifiques, refus d'interagir avec les femmes, etc.). Autant de symptômes alarmants d'un corporatisme religieux susceptible, à terme, d'enrayer l'outil de production.

Qu'ils s'expriment par la revendication syndicale ou se dissimulent derrière une intégration de façade (la radicalisation « à col blanc »), l'objectif stratégique des islamistes demeure l'établissement d'un Califat en « territoire ennemi », sur les ruines d'un État déstabilisé par une économie en perte de vitesse, au tissu social en décomposition. Le repli des valeurs du « vivre ensemble » est souvent prétexte à leur action. Ainsi se présentent-ils à la fois comme victimes (d'ostracisme), bourreaux (des mécréants), et sauveurs (de leurs frères). Un « triangle dramatique », classique de l'analyse transactionnelle du psychologue américain **Stephen Karpman**, qui s'appliquerait aussi au « système pervers » de la radicalisation. **Thomas Bouvatier** décrypte les ressorts psychanalytiques communs à toute forme de radicalisation, montrant que ces comportements peuvent constituer une réponse à un manque de reconnaissance, de quête de sens de la part des salariés. Aussi, si les centres de « déradicalisation » permettent de restaurer le dialogue avec les « victimes », et dans une certaine mesure, d'évaluer l'efficacité du prosélytisme, leur multiplication pourrait n'être qu'une solution « pansement ». Le risque serait de traiter le symptôme plutôt que la cause.

Les entreprises ont-elles les moyens humains et juridiques de faire face au phénomène ? Les secteurs les plus exposés s'organisent, forment leurs salariés à la détection des comportements douteux, les sensibilisent aux risques d'attentats, etc. ADP, RATP, VEOLIA, Centres commerciaux… les témoignages ci-après attestent du rôle clé de la prévention dans la gestion de la radicalisation. Le *Guide pratique du fait religieux dans les entreprises privées,* édité ce mois de décembre 2016, par le ministère du Travail, veut apporter des réponses concrètes et liste les outils juridiques à disposition des entreprises.

Prosélytisme organisé, clivages identitaires conduisant à la revendication de conditions de travail spécifiques, détournement de l'outil de production à des fins d'actions violentes (Nice), actes de pure barbarie (Yassin Salhi décapite son patron sur le site gazier de Saint-Quentin-Fallavier), l'exposition directe de l'entreprise à la menace terroriste ne fait plus doute. Ce phénomène est-il pour autant nouveau ? Signe de l'évolution de notre perception, certains experts s'interrogent aujourd'hui sur l'origine présumée « accidentelle » de l'explosion du hangar de l'usine AZF de Toulouse, le 21 septembre 2001. **Amarante** nous rappelle que les entreprises présentes à l'international sont des « cibles traditionnelles » du djihad, qui ont par conséquent « pris la mesure de la menace accrue pesant sur leur intérêt ».

Pour celles qui n'ont pas eu cette clairvoyance, le réveil est difficile. Quelles furent les causes de leur aveuglement ? Une tendance naturelle au déni ? Le manque d'échange d'information entre les services de l'État et les directions Sûreté ? Un descriptif situationnel tronqué par les médias ? Le « gouffre culturel » décrit par Gilles Kepel, qui menace les élites politiques du syndrome de décalage avec la réalité du terrain ? **Alain Juillet** constate qu'« absorbés dans la poursuite d'objectifs financiers à court terme voulus par leurs actionnaires, les chefs d'entreprises n'ont pas compris cette évolution (…) ; ils restent dans un schéma dépassé dans lequel l'État doit s'occuper de ces problèmes tandis que eux créent de la richesse (…) ».

Pourtant, depuis les jurisprudences Karachi et Sanofi, l'employeur a obligation d'évaluer les risques et de mettre en œuvre les mesures nécessaires à la protection des salariés « dans un lieu particulièrement exposé au risque »[8]. Qu' en est-il dans le contexte d'état d'urgence sur le territoire ? *Quid* de la couverture assurantielle ? **Olivier Hassid** nous met en garde : « Dans un contexte où le plan Vigipirate est maintenu à un niveau élevé (et que tout chef d'établissement ne peut l'ignorer), il pourrait être considéré comme inexcusable qu'un chef d'entreprise n'ait pas mis en place une organisation de la sûreté… ».

(7) KEPEL Gilles, *La fracture*, Gallimard, Paris 2016.
(8) C.cass., ch. Soc., 7 décembre 2011, pourvoi n° 10-22875 : https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000024947630

Responsable, est donc, le chef d'entreprise. Mais quelle est sa marge de manoeuvre lorsqu'il s'agit de prendre des mesures d'exception ? Le cadre juridique est-il adapté ? D'après **Claude Tarlet**, « des attentes fortes (non encore satisfaites) existent notamment en matière de *benchmark* (et de transposition de solutions efficaces dans nos pratiques) et à l'égard de notre système législatif. ». En matière de protection des données, d'armement des agents privés de sécurité ou de vidéo surveillance, des savoir-faire existent dont le droit ne permet pas l'utilisation.

L'effort de mise à niveau des dispositifs de sûreté représente un surcoût que toutes les entreprises ne sont pas en mesure d'absorber. Dans certains secteurs particulièrement exposés comme la vente, les loisirs, la culture, la mode ou les transports, l'obligation morale de protection des biens et des personnes impose d'accroître – parfois exponentiellement - les budgets alloués aux départements Sûreté. Pour les autres, plus modestes ou moins directement exposés, la tentation du déni est forte : « ça n'arrive qu'aux autres ! ». Se pose alors la question cruciale du seuil d'acceptabilité de la menace qui relève de l'éthique d'entreprise. Où sont les limites de tolérance ? Quel déficit de protection le citoyen-salarié est-il prêt à accepter pour ne pas infléchir les courbes de résultat de son employeur ? Alain Juillet nous rappelle que dans notre société surprotégée, nos « concitoyens ont une exigence croissante de sécurité collective ».

Tout comme le secteur privé, l'État est confronté à ses propres limites capacitaires. Une fois déployées dans l'espace public et concentrées sur les opérateurs d'importance vitale (OIV), les forces de l'ordre, qui n'ont d'habitude pas vocation à protéger les infrastructures et les activités privées, se trouvent exsangues.

Corollaire de la question du périmètre régalien, celle, toujours épineuse, des limites d'emploi des agents de sécurité privée. Question maintes fois soulevée depuis que les SMP[9] sont devenues des ESSD[10]. Le débat s'oriente alors sur les sujets d'accréditation – notamment de port d'armes, de formation et d'usage légitime de la force. Pour Alain Juillet, « La seule solution est donc un transfert de responsabilité régalienne de la police nationale vers les polices municipales, la garde nationale et les sociétés privées de sécurité. (…) L'activité implique, par exemple, d'avoir résolu le problème de l'armement et de l'ouverture du feu en légitime défense».

On le voit, le contexte extrême d'aujourd'hui appelle un redécoupage des zones de responsabilité de chacun. Il pose aussi à l'entreprise le dilemme de la relocalisation, voire de l'annulation pure et simple de certaines activités «non-indispensables» comme les colloques ou symposiums annuels. Le changement des *us et coutumes* se présente comme une alternative au renforcement drastique des mesures de sûreté. Il n'est plus possible de nier que la baisse de fréquentation de certains sites touristiques, en premier lieu Paris, contribue à très largement impacter le CA de certains secteurs d'activité. Paris, déclarée « No Go Zone pour les touristes de luxe »[11], regroupe 751 des « zones interdites sur 900 ». Comment contester ce chiffre ?

En moins de deux ans, la France symbole d'art de vivre, de patrimoine, de culture et de luxe, a dû descendre de son piédestal de pays le plus visité au monde. « Les touristes étrangers boudent la France »[12], et certains tour-opérateurs asiatiques ne proposent plus aucune visite de Paris. La fréquentation de la capitale a baissé de 20 à 35 pourcents, avec un impact brutal sur certains secteurs dont celui du commerce haut de gamme. Les prestigieuses enseignes de la Place Vendôme et de l'Avenue Montaigne sont à la peine…

Nous ne lutterons pas contre le totalitarisme islamiste en nous voilant la face devant nos erreurs et nos faiblesses endogènes. La globalisation, l'ultra libéralisme et l'économie « hors sol », dont les multinationales sont le vecteur, ont contribué à nous enfermer dans l'abrutissement du consumérisme. Ce que Hervé Juvin nomme « radicalisation de la modernité » en 2014, dans *La Grande Séparation*, consiste à casser les structures sociales et les liens avec le territoire et ouvre la voie à toute forme de prédation[13]. Triomphe de l'idéologie consacrée au progrès du bien-être, ce « droit des peuples à disposer d'un écran plat et d'un iPad qui permet l'assentiment. »[14] Triomphe et déboire du « transhumanisme » sur la capacité des individus à être autonomes. Ne sous-estimons pas les effets pervers de notre mode de vie, autre forme de totalitarisme, qui souvent gangrène nos organisations : fracture sociale et identitaire, exclusion, crise de sens, « burn-out », risques psychosociaux… le terreau humain dégradé sur lequel prospèrent les fondamentalismes.

Les entreprises ont un rôle prépondérant à jouer dans la restauration des économies souveraines. Certains secteurs d'activité prennent le tournant de nouveaux modes de production qui nous laissent croire à un avenir moins conflictuel et plus serein. Face au terrorisme, ces acteurs émergeants pourraient s'ériger en rempart contre la terreur et former un indicateur de résilience de notre pays dangereusement menacé.

Notre prochain *DéfIS* s'efforcera de les présenter. ■

(9) Sociétés militaire privées.
(10) Entreprises de Service de Sécurité et de Défense. *Cf.* pour aller plus loin : *DéfIS n°2*, p.89
(11) *Le point,* 3 octobre 2016.
(12) *Cf.* Article «Les touristes étrangers boudent la France», Le Monde, 23 août 2016
(13) JUVIN Hervé. *La Grande Séparation*, Gallimard, 2014.
(14) POLONY Natacha. Comité Orwel, https://comiteorwell.net/tag/natacha-polony/

QUELS ENJEUX ?

FACE AU TERRORISME, LA SÛRETÉ N'EST PLUS UNE OPTION !

Alain JUILLET
Président du CDSE, Conseiller senior
chez Orrick, Herrington & Sutcliffe LLP

Curieusement, le terrorisme est longtemps resté un problème concernant exclusivement l'État et les citoyens. La localisation de l'attentat était perçue comme un point conjoncturel secondaire pour une action ciblant des personnes identifiées comme ennemies de l'attaquant. L'utilisation des transports, initiée par les palestiniens comme support privilégié, a mis cette filière dans l'obligation d'organiser sa protection avec l'aide de l'État. L'obligation est devenue d'autant plus forte que nous sommes passés du détournement, avec demande de contrepartie ou d'échange s'accompagnant de pressions plus ou moins mortifères, à la destruction partielle ou totale du support ou du lieu de rassemblement en y incluant l'ensemble des personnes s'y trouvant. De même, la sélection de cibles visant à déstabiliser l'économie d'un pays, comme on l'a vu avec les attaques en Tunisie ou en Égypte, par l'effondrement de la fréquentation et des recettes touristiques, oblige à élargir le champ du possible en intégrant des sites et des activités.

Dans le concept de guerre dissymétrique du faible au fort, avec la rapidité de circulation de l'information, l'impact médiatique est devenu prioritaire par rapport à celui idéologique ou religieux. L'important est de créer un choc dans lequel un très grand nombre de gens se sentent menacés par quelque chose qu'ils ne maîtrisent pas et tiennent le politique pour responsable. Cette stratégie trouve un terrain favorable dans la société française qui ne sait plus faire face collectivement. La perte d'éthique à tous les niveaux sociaux et l'individualisme croissant font que beaucoup de nos concitoyens, ayant perdu toute référence aux valeurs fondamentales de la République, ne croient plus en rien. Dans une vision exclusivement centrée sur leurs intérêts personnels, ils ont tendance à tout rejeter en dehors d'eux-mêmes et de leur environnement.

Les groupes terroristes de tous bords ont été amenés à diversifier leurs actions pour élargir leur champ d'action en touchant, par des moyens différenciés, un maximum de cibles variées. À côté de l'action planifiée de destruction de masse, où le nombre de victimes et le choix du lieu sont essentiels pour créer la peur et déstabiliser le pays, ils ciblent également des entreprises et leurs dirigeants ou des personnalités, accusés de contribuer sous une forme ou une autre à la lutte contre leurs idéaux. Le spectre est très large puisqu'actuellement on va y trouver aussi bien des entreprises de défense fournissant du matériel de guerre que des entreprises agro-alimentaires utilisant des produits porcins ou alcoolisés, des sociétés de production ou des journaux réalisant des reportages jugés sectaires, ou des publicitaires dégradant l'image de la femme.

Les chefs d'entreprises, absorbés dans la poursuite d'objectifs financiers à court terme voulus par leurs actionnaires, n'ont pas compris cette évolution et ont

CHRONOLOGIE

New York (USA) 11/09/2001
Deux avions percutent les tours du World Trade Center. ***2977 morts***

2001

France 15/11/2001
Adoption de la Loi relative à la sécurité quotidienne (LSQ).

Madrid (Espagne) 11/03/2004
Dix bombes explosent dans des trains en heure de pointe. ***191 morts***

2004

Paris (France) 8/10/2004
Une bombe explose devant l'Ambassade d'Indonésie. ***10 blessés***

Attentat au Bataclan à PARIS
2015 - mint0752_041_plr89

beaucoup de mal à la prendre en compte. Ils restent dans un schéma dépassé dans lequel l'État doit s'occuper de ces problèmes tandis qu'eux créent de la richesse pour le bénéfice de quelques-uns et de l'emploi pour un plus grand nombre. Isolés dans leur cadre sociétal, ils ne voient pas une évidence du monde actuel : la sécurité est une co-production dans laquelle chacun à son rôle à jouer. Pourtant la justice, avec les arrêts Karachi ou Sanofi, a rappelé la responsabilité personnelle des dirigeants en cas d'attaques contre des salariés expatriés ou missionnaires et leurs familles. De même, les problèmes concernant les libérations des otages au Sahel ont eu un impact significatif sur l'image des entreprises concernées et de leurs dirigeants.

Au plan territorial et interne aux entreprises, le problème devenu incontournable est celui de la radicalisation d'un certain nombre de nationaux et de bi nationaux. On l'a ignoré trop longtemps pour des raisons idéologiques issues d'un dévoiement du concept de laïcité. Rejetant exclusivement les pratiques et l'histoire judéo-chrétienne, on y a intégré une vision tiers mondiste de la diversité et du droit des minorités, privilégiant la communautarisation à l'intégration par le partage de valeurs communes, sans en mesurer les conséquences sociales. La crise économique a ajouté un sous-emploi croissant qui tue l'espérance en un monde meilleur et ouvre à tous les fantasmes parmi ceux qui n'ont pas d'espoir d'évolution. Dans les prisons ou dans les entreprises, il suffit d'un individu pour influencer par le verbe ou la menace ceux qui sont autour en leur donnant la clé d'une soumission à Dieu qui transforme leur avenir. Dès qu'un groupe se forme, il fait du prosélytisme tout en se sanctuarisant. Exigeant le respect de ses pratiques religieuses, il bénéficie de la mansuétude de la hiérarchie qui a tendance à fermer les yeux et laisser faire.

Il est vrai que le problème religieux est généralement traité en entreprise par les ressources humaines qui ont du mal à percevoir derrière les demandes de salles de prière ou de cantines hallal, le risque d'une dérive pouvant aller jusqu'au terrorisme. De même, la solution consistant à regrouper tous les perturbateurs dans le même service pour en faciliter la gestion a pour conséquence la création d'un foyer à risque beaucoup plus important. Il faut reconnaître que les responsables sont tenus par des lois, souvent difficiles à interpréter, qui facilitent l'accusation de discrimination, et sont soumis à la pression de groupes idéologiques prônant la tolérance qui les accusent de brimer la liberté en refusant des pratiques communautaristes. Ainsi, ils se laissent généralement entraîner plus loin qu'ils le voudraient, sans toujours avoir conscience que, derrière les petits arrangements, ce sont les principes républicains qui sont bafoués.

Les directions sûreté et sécurité sont mieux préparées à traiter ces situations par la formation initiale de leur

Londres (Angleterre) **7/07/2005**

Quatre explosions touchent les transports publics. ***56 morts. 700 blessés***

2005 — 2006 — 2011

France 23/01/2006

Adoption de la Loi n°2006-64 relative à la lutte contre le terrorisme *liant « sécurité privée » et « terrorisme » et* ***nouvelle extension de compétences pour les agents de sécurité privée.***

Paris (France) **2/11/2011**

Destruction du ***siège de Charlie Hebdo*** *dans un* ***incendie criminel, le jour où le journal satirique publie une édition rebaptitisée «Charia Hebdo», avec le prophète Mohammed caricaturé en Une.***

Son site internet est piraté, la page d'accueil est remplacée pendant plusieurs heures par celle de la Mecque avec le slogan « No God but Allah ».

encadrement et leur expérience opérationnelle. Elles sont capables de se renseigner, d'évaluer les risques et de se projeter dans l'avenir en croisant leurs expertises avec celles de collègues d'autres entreprises. Grâce à leurs relations avec les services de l'État, elles sont informées du niveau d'alerte et des types de risques existants, ce qui leur permet d'imaginer des parades avec les mesures à prendre et les réponses à apporter. Enfin, elles peuvent conseiller la mise en place de matériels performants répondant aux menaces identifiées. Malheureusement, les directions sûreté n'ont pas l'écoute de la plupart des dirigeants d'entreprises pour qui la sécurité relève plus du gardiennage que d'une activité transversale spécifique dont les failles peuvent coûter très cher tant au niveau du coût que de l'image.

La baisse des capacités financières de nos ministères suite à la crise économique ne permet pas d'augmenter les effectifs de policiers et de gendarmes alors que nos concitoyens ont une exigence croissante de sécurité collective. La multiplication des cibles potentielles et la variété des types d'actions demandent pourtant un accroissement sensible des moyens humains et matériels de sécurité dans les sites publics ou privés. La seule solution est donc un transfert de responsabilité régalienne de la police nationale vers les polices municipales, la garde nationale et les sociétés privées de sécurité. Mais ceci n'est envisageable que dans un cadre parfaitement défini pour répondre aux exigences de ce type d'activité dans le respect du droit.

L'utilisation de militaires, de policiers ou de gendarmes pour faire des gardes statiques pose le problème de l'optimisation des moyens. Il est évident que ce type de travail ne requiert pas les années de formation propre à d'autres actions de service public. Utiliser pour les patrouilles de *Vigipirate,* un militaire, formé pour la guerre sur un territoire extérieur avec un armement sophistiqué, est à l'évidence une mauvaise solution. C'est pourquoi il faut identifier toutes les activités n'exigeant pas un niveau de qualification élevé et envisager une délégation de responsabilité à un personnel capable d'assurer ce type de mission. Ceci permettra de dégager les spécialistes de ces missions banales pour qu'ils soient pleinement utilisés dans leur domaine d'expertise. La sécurité des fans zones qui a vu la collaboration de la police nationale, des polices municipales et des sociétés de sécurité privée en est une magnifique et probante démonstration.

Dans un certain nombre de cas, les nouveaux outils de sécurité numérique permettent de remplacer avantageusement la surveillance humaine. La télésurveillance interconnectée avec les logiciels d'identification ou d'analyse comportementale a fait la preuve de son efficacité en réduisant sensiblement les incidents et les temps de réponse. Les drones remplacent avantageusement les patrouilles sur une zone déterminée pour en assurer une surveillance permanente. Les robots de surveillance interne multi-capteurs se montrent souvent plus efficaces que les gardiens faisant des rondes dans les sites. Ceci permet de libérer du personnel pour rejoindre les forces d'intervention.

Transférer la sécurité de personnes ou de sites, assurés par l'État, à des sociétés présentant toutes les garanties nécessaires et travaillant sous le contrôle du ministère de l'Intérieur, implique de bien les différencier des activités classiques de sécurité privée. La solution la plus simple, comme le font déjà nombre de pays étrangers, pourrait être d'utiliser des sociétés de type ESSD qui assurent déjà la sécurité maritime ou celle de certaines de nos ambassades, car chacun comprend que ceci n'a rien à voir avec une société de gardiennage. L'activité implique, par exemple, d'avoir résolu le problème de l'armement et de l'ouverture du feu en légitime défense. Il faut également avoir la certitude que l'agent est irréprochable, ce qui suppose une enquête préalable et un suivi régulier. Il faut, enfin, qu'il ait reçu la formation nécessaire et puisse en fournir la preuve.

Tout ceci se fait pour les convoyeurs de fonds depuis des années sans qu'il y ait de problèmes. On sait également que de nombreux militaires, en fin de contrat opérationnel, recherchent des emplois dans le civil. Ils pourraient parfaitement assumer ce type de travail dont ils maîtrisent les techniques avec l'expérience requise. ■

CHRONOLOGIE

2012

Toulouse *et* **Montauban (France) du 11 au 19/03/2012**

Mohammed Merah ***tue 7 personnes*** *et fait* ***6 blessés*** *Le 11, il tue d'une balle dans la tête* ***un sous officier*** *du 1er RTP. Le 15, il tue* ***deux militaires*** *du 17ème RGP avec des armes à feu. Le 19, il se rend au collège-Lycée juif Ozar Hatorah à Toulouse.* ***4 victimes dont 3 enfants.***

2013

Paris (France) 15/11/2013

Le directeur adjoint de ***BFM TV*** *est menacé par Abdelhakim Dekhar, armé d'un fusil, dans le hall de la rédaction.*

L'auteur de l'attaque serait également à l'origine de celle, perpétrée trois jours plus tard, sur un assistant de ***Libération****, grièvement blessé, des coups de feu devant la* ***Société Générale à La Défense*** *et de la brève* ***prise d'otage d'un automobiliste****.*

LES ENTREPRISES FACE À LA MENACE DJIHADISTE CONTEMPORAINE

AMARANTE International

Rapidement suivies par une série d'actions visant la Belgique ou encore l'Allemagne, ces attaques ont érigé la lutte contre la menace djihadiste au rang de priorité nationale, entraînant une mobilisation sans précédent des pouvoirs publics - français comme européens - autour du renforcement de la protection des cibles sensibles (bâtiments gouvernementaux, lieux de culte, événements sportifs et culturels).

Or, en France, les mesures et dispositifs instaurés dans le cadre de l'état d'urgence (renforcement de l'opération Sentinelle, adaptation des dispositions légales relatives à la lutte anti-terroriste) n'ont donné lieu qu'à peu ou pas de mesures spécifiques visant la protection des entreprises, entretenant la perception que ces dernières font office de cibles secondaires pour les organisations djihadistes.

Pourtant, les mutations stratégiques en cours au sein de la nébuleuse djihadiste transnationale - incarnée par Al-Qaïda (AQ) et l'état Islamique (EI) - tant dans l'accélération des opérations que dans la démultiplication des cibles, tendent à remettre en cause cette assertion.

Les entreprises : une cible traditionnelle de l'action djihadiste à l'international

En tant que symbole et vecteur de la puissance économique d'un État, les entreprises ont traditionnellement constitué une cible privilégiée pour les organisations djihadistes, à l'image des exemples qu'offre l'histoire contemporaine des opérations menées par Al-Qaïda et ses affidés. Action la plus emblématique, les attentats du 11 septembre 2001 constituent sans aucun doute le précédent le plus spectaculaire de ciblage d'une entité économique occidentale, engendrant, outre la portée symbolique de l'opération, un véritable séisme économique pour la ville de New York, avec la perte temporaire de près de 143 000 emplois et plus de 40 milliards de dollars de dédommagements assuranciels.

Les nombreuses attaques menées par les unités locales d'Al-Qaïda (*cf. chronologie*) visaient ainsi à servir les intérêts de l'organisation dans le combat contre ses ennemis occidentaux par deux biais :

– un biais symbolique d'abord, en portant atteinte aux intérêts économiques occidentaux en dehors de leurs frontières, à l'heure où l'organisation disposait de peu de moyens de projection en Europe ou aux États-Unis ;

France 23/04/2014

Le ministre de l'Intérieur présente les grandes lignes du plan contre la radicalisation violente et les filières terroristes en Conseil des ministres.

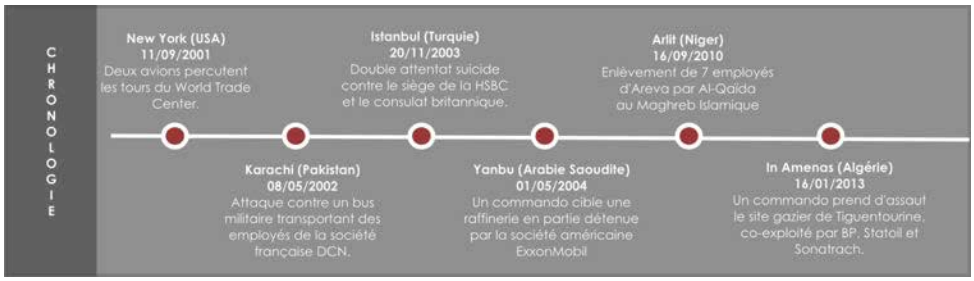
France 13/11/2014

Adoption de la Loi n°2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme.

2014

Bruxelles (Belgique) 24/05/2014

*Mehdi Nemmouche **abat quatre personnes** à l'aide d'un revolver puis d'un fusil d'assaut dans le Musée juif de Belgique.*



– un biais stratégique ensuite, visant à répondre aux ambitions locales des groupes djihadistes (contrôle de territoire, exploitation des ressources, développement de modes de financement par la revente de pétrole ou de véhicules volés, etc…) ou en renforçant leurs moyens de pression sur les autorités des pays ennemis, notamment via le recours aux enlèvements.

Si les entreprises étaient prioritairement ciblées à l'international, et les actions dictées par des logiques locales de puissance, l'avènement de l'État Islamique et la proclamation du Califat en mai 2014 a rebattu les cartes de la stratégie poursuivie par les organisations djihadistes, mettant en concurrence les combattants d'Abou Bakr al-Baghdadi et ceux d'Ayman al-Zawahiri. Dans cette course aux actions spectaculaires – aujourd'hui dominée par l'EI – les acteurs privés occidentaux sont désormais érigés, par les deux organisations, au rang de cible déclarée.

Une mutation de la menace djihadiste qui renforce l'exposition des entreprises

Jusqu'alors prisées en tant que cibles de proximité – car implantées sur les théâtres d'opération des groupes djihadistes – les entreprises font désormais partie intégrante de la typologie des objectifs militaires visés par Al-Qaïda et l'État Islamique, dont le discours récent vient confirmer, par des menaces explicites de deux ordres, l'inclusion des acteurs privés comme ennemi avéré du combat djihadiste :

– Des menaces à l'encontre des acteurs considérés comme des vecteurs de la puissance économiques des États ennemis, à l'image de l'allusion à une cible économique française de renommée internationale dans une vidéo de l'État Islamique, publiée au lendemain des attaques du 13 novembre.

– Des menaces à l'encontre des acteurs économiques accusés d'entraver le combat idéologique menée par les organisations djihadistes, à l'image de l'avertissement adressé par l'EI à Jack Dorsey - patron de *Twitter* - et Mark Zuckerberg - créateur de *Facebook* - en raison de la suppression croissante des comptes de militants sur les réseaux sociaux. Les entreprises engagées dans des activités contraires aux moeurs islamiques – considérées comme « haram » – constituent également des cibles légitimes, à l'image de l'attentat déjoué contre une usine *Carlsberg* située près de Kuala Lumpur (Malaisie), en août 2014.

À l'heure où ces menaces récentes viennent confirmer l'intérêt porté par les organisations djihadistes au ciblage des entreprises, le renforcement de la menace pesant sur les acteurs privés est aujourd'hui mû par deux tendances distinctes mais concomitantes :

– L'évolution à la hausse du développement international des acteurs privés, qui démultiplie les opportunités de ciblage pour les militants du djihad armé. Alors que cette menace concernait principalement, pour le marché français, les entreprises du CAC40 implantées en zones à risques (Irak, Yémen, Sahel) - relevant du secteur du Oil&Gas et du BTP - les entreprises de plus petite taille (PME et ETI du secteur des services ou du consulting) trouvent désormais leurs relais de croissance à l'international, s'exposant *de facto* à une menace dont elles parviennent généralement moins à se prémunir (*cf. infra*).

– L'accroissement significatif du nombre de sympathisants

CHRONOLOGIE

Dijon (France) 21/12/2014
*Un conducteur **renverse** volontairement **13 personnes** sous les cris de « Allah ouakbar ».*

Le Mans (France) 22/12/2014
*Un terroriste, hurlant « Allah ouakbar ! », **attaque des policiers** et tente de s'emparer de leurs armes.*

2014

Metz (France) 2/01/2015
*Un terroriste, hurlant « Allah ouakbar ! », **tente d'étrangler à mains nues un policier***

Paris (France) 07/01/2015
***Charlie Hebdo** victime d'une attaque terroriste perpétrée par Saïd Kouachi et Chérif Kouachi. **Dix journalistes et deux policiers meurent** sous une fusillade sous les cris de « Allah Akbar » et « On a vengé le Prophète Mohammed, on a tué Charlie Hebdo ».*

2015

de la cause djihadiste et l'extension non négligeable de leurs zone d'influence, sous l'impulsion de l'État Islamique. Fort d'un appareil de communication pouvant toucher le plus grand nombre - *via* une utilisation stratégique des réseaux sociaux - l'EI dispose aujourd'hui d'une capacité de recrutement international jamais égalée par Al-Qaïda, lui permettant de mener des opérations complexes sur des zones réputées sûres, à l'image de la France.

Alors que ce constat renforce la probabilité d'actions malveillantes visant les entreprises, ces dernières doivent désormais se prémunir contre une menace pouvant concerner trois types de cibles :

1) **Les personnels d'abord**, particulièrement concernés par un risque de dommages collatéraux lors d'attentats ciblant les infrastructures de transports (aéroport d'Istanbul ou Bruxelles) ou les hôtels (*Radisson Blu* à Bamako), mais également par la menace d'enlèvement, à l'heure où la mobilité internationale embrasse une courbe exponentielle ;

2) les **infrastructures** ensuite, selon un niveau de criticité propre à chaque secteur : alors que certaines entités seront ciblées pour leur caractère névralgique - centrale électrique, raffinerie, etc… – d'autres seront prisées pour leur forte concentration de civils, venant servir les visées médiatiques des organisations djihadistes. Présentant dans leur grande majorité des dispositifs de sécurité bien plus légers que les infrastructures étatiques, les infrastructures privées sont, à cet égard, considérées comme des cibles « molles » pour les militants djihadistes, amenant Abou Mohammed al-Adnani, porte-parole de l'EI neutralisé le 30 août 2016, à explicitement appeler ses partisans à se détourner des « cibles militaires » pour leur préférer les acteurs économiques, plus accessibles (agence de communication *Al-Furqan,* 21/05/2016) ;

3) enfin, les atteintes à l'image de l'entreprise, *via* l'association publique de certaines marques avec des organisations djihadistes, ne doivent pas être négligées. Pour exemple, l'unité de financement du terrorisme du département américain du Trésor a ainsi ouvert une enquête en 2015 sur l'utilisation massive de véhicules Toyota par l'État Islamique.

Si les entreprises françaises ont, pour la plupart, pris la mesure de la menace accrue pesant sur leurs intérêts à l'international, le risque d'action ciblant des acteurs économiques dans l'Hexagone est souvent jugé moins immédiat. Bien que la plupart des opérations recensées

Image extraite d'une vidéo de propagande de l'EI

sur le territoire national visait en priorité des cibles symboliques – forces de sécurité, salle de concert, bars, communautés religieuses – de nombreuses actions ont directement menacé des opérateurs privés, au premier rang desquels les professionnels des médias, à l'image de l'attaque des locaux de *Charlie Hebdo*, le 7 janvier 2015, mais également des actions menées par Abdelhakim Dekhar en novembre 2013 contre *BFMTV* et Libération.

Alors que les médias constituent une cible traditionnelle des militants djihadistes, l'attaque ayant visé le site de l'usine *Air Products* - classé Seveso seuil bas, le 26/06/2015 à Saint-Quentin-Fallavier (Isère), constitue une matérialisation inédite du ciblage d'une entreprise par l'État Islamique sur le sol français.

Dans la cinquième édition de la revue francophone, Dar al-Islam, l'organisation a ainsi consacré une section dédiée à l'« **opération du frère Yassin** », en y associant un argumentaire détaillé sur l'activité de l'entreprise et sur la nationalité supposée de son dirigeant, afin de légitimer l'opération.

Bien que les éléments constitutifs de la menace djihadiste attestent ainsi de la crédibilité du risque pesant sur les entreprises – y compris dans l'Hexagone –, la mobilisation des ressources nécessaires à la protection des intérêts privés peine à se concrétiser.

De l'urgence de la protection des entreprises : une prise de conscience en demi-teinte ?

En effet, forte de ce constat, la nécessité de mettre en place des solutions de protection spécifiques aux entreprises se heurte à une prise de conscience en demi-teinte de la part des acteurs concernés.

2015

Paris (France) 8/01/2015
*Une **policière municipale est tuée** et **un agent municipal grièvement blessé** par Amedy Coulibaly, terroriste se revendiquant de l'Etat Islamique portant un gilet d'assaut et lourdement armé.*

Carcassonne (France) 8/01/2015
*Un individu, armé d'un couteau, hurle «Allah ouakbar !» et **menace de mort un militaire** du 3e RPIMa.*

Dammartin-en-Goële (France) 9/01/2015
Les frères Kouachi se retranchent dans l'entreprise CDT. Échange de coups de feu entre une patrouille de la brigade de Dammartin et les terroristes, avant que ces derniers ne soient neutralisés part le GIGN.

Paris (France) 9/01/2015
*Prise d'otages dans une épicerie casher par Amedy Coulibaly. **4 morts**. L'auteur de la prise d'otages succombera lors de l'assaut du RAID/BRI.*

Du côté des entreprises d'abord, l'appréhension de la menace djihadiste est régie par une dichotomie liée à la taille des acteurs : si les sociétés du CAC40 peuvent capitaliser sur une expérience de longue date en matière de sûreté – disposant pour la plupart de directions dédiées, forgées par leur expérience à l'international – les PME et ETI n'intègrent pas systématiquement les questions de protection au coeur de leur schéma décisionnel.

Souvent peu conscientes de la prégnance de la menace pesant sur les acteurs privés, les petites et moyennes entreprises adoptent généralement une approche de rationalisation des coûts liés à la sûreté, misant davantage sur la faible probabilité d'une attaque que sur le fort impact que celle-ci aurait sur l'entreprise.

Dans ce contexte, les moyens de protection soumis à obligation légale (selon les jurisprudences Jolo et Karachi) connaissent une tendance à la hausse – information aux voyageurs d'affaires des risques inhérents à leur destination, *Meet & Greet*, dispositifs d'escorte dans les zones les plus à risque – mais les mesures d'anticipation – étude de vulnérabilité, audit de site, plans d'évacuation – ne sont quant à elles pas systématiques.

Quant aux acteurs privés désireux de renforcer la sécurisation de leurs intérêts, ces derniers se heurtent aux apories du **cadre légal et étatique**, qui proposent des solutions en augmentation mais encore peu conformes aux besoins du marché. Marquée par la tradition jacobine, la France a jusqu'alors capitalisé, à juste titre, sur la mission régalienne de l'État pour sécuriser les acteurs privés présents sur son sol. Néanmoins, à l'heure où la menace concerne désormais une multitude de cibles, les moyens d'État sont prioritairement alloués aux missions de renseignement et de maintien de l'ordre, ne permettant pas d'embrasser le besoin croissant de protection pouvant être exprimé par les entreprises.

Si certains signaux semblent témoigner d'une inclinaison favorable à un assouplissement du cadre régissant la sollicitation des acteurs privés de la sécurité – à l'image de la loi Savary votée en mars 2016, autorisant depuis le 1er octobre dernier les agents de sécurité de la SNCF et de la RATP à patrouiller en civil et en armes dans les transports – la question de la qualité des services offerts par les acteurs du privé demeure un sujet de préoccupation pour les dirigeants d'entreprise, à laquelle la perspective d'une collaboration plus étroite des pouvoirs publics avec les professionnels privés de la sécurité privée semble constituer la meilleure des réponses à venir. ■

ATTAQUE CONTRE L'UNE DES USINES GAZIÈRES DE FRANCE

L'équipe de Dār Al-Islām salut l'opération du frère Yassin et encourage tout musulman qui ne peut émigrer et qui a de la fierté pour sa religion de frapper les intérêts des ennemis d'Allāh qui font quotidiennement la guerre à l'Islām et aux musulmans.

La Cible

L'opération a été effectuée le 9 joumoûzah (vendredi) de ce mois béni de Ramadān sur le site sensible d'Air Products, fournisseur de gaz et de produits chimiques à usage industriel, une société américaine située dans la zone logistique de Saint-Quentin-Fallavier, entre Lyon et Bourgoin-Jallieu, non loin de l'aéroport Saint-Exupéry, en Isère. Il s'agit du plus grand fournisseur d'hydrogène et d'hélium au monde.

En avril dernier, la compagnie avait signé un contrat avec la société saoudienne Saudi Aramco pour créer et exploiter le plus grand complexe industriel d'exploitation de gaz au monde pour les vingt prochaines années à Jazan. Cette même compagnie est dirigée depuis 2014 par un Iranien d'origine, naturalisé citoyen américain, le nommé Seifi Ghasemi.

L'attaque

Le frère est arrivé à bord d'une camionnette de livraison. Comme il avait l'habitude de venir sur le site, la porte lui a été ouverte. Il a d'abord foncé au volant de son véhicule sur plusieurs bonbonnes de gaz stockées dans un des hangars du site, provoquant une explosion dont il a pu réchapper. Il s'est alors rendu dans un second hangar pour tenter de déclencher une seconde explosion en ouvrant des bouteilles d'acétone.

Le frère a pu aussi mettre la main sur le chef d'entreprise nommé Hervé Comara, il l'a fait monter à l'arrière de sa fourgonnette, l'a assommé d'un coup de cric, l'a étranglé d'une seule main puis l'a décapité, par la grâce d'Allāh.

Il a ensuite accroché sa tête à l'aide de chaînes au grillage d'enceinte du site et l'a entourée de deux drapeaux du Tawhīd.

Dar al-Islam - édition n°5 - juillet 2015

Interview de
GILLES KEPEL

Gilles KEPEL

Directeur de la Chaire Moyen-Orient-Méditerranée
à l'École Normale Supérieure et professeur à Sciences-Po.

2 novembre 2016, ENS Paris – Propos recueillis par Diane de Laubadère

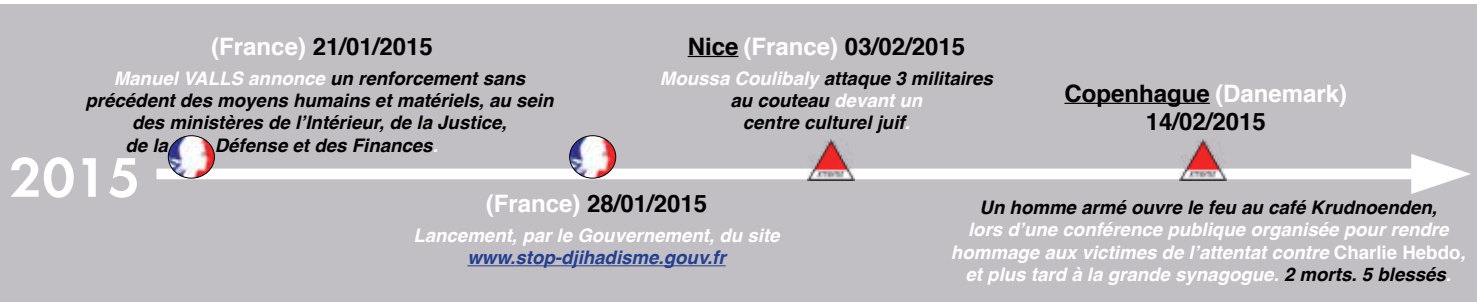
? Les entreprises comme les pouvoirs publics n'ont pas vu la menace terroriste islamiste arriver sur le territoire. Pourtant les prospectivistes en matière de recherche sur les nouveaux conflits ont inondé le marché des centres d'études pendant une dizaine d'années. Est-ce un aveu d'échec de la pensée stratégique française ? Ou bien la recherche universitaire n'a-t-elle pas l'écoute des pouvoirs publics ? Le fait est que les conséquences du terrorisme islamiste sur le territoire se mesurent en nombre de morts et en perte de chiffre d'affaires pour les entreprises victimes de la dégradation de l'image et de la réputation de la France.

Or, pour gérer la menace nous avons besoin de la comprendre. Ne faut-il pas en revenir à une démarche analytique, pour en déchiffrer les origines, l'ampleur et son expression contemporaine sur le territoire ? N'est-il pas le moment, à nouveau, de croire en la capacité de la recherche à nourrir l'action publique ?

C'est en partie le sens de mon dernier ouvrage *La fracture*, publié chez Gallimard. L'idée était d'adopter une démarche chronologique couvrant les 2 années d'entretiens radiophoniques sur *France Culture* pour remonter de l'attentat contre la rédaction de *Charlie Hebdo* jusqu'à celui de Saint-Etienne-du-Rouvray. Il s'agit d'informer nos concitoyens des logiques du djihadisme. Ni les élites dirigeantes, elles-mêmes désemparées, ni les médias ne l'ont fait après les tueries de janvier 2015.

Je vois une nécessité à diffuser cette connaissance. D'une part, pour échapper aux clivages identitaires et communautaristes qui font prévaloir l'appartenance religieuse et ses marqueurs sur le territoire et dans l'espace public et qui fracturent la France aujourd'hui. D'autre part, pour combler le « gouffre culturel » qui explique en partie l'incapacité des pouvoirs publics à comprendre les bouleversements qui se sont opérés dans la société. C'est aussi ce qui peut expliquer qu'ils n'aient pas vu ce djihadisme de 3ème génération pénétrer le tissu social français. Les rapports qui auraient pu servir à éclairer la décision sur ces aspects sécuritaires n'ont pas, ou peu, été exploités. Par exemple les techniques opératoires de casting des potentiels protagonistes sont connues depuis longtemps. Elles sont présentes dans les textes fondateurs que j'ai traduit en français dans *Terreur et martyrs*, cela depuis 2008.

Les enquêtes de terrain *Quatre-vingt-treize* que j'ai publiées, début 2012, sur la Seine Saint-Denis et *Passion Française*, en 2014, n'ont eu qu'un faible écho dans la presse et auraient pu davantage être exploitées par les pouvoirs publics. Nous avons affaire à une forme de déni qui consiste à ne pas vouloir comprendre le monde dans lequel nous vivons. Les deux écrits *L'Appel à la résistance islamique mondiale et Management de la sauvagerie* constituent leur doctrine d'emploi dont on retrouve malheureusement une application quasiment à la lettre dans certains des événements qui ont frappé le territoire depuis janvier 2015.



Il y a un changement culturel à mettre en oeuvre dans le fonctionnement de l'État et une remise en question importante à faire de la part de ceux qui aspirent à diriger le pays. C'est aussi l'enjeu pour 2017.

Le rapprochement entre la recherche universitaire et les dirigeants politiques me paraît en cela être essentiel. C'est le sens du Conseil de la stratégie et de la prospective, dont la première réunion s'est tenue le 18 octobre 2016 sous la présidence du Ministre de l'Intérieur.

? Quel est votre regard sur les attentats depuis janvier 2015 ?

Les faits parlent d'eux-mêmes. Ils disent l'ampleur de la menace et sa capacité à pénétrer le territoire. Il a eu 239 morts entre « *Charlie hebdo* », le 7 janvier 2015, et « Saint-Etienne-du-Rouvray », le 26 juillet 2016. Le bilan de la nuit du 13 novembre est de 130 morts et de 413 blessés hospitalisés, dont 99 en situation d'urgence absolue, le plus grand massacre de civile en une journée sur le territoire français depuis Oradour-sur-Glane, le 10 juin 1944. Les 86 morts à Nice, attentat perpétré par un camion de livraison par une seule personne, montre l'utilisation de moyens triviaux de destruction.

Cette menace est d'autant plus préoccupante que nous avons affaire à un djihadisme de 3ème génération, réticulaire, qui confie la réalisation des attentats à leurs exécutants. Il se distingue d'Al-Qaïda où le commandement central, coiffé par Oussama Ben Laden, planifiait ses actions à l'image des opérations militaires. L'attaque du 11 septembre illustre cette organisation pyramidale et l'utilisation de moyens élaborés, perpétrée par des individus longuement formés et entraînés. Aujourd'hui, avec le djihadisme de 3ème génération, les exécutants ne le sont plus nécessairement. Ils partent sur le terrain syrien moins pour se former que pour se familiariser avec la violence. Là, ils multiplient les assassinats des « apostats » et la profanation des cadavres. Les vidéos circulent ensuite sur l'Internet et servent de vecteur de propagande. Ils peuvent être activés à partir de la messagerie sécurisée préférée des djihadistes en 2016, *Telegram*, et par l'intermédiaire des chaînes de télévision privées telles que *Ansar al-Tawhid*. Autre distinction est l'utilisation des moyens : que ce soit dans le cas des « attaques ciblées » visant des individus spécifiques, comme la rédaction de *Charlie Hebdo*, ou les « attaques de masse », comme celle de Nice, ils sont incités à utiliser les moyens du bord, couteau de cuisine, camion de livraison, bonbonne de gaz... Leurs actions mêlent la truanderie à l'idéologie.

L'exemple le plus frappant est celui de Saint-Etienne-du-Rouvray où les 2 tueurs de 19 ans, Adel Kermiche et Abdel Malik Petitjean, qui ne se connaissaient pas, ont été mis en contact par l'intermédiaire de *Telegram*. Ils ont vraisemblablement été manipulés à distance par une tête du réseau, Rachid Kassim. Kermiche, d'origine Kabyle d'Algérie, ne parlait pas arabe, avant d'être incarcéré et radicalisé en prison. Il en sort en étant capable de prononcer le sermon en allégeance à peu près correctement en arabe. Le 26 juillet 2016, ils utilisent un couteau de cuisine pour exécuter le prêtre alors même que l'individu en question a un bracelet de surveillance électronique et qu'il agit pendant ses heures légales de sorties de domicile du fait de son contrôle judiciaire. On ne peut pas avoir un exemple plus frappant du djihadisme de proximité et de la menace aujourd'hui.

Le cas de Magnanville est également illustratif de ces attaques ciblées visant des individus spécifiques. Dans le cadre de l'entreprise, le jeune salarié, Yassin San, là encore pour des raisons que nous ne connaissons pas très bien, entre en contact avec l'État Islamiste. Il va décapiter son patron, mettre sa tête sur la clôture de l'entreprise classée SEVESO, et s'efforcer de faire exploser cette dernière, un peu dans la logique de ce qui s'était passé à Toulouse chez AZEDEF. L'hypothèse terroriste écartée à l'époque refait surface aujourd'hui. Nous avions sous-estimé l'importance de la *communauté islamiste d'Artigat*, en Ariège, par où était passé tout le milieu toulousain.

? Qu'est-ce qui explique que nous n'ayons pas perçu cette réalité de la menace ?

Cela montre les limites du renseignement à avoir perçu l'évolution du djihadisme dans ses modes opératoires, ses moyens de communication et de recrutement.

Durant la première phase du Djihadisme, de 1979 à 1997, où les ennemis de proximité, les régimes « apostats », sont les principales cibles, les services de renseignements français s'investissent dans la détection de la menace djihadiste en France. Dans la deuxième phase du djihadisme, celle du terrorisme d'Al-Qaïda, entre 1998 et 2005, les services sont très performants notamment du fait des arrestations en nombre qui auront permis d'éviter une série d'attentats.

Cette méthode a fonctionné jusqu'à l'affaire Mohammed Merah, le 19 mars 2012. En concentrant leurs actions sur les arrestations, ils n'ont pas perçu en parallèle la force du prosélytisme qui se développait en prison et dans les quartiers

CHRONOLOGIE

2015

Lyon (France) 17/02/2015

*Un déséquilibré, hurlant des **propos incohérents faisant référence à l'État Islamique**, agresse violemment **une septuagénaire**.*

Villejuif (France) 19/02/2015

*Une tentative d'attentat contre deux églises de Villejuif est détourné. À 8h50 Sid Ahmed Ghlam appelle le SAMU, il est blessé par deux balles. Selon les enquêteurs il se serait lui-même blessé au cours de la tentative de vol du véhicule d'**Aurélie Châtelain**, celle-ci est tuée et il aurait ensuite brûlé la voiture, qui contenait le corps de la jeune femme, avant de regagner le XIIIème arrondissement. La police arrête alors Sid Ahmed.*

Grasse (France) 20/02/2015

*Un **détenu**, qui était sur le point d'être libéré, poste, depuis la cellule de sa prison, sur le **compte Facebook** d'une amie, une **vidéo de 25 minutes à la gloire de l'État Islamique** et la **photo d'un djihadiste posant avec cinq têtes décapitées.***

populaires enclavés dans lesquels les musulmans devenaient la cible des recruteurs. Ils leur promettent encore la rédemption par le Djiad.

Les services, habitués à Ben Laden, n'ont pas su détecter la révolution culturelle de ce djihadisme de 3ème génération, réticulaire, qui va transformer en vecteurs de prédication les sites de partage vidéo, les réseaux sociaux, *twitter*, *facebook* jusqu'à *Instagram*.

Le cloisonnement du fonctionnement des services de l'État et le mépris total dans lequel la recherche universitaire est tenue, par les hiérarchies policières, du renseignement et de la justice, ont abouti au fait que nous avons eu dix ans de retard pour appréhender le phénomène.

Le fait que Merah soit encore décrit comme «un loup solitaire» par la plupart des journalistes et par de nombreux analystes est simplement l'expression de leur ignorance et de l'impréparation de la majorité de notre classe politique. Socialisé à travers ses voyages dans le milieu djiadiste international, Merah est ensuite activé pour agir dans sa proximité immédiate, à Montauban, et à l'École juive Ozar- Hatorah de Toulouse, tout comme Kermiche le sera quatre ans plus tard. Cette affaire aurait dû être entendue comme un signal fort d'une menace qui allait devenir la principale préoccupation du pays.

? En quoi consiste cette fracture et percevez-vous des leviers sur lesquels agir pour l'éviter ?

La fracture est double et menace de conduire à la guerre civile. Les tentations du repli viennent, d'un côté, des mouvements communautaristes musulmans qui perçoivent la Nation comme un instrument au service d'un idéal distinct et réduisent la nationalité française à ces avantages sociaux et aux papiers d'identités. Cette posture montre, entre autre, l'échec de l'idéal de cohésion de la Patrie que les enfants d'immigrés postcoloniaux auraient dû incarner. De l'autre, une conception identitaire de la France au fond ethno-racial, xénophobe. L'affaire du «burkini» a renforcé ces extrêmes mais a surtout donné l'occasion de renverser l'image internationale de la France de victime en pays islamophobe. Ce coup réputationnel à l'égard de la France a servi les stratégies d'hégémonie sur l'islam de France en faisant notamment passer au second plan le djiadisme.

Les attentats jouent également un rôle précis dans le renforcement des extrêmes. Leur violence a pour fonction de sidérer la société, de susciter des réactions d'une brutalité égale voire supérieure, qui auront pour effet de générer des pogroms, de nouveaux massacres en riposte dans les mosquées etc… Cela renforcerait irrémédiablement le processus de victimisation d'une communauté musulmane alors doublement tentée par le djihadisme.

Le CCIF (collectif contre l'islamophobie en France), dirigé par des Frères musulmans immigrés, a contribué à ce retournement de situation. Il s'inscrit dans la mouvance d'un Tariq Ramadan, s'entoure de certains universitaires, de l'extrême gauche et de relais dans les médias, et cherche à occuper le leadership des «élites musulmanes de France» et se faire les représentants d'une communauté victimisée. Le *tweet* du 19 août dernier de Philippe Poutou en témoigne: «stop à l'#islamophobie d'État! Non à l'interdiction des #burkinis!». Cet épisode relève d'une opération montée par le CCIF dans la perspective de construire un lobby d'influence islamiste dans l'électorat qui consistera à le diviser en 2017 entre candidats islamophobes et ceux qui ne le sont pas.

Cette fracture menace la société dans ses fondements puisés dans la philosophie des Lumières et la Révolution française. L'attaque du 14 juillet est, en ce sens, une opération symbolique créant à la fois la terreur et la déstabilisation d'une Nation qui s'est construite sur le principe de laïcité et de l'autonomie par l'éducation. Comme on était Grec par la palestre dans l'Athènes classique, on était Français par l'école et le lycée.

La crise que traverse le système éducatif français n'est pas anodine. Les savoirs ne sont plus utilisables dans la société post-industrielle et numérique, comme c'est le cas aujourd'hui dans les lieux défavorisés où un pourcentage important des jeunes est au chômage. Cela explique, en partie, que les valeurs portées par l'école soient rejetées. Et c'est dans le repli communautaire et dans la soumission à une charia façon salafiste qui lutte contre la république laïque, que le glissement vers le djihadisme va se produire. Ce débat dépasse *stricto sensu* le djihadisme mais il met le doigt sur nos propres failles sur lesquelles il prospère.

L'éducation est donc à la fois une faille et un levier sur lequel nous devons concentrer nos efforts.

? L'entreprise n'est-elle pas un lieu où cette fracture se cristallise ? Ou bien se présente-t-elle comme un autre levier possible sur lequel agir ?

Par définition, l'entreprise est le lieu où cette fracture devrait se résorber

puisque l'ensemble des actions qui y sont menées visent à entreprendre, produire du capital et du travail, de la richesse et de l'épanouissement de soi.

A contrario, parce qu'elle peut générer de l'insatisfaction de la part des salariés, elle peut aussi constituer une cible de la part de ceux qui veulent se venger d'un système dont ils se sentent rejetés. Elle peut aussi favoriser les regroupements communautaristes religieux. Les pratiques religieuses, sont de plus en plus ostentatoires et revendiquées comme des droits. Ce phénomène est particulièrement présent dans les emplois logistiques et dans la sécurité. La mouvance des Frères musulmans recrute plutôt des gens diplômés qui vont occuper des emplois de cadres. Ceux-là conduisent des actions d'influence qui se distinguent de la radicalisation violente et posent d'autres types de questions. Ils constituent les marqueurs d'une clôture communautaire et religieuse. C'est la stratégie de Tarik Ramadan et du CCIF de former une élite structurée en lobby électoral, en groupes de pression professionnels, etc.

Il y a une vraie réflexion à conduire au sujet du prosélytisme en entreprise et de la pratique religieuse.

Mais, il ne faut pas confondre ce phénomène avec le Salafisme en tant que tel, peu présent dans l'entreprise. Les actes de Yassin Sahi, qui finit par découper la tête de son patron, ne sont pas des actes de vengeance, le résultat d'un banal conflit de travail. Attention à cette assimilation qui peut donner raison à une pensée dénégationniste ne voulant voir dans ces criminels que des déstabilisés psychologiques. Psychose et djihad sont mêlés, mais tous les psychotiques ne sont pas djihadistes, comme toutes les pratiques religieuses, même ostentatoires ne conduisent pas à décapiter son patron. Attention à ces interprétations qui contribuent à fracturer la société.

Pouvons-nous considérer que nous sommes en situation de guerre sur le territoire ?

Je récuse la formule de « la France est en guerre ». Nous ne sommes pas dans un état de guerre à proprement parler. Ce serait aller dans le sens des djihadistes qui cherchent précisément à déclencher une guerre civile en Europe.

Les interventions sur le territoire restent policières. La haute administration dispose d'une masse d'informations permettant les arrestations de suspects.

Poser la question de la fracture c'est aussi donner à la société française, remarquablement résiliente, la possibilité de résister sans tomber dans l'écueil des extrémismes.

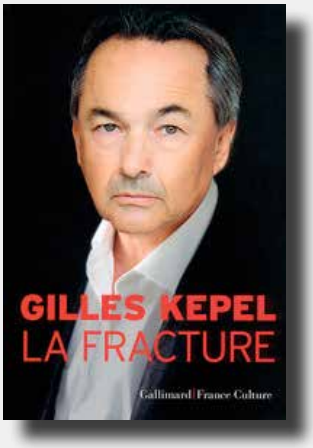
Pensez-vous qu'en France nous parviendrons à créer davantage de passerelles entre ces sphères du privé, du public et de la recherche universitaire pour améliorer la protection ? Pensez-vous que ce serait une piste à creuser pour renforcer notre capacité de résilience ?

Oui et je crois que c'est tout à fait faisable en France parce que l'entreprise, notamment grâce aux ressources qu'elle peut mobiliser, est capable de contribuer à cette résilience. Il y a aujourd'hui énormément d'officines de sécurité qui vendent des services de protection dont certains sont factices. Cela représente des budgets énormes qui pourraient être davantage rationalisés par une concertation entre les entreprises et les pouvoirs publics sur l'emploi des forces et des moyens.

Or, il me semble que nous pourrions progresser si les pouvoirs publics associaient à leur réflexion avec les entreprises, la recherche universitaire, qui apporte une analyse de la menace suffisamment précise pour éclairer la décision et adapter nos dispositifs de protection à la réalité. C'est quelque chose qui est à faire et dans des délais courts. ■

POUR ALLER PLUS LOIN

LA FRACTURE



Coédition Gallimard / France Culture
Hors série Connaissance, Gallimard , Novembre 2016

TERREUR DANS L'HEXAGONE.
Genèse du djihad français

Avec la collaboration d'Antoine Jardin

Hors série Connaissance, Gallimard, Décembre 2015

CHRONOLOGIE

Paris (France) 09/04/2015
TV5 Monde est victime d'une attaque cyber-terroriste sans précédent et revendiquée par l'Etat Islamique (EI).

(France) 24/07/2015
Promulgation de la loi n°2015-911 relative à la nomination du président de la Commission nationale de contrôle des techniques de renseignement et de la loi n°2015-912 relative au renseignement

2015

Saint-Quentin-Fallavier (France) 26/06/2015
Yassin Salhi attaque une usine de production de gaz industriels. Il décapite son patron, Hervé Cornara, avec un couteau. Yassine Salhi agissait pour le compte de l'Etat Islamique.

ÉVOLUTIONS DU DJIHADISME

La société civile et les entreprises interpellées par la lutte contre la radicalisation

Romain SEZE

Sociologue, Chargé de recherche à l'INHESJ
et rattaché au GSRL (EPHE-CNRS)

Alors que la gestion du terrorisme relevait jusque-là des compétences de l'appareil régalien, les évolutions du djihadisme et de l'action publique mise en oeuvre pour l'endiguer en ont fait un sujet de mobilisation pour l'ensemble de la société civile, et notamment les entreprises qui se trouvent depuis peu confrontées à des défis inédits.

Depuis 2012, la France fait face à la résurgence d'une menace sécuritaire d'une intensité qui n'a que peu d'égal au regard de son histoire récente. Le djihadisme est désormais au coeur du débat public, notamment sous l'angle de ses modes opératoires et de ses cibles qu'il est nécessaire de cerner avec précision afin d'être en mesure de prévenir plus efficacement les attentats. Ceux-ci se multiplient pourtant depuis plus de quatre ans sans que rien ne puisse laisser envisager une accalmie, tandis que leurs caractéristiques compliquent toujours un peu plus la compréhension du phénomène. Le terrorisme perpétré au nom de l'islam dans l'Hexagone est-il le fait de groupes paramilitaires, organisés et missionnés par des émirs situés au Proche-Orient pour générer le plus grand nombre de victimes ? De « loups solitaires 1 » animés par une haine sacralisée des forces de sécurité, des juifs ou de toute autre cible de prédilection de la propagande djihadiste qui les inspire ? De déséquilibrés sévissant au hasard ?

Le débat occasionné par l'affaire Mérah sur les loups solitaires était significatif de la difficulté à caractériser cette menace, et si ce débat persiste, c'est parce-que de nouvelles affaires viennent ponctuellement étayer les tenants de ces diverses hypothèses, quand bien même elles demeurent contradictoires (1). Or, ce sont précisément son extrême malléabilité et son aspect diffus qui caractérisent le djihadisme contemporain en Europe et en Amérique du Nord, traversé par un phénomène d'individualisation encouragé par ses idéologues (2). Ces évolutions ont mis durablement en difficulté l'appareil régalien et justifié le développement de plans de prévention, dont le succès repose sur l'implication de divers services de l'État, de la société civile, et notamment des entreprises devenues l'un des points névralgiques de la lutte contre la radicalisation (3).

Du terrorisme organisé aux loups solitaires ?

En mars 2012, la France redécouvrait un « terrorisme intérieur » qui, plus de 15 ans après l'affaire Khaled Kelkal, augurait l'émergence d'une menace d'un genre nouveau. Mohammed Mérah assassinait sept personnes dans une série d'attentats revendiqués par le groupe *Jund al-khila ̄fa* (alors lié à Al-Qaïda), selon un mode opératoire qui laisse alors les autorités perplexes tant il semble éloigné, à première vue, du terrorisme organisé auquel Al-Qaïda avait

(1) Cette expression, appliquée au terrorisme après le 11 septembre 2001, désignait un individu, seul, qui après un brusque endoctrinement sur Internet, recourait à l'action violente.

Entre Amsterdam et Paris 21/08/2015

*Ayoub El Khazzani, armé d'un pistolet automatique et d'un fusil d'assaut kalachnikov, ouvre le feu sur les passagers d'un train Thalys avant d'être maîtrisé par des militaires américains en vacances. **Deux blessés***

(France) 14/11/2015

*Instauration de **l'état d'urgence***

2015

(France) 13/11/2015

Neuf terroristes ayant prêté allégeance à Daesh abattent des civils au Stade de France, au Bataclan, au bar Comptoir Voltaire dans le XI^e^ arrondissement, rue de la Fontaine au Roi et rues Bichat et Alibert. Leurs modes opératoires : fusillades et opérations kamikazes. 130 morts, 352 blessés

commencé à habituer l'Occident [Khosrokhavar, 2014]. Le procureur de la République de Paris, François Molins, évoquait une « auto-radicalisation salafiste atypique » sans rattachement à une organisation terroriste[2]. Le Directeur central du renseignement intérieur (DCRI) de l'époque, Bernard Squarcini, décrivait Mohammed Mérah comme un jeune s'étant auto-radicalisé en prison, agissant seul, et sans lien avec aucune organisation[3]. L'ancien juge antiterroriste, Jean-Louis Bruguière, pointait à son tour du doigt la difficulté d'identifier ces individus dont la radicalisation se déroule en partie sur le Net, sans s'inscrire dans des réseaux structurés et déjà connus, ou pour le moins repérables par les services de renseignement[4]. Certes, l'expression « loup solitaire » fut rapidement décriée (Mohammed Mérah lui-même était largement intégré dans des réseaux délinquants, criminels, salafis et terroristes). En effet, les enquêtes instruites à la suite des attaques à caractère terroriste, qui se sont multipliées depuis 2012, continuent d'établir le rôle déterminant que jouent les personnes physiques et les réseaux dans la préparation des attentats, et la majorité des condamnés pour terrorisme de type djihadiste l'est encore au visa de l'incrimination d'« association de malfaiteurs en lien avec une entreprise terroriste » (bien que plusieurs mises en examen aient été établies pour « entreprise individuelle terroriste » après la création de cette infraction en novembre 2014).

Certes, la brève controverse n'aura eu que peu de valeur en soi, si ce n'est qu'elle demeure révélatrice des difficultés à appréhender un phénomène que l'on voyait déjà poindre depuis quelques années en Europe. Bien que plusieurs observateurs aient rapidement établi que les loups étaient moins solitaires que l'opinion et les responsables politiques n'étaient un temps disposés à le croire [Pathé Duarte, 2013], le phénomène (mode opératoire relativement autonome et cibles hétérogènes) semblait apparemment se confirmer les mois et années suivants, à la faveur d'une série d'affaires : Alexandre Dhaussy en mai 2013, Bertrand « Bilal » Nzohabonayo en décembre 2014, Moussa Coulibaly en février 2015, Sid Ahmed Ghlam en avril 2015, le lycéen de Châlons-en-Champagne qui a été arrêté en octobre 2015 après avoir agressé l'une de ses enseignantes et qui a avoué avoir projeté d'attaquer une gendarmerie (le même mois, un jeune homme était arrêté pour avoir planifié une attaque contre la marine nationale à Toulon), Tarek Belgacem en janvier 2016, l'adolescent qui a agressé un enseignant juif à l'aide d'une machette à Marseille le 11 janvier 2016, Larossi Abballa à Magnanville le 13 juin 2016, Mohamed Lahouaiej Bouhel à Nice le 14 juillet 2016… Dans le même temps qu'un nombre grandissant de jeunes rejoignent la zone syro-irakienne, ceux qui en reviennent, ceux qui ne peuvent pas ou ne souhaitent pas partir tout en manifestant une sympathie pour les idéologies djihadistes, des individus qui entretiennent des liens très variables avec Al-Qaïda et/ou l'organisation État islamique (EI)[5] (de la seule admiration à la coordination), passent à l'acte sur le territoire français où ils s'en prennent aux cibles les plus diverses (militaires, forces de sécurité, juifs, enseignants, population en général, bien sûr les musulmans qui n'embrassent pas la même conception de l'islam) sur la base de modes opératoires largement individualisés.

Un infléchissement stratégique encouragé par les idéologues du djihad

Comment appréhender ce phénomène ? Il importe déjà de garder à l'esprit qu'il est encouragé par un infléchissement stratégique des idéologues du djihad. La lutte contre al-Qaïda et son affaiblissement après les attentats du 11 septembre 2001, ont en effet été favorables à un virage dans la direction que préconisaient des entrepreneurs du djihad dès les années 1990/2000 [Kepel, 2008 ; Lia, 2008 ; Stenersen, 2008]. Alors que les missions confiées à des groupes organisés sont plus souvent déjouées par les services de sécurité, l'enjeu est de susciter des vocations à l'international via les moyens modernes de communication, aussi bien pour rejoindre les théâtres de combats proche-orientaux que pour éveiller des loups solitaires au djihad dans les pays occidentaux. Abou Mohammed al-Adnani, le porte-parole de l'EI (qui aurait trouvé la mort à Alep en août 2016, selon l'agence de presse de l'EI, *A `ma¯q*) exhortait par exemple en 2014 : « *Si vous ne pouvez pas trouver d'engins explosifs ou de munitions, isolez l'Américain infidèle, le Français infidèle ou n'importe lequel de ses alliés. […] Écrasez-lui la tête à coups de pierre, tuez-le avec un couteau, renversez-le avec votre voiture, jetez-le dans le vide, étouffez-le ou empoisonnez-le* ». Les années 2010,

(2) http://www.lepoint.fr/societe/tueries-de-toulouse-et-de-montauban-le-raid-a-deja-tente-plusieurs-assauts-21-03-2012-1443661_23.php.

(3) http://www.lemonde.fr/societe/article/2012/03/23/toulouse-les-revelations-du-patron-du-renseignement_1674664_3224.html.

(4) http://www.lefigaro.fr/actualite-france/2012/03/21/01016-20120321ARTFIG00416-les-filieres-afghanes-ne-sont-pas-toutes-purgees.php.

(5) Ou « Daesh », acronyme de *Ad-dawla al-islāmiyya fī-l-`irāq wa ash-shām* (en français : l'État islamique en Irak et au Levant).

marquées par le développement concurrentiel du Jahbat an-Nos.ra et de l'EI, donnent en effet lieu à un regain d'efforts pour recruter des affidés dans les pays occidentaux et notamment en France, dont est significative la diffusion d'une propagande largement professionnalisée dans les langues des pays visés, et qui cherche à atteindre les jeunes en empruntant leurs codes. Al-Qaïda dans la Péninsule arabique (AQPA) édite sa revue anglophone depuis 2010 (au titre explicite : Inspire), et l'EI depuis 2014 (*Da¯biq*), à laquelle il faut ajouter depuis décembre 2014 une livraison francophone (*Da¯r al-Isla¯m*), puis une seconde en septembre 2016 (*Rumiyah*), ainsi que des vidéos régulièrement mises en ligne par leurs agences de communication et les terroristes à l'occasion de la commission de leurs crimes (Mohammed Mérah, Amedy Coulibaly, Larossi Abballa…). Ces contenus justifient la violence (avec parfois la désignation de cibles nominatives) et fournissent de véritables manuels qui rendent le crime accessible à tous[6], tout en incitant à la discrétion aussi bien sur le plan de la religiosité (renoncer à l'ostentation religieuse pour se fondre dans un style de vie plus anonyme, sur le mode de la *taqiyya*[7]) que sur le plan organisationnel (encourager des initiatives individuelles tout en fournissant éventuellement un soutien logistique plutôt que la mise en place de structures organisées mais aussi moins difficilement repérables). Cette propagande est tant relayée sur l'Internet (sites, blogs, réseaux sociaux) qu'elle a acquis une position prééminente sur le marché idéologique mondial.

Son efficacité profite encore d'un effort d'embrigadement déjà mis en oeuvre par le biais de réseaux virtuels. Al-Qaïda a très tôt investi les télécommunications et notamment le Web, a expérimenté les difficultés du site Internet, avant de s'orienter vers une communication directe avec les internautes (avec la mise en place de « foires à questions » par Ayman al-Zawahiri en 2007) et de généraliser sa présence sur les chats, les forums, les réseaux sociaux (notamment *Facebook* et *Twitter*[8]) dès la fin des années 2000 et les applications mobiles (*WhatsApp*, *Viber*, *Telegram*…), privilégiant ainsi une relation directe avec son public, à l'instar de l'EI à sa suite [Berger, 2014 ; Department of Homeland Security, 2010 ; Hecker, 2015]. Bien qu'ils soient sérieusement discutés, les travaux du Centre de Prévention, de Déradicalisation et de Suivi Individuel (CPDSI) ont néanmoins montré combien l'activité des recruteurs sur l'Internet pouvait relever d'un véritable harcèlement quotidien mis en oeuvre et ajusté à des profils présélectionnés, et qu'elle se doublait, dans bien des cas, de pressions physiques mettant en jeu des individus facilitant le passage à l'acte [Bouzar, Caupenne, 2014]. En définitive, les organisations djihadistes se veulent être les sources d'inspiration d'une menace diffuse (ce qui explique que les frères Kouachi et Amedy Coulibaly puissent mener une action coordonnée en France tout en en attribuant les bénéfices symboliques à deux organisations concurrentes, respectivement AQPA et l'EI), sachant maintenir une violence de basse intensité avec pour horizon l'établissement d'une guerre civile en Europe. À la controverse générée sur les loups solitaires à l'occasion de l'affaire Mérah était ainsi sous-jacente la perception d'un phénomène d'individualisation du djihad. Cela ne signifie pas que des individus gravitent seuls dans leurs processus de radicalisation pour commettre un attentat de façon complètement isolée. Cela renvoie à une autonomisation relative vis-à-vis des structures opérationnelles qui autorise une pluralité de modes opératoires et de cibles. Il peut s'agir aussi bien d'individus qui agissent relativement seuls pour se revendiquer finalement de tel ou tel groupe terroriste (Tarek Belgacem en janvier 2016…), d'individus qui bénéficient d'un soutien logistique léger mais déterminant (Sid Ahmed Ghlam en avril 2015…), que d'actions commanditées par le haut, coordonnées et ayant été précédées d'une préparation paramilitaire (attentats de janvier et de novembre 2015). L'individualisation du djihad se traduit par une pluralisation des modes de passage à l'acte qui sont, de ce fait, beaucoup plus diffus et imprévisibles.

Crise du paradigme répressif et développement de la lutte contre la radicalisation

Ces évolutions ont engendré une crise du paradigme répressif qui a pour corrélat le développement d'un faisceau complexe d'actions à caractère préventif : la lutte contre la radicalisation, qui suppose la mobilisation de la société civile.

Ces évolutions se sont en effet traduites, dès l'affaire Mérah,

(6) Comment manier des armes à feu, commettre des assassinats avec des moyens rudimentaires, incendier un véhicule, provoquer un accident, préparer une embuscade, fabriquer (et dissimuler) une bombe à partir de matériaux aisément procurables dans le commerce, rester discret (utilisation de logiciels d'encryptage et de décryptage tels Asrar al-Mujahideen…).

(7) Précaution, permise par la *shart`a*, qui consiste à dissimuler son appartenance pour se protéger, et qui, telle qu'elle est désormais enseignée dans les réseaux djihadistes, devient une habilité à tromper pour combattre son ennemi.

(8) La *Brookings Institution* recensait 46 000 comptes *Twitter* de djihadistes entre septembre et décembre 2014.

RAID BRI prise d'otages
à VINCENNES 2015mint0019_03

par une mise en cause des institutions de justice et de sécurité. Les rapports de Jean-Jacques Urvoas [Urvoas, 2012], Patrick Verchère [Urvaos et Verchère, 2013] et Christophe Cavard [Cavard et Urvoas, 2013] pointaient les difficultés des services de renseignement devenus l'une des cibles du débat public après l'affaire Mérah (le candidat à la présidence François Hollande s'était publiquement inquiété d'éventuelles failles des services de renseignement en mars 2012 [9], et les juges d'instruction avaient demandé la levée du secret défense le 6 juin 2012 afin de vérifier cette hypothèse). Tous les individus ne sont pas identifiés avant leur départ dans la zone syro-irakienne (en janvier 2014, seul un individu sur deux approximativement était identifié avant son départ) [10], et il est techniquement impossible de diligenter une enquête pour chaque personne censée présenter des signes de radicalisation qui, en outre, n'ont guère toujours de pertinence. Au niveau judiciaire ensuite, les qualifications juridiques existantes ne permettent pas toujours aux magistrats d'incriminer les comportements résultant de ces pratiques du djihad. L'incrimination d'« association de malfaiteurs en lien avec une entreprise terroriste », qui est le pilier juridique de la lutte anti-terroriste en France, n'est pas applicable à un individu seul, et la fluidité des réseaux terroristes complique leur identification (démontrer que des individus partagent des points de vue communs ne suffit pas à établir l'association de malfaiteurs qui requiert d'apporter la preuve de l'existence d'échanges opérationnels). Les magistrats font face à une profusion d'individus présentant des profils inquiétants sans toujours pouvoir faire l'objet d'un traitement judiciaire. Marc Trévidic [2012] déplorait déjà cette situation lorsqu'il était juge d'instruction au pôle anti-terrorisme du tribunal de grande instance de Paris.

La crise du paradigme répressif, apparue dans les années 1980 en matière de gestion de la délinquance [Roché, 2004], s'étend donc au champ de la lutte anti-terroriste, et elle se traduit de la même façon par le développement concourant d'un investissement dans la prévention. En est significative l'apparition d'un terme dans les discours des responsables politiques : Jean-Marc Ayrault (alors premier ministre) parle pour la première fois de radicalisation en octobre 2013 [Ragazzi, 2014], c'est-à-dire non pas du passage à l'acte lui-même, mais du processus qui le précède et sur lequel il conviendra alors d'agir. Le gouvernement prévoit en effet de prévenir la radicalisation dans le courant de l'année 2013 [Jounot, 2013], la décision est arrêtée en avril 2014 (plan d'action contre la radicalisation violente et les filières terroristes), et la mise en oeuvre d'une action

(9) http://www.lemonde.fr/societe/article/2012/03/22/questions-sur-la-surveillance-de-mohamed-merah-par-la-dcri_1674087_3224.html.

(10) Source : ministère de l'Intérieur.

CHRONOLOGIE

2016

Marseille (France) **11/01/2016**
Un adolescent turc agresse à la machette un enseignant juif. L'auteur dit avoir agi « au nom d'Allah » et de l'organisation État islamique. Un blessé.

(France) **09/03/2016**
Adoption de la loi sur la sécurité dans les transports, ou Loi Savary.

(France) **22/03/2016**
Adoption de la Loi n°2016-339 relative à la prévention et à la lutte contre les incivilités, contre les atteintes à la sécurité publique et contre les actes terroristes dans les transports collectifs de voyageurs.

Bruxelles (Belgique) **22/03/2016**
Série de trois attentats-suicide à la bombe, revendiqués par l'organisation terroriste État islamique : deux à l'aéroport de Bruxelles, à Zaventem, et le troisième à Bruxelles, dans une rame du métro. 32 morts, 340 blessés.

publique dédiée s'opère alors en deux temps. Le Plan de prévention de la radicalisation et d'accompagnement des familles voit le jour en avril 2014 (prévention secondaire). Il donne lieu à la création de dispositifs de détection, de signalement et de suivi (« déradicalisation ») des personnes suspectées de se radicaliser ainsi que d'accompagnement (psychologique notamment) de leurs familles. Après les attentats de janvier, diverses actions sont ensuite entreprises avec l'objectif de réduire les vulnérabilités sociales qui favoriseraient la radicalisation et de diffuser des contre-influences (prévention primaire) : lancement de la campagne « #Stop-djihadisme » sous l'égide du Service d'information du gouvernement, de la Grande mobilisation de l'École autour des valeurs de la République, mise en place du Comité interministériel « Égalité et citoyenneté », impulsion d'une dynamique dans le champ religieux (notamment *via* la création de l'Instance de dialogue avec le culte musulman), etc. Les évolutions des manifestations (modes opératoires et cibles) du djihadisme se traduisent par une mise en difficulté de l'appareil régalien en matière d'anti-terrorisme (dont les outils continuent néanmoins d'être renforcés sur les plans policiers et juridiques : réforme de la DCRI, Projet de loi sur le renseignement…) et, simultanément, par un investissement dans la prévention qui va constituer une nouvelle source d'interrogation pour les entreprises.

Conclusion

En effet, avec la prévention, l'État est partiellement dépossédé de la gouvernance de la sécurité qui s'appuie, dès lors, sur une hybridation inédite d'un ensemble d'acteurs issus de la société civile [Roché, 2004], au sein desquels les entreprises acquièrent une responsabilité nouvelle. Cette question est apparue avec force après les attentats du 13 novembre, lorsque l'opinion apprenait que l'un de ses auteurs, Samy Amimour, fut chauffeur de bus à la RATP avant de partir en Syrie en 2013. Les entreprises rencontrent en effet la radicalisation de maintes façons. Sur les 10 200 individus signalés comme radicalisés par l'Unité de coordination de la lutte anti-terroriste (Uclat) à l'été 2016 [11], nombre d'entre eux ont bien entendu un emploi (la RATP serait d'ailleurs particulièrement impactée [12]), et ils peuvent également user de leur matériel (outre le camion loué par Mohamed Lahouaiej-Bouhel, les grandes entreprises du Web sont par exemple directement concernées par la diffusion de la propagande djihadiste). Les entreprises sont encore touchées dans la mesure où elles peuvent constituer une cible de choix, tels les transports bien sûr (prise d'otage du vol Air France en 1994, attentat dans le RER B en 1995, tentative d'Ayoub El-Khazzani dans un train Thalys en août 2015…), mais encore les sites nucléaires, ceux classés Seveso (après avoir assassiné son employeur en juin 2015, Yassin Salhi a tenté de faire exploser l'usine *Air Products* de Saint-Quentin-Fallavier).

Les entreprises sont donc impactées certes, mais face au caractère nouveau de la menace et de la réponse qu'il appelle, elles acquièrent une responsabilité dans l'action publique mise en oeuvre pour tenter d'endiguer le phénomène (outre la sécurisation des sites et des employés qui relève de leurs obligations et qui se pose dorénavant avec une acuité particulière). Si elles ne sont guère concernées par la prévention primaire (qui en l'état relève du domaine de compétences de l'État, d'autres instances de socialisation ou de collectifs *ad hoc*), leur implication est croissante en matière de prévention secondaire. Quand bien même les services de l'État et les entreprises évitent souvent de rendre cette réalité publique (voir les polémiques qui ont touché la police, l'armée, la RATP, les zones aéroportuaires…), ils sont en leur sein confrontés à des comportements inquiétants, et à la difficulté de faire la part entre ce qui relève de la liberté d'expression religieuse, ce qui se règle par le dialogue voire des mesures disciplinaires, et ce qui peut légitimer une inquiétude crédible et devrait faire l'objet d'un signalement, tout en évitant les amalgames qui instillent un poison dangereux pour le lien social. Or, il n'existe pas, bien sûr, de réponse parfaite. D'où l'importance des campagnes de sensibilisation/formation, mais aussi l'intérêt à prendre attache avec le Centre national d'assistance et de prévention de la radicalisation (CNAPR- Uclat) qui sait évaluer la situation et conseiller l'attitude à adopter selon les circonstances.

Après le surgissement de la question de l'islam dans le monde du travail avec l'affaire Baby Loup en 2008, les évolutions récentes du djihadisme confrontent désormais les entreprises à la nécessité de dépasser le seul cadre d'une coopération renforcée avec les autorités, en ce sens qu'elles deviennent à leur tour l'un des points névralgiques d'une lutte qui engage l'ensemble de la société civile. ■

(11) Source : ministère de l'Intérieur.

(12) http://www.leparisien.fr/societe/inquietante-montee-religieuse-a-la-ratp-17-11-2015-5284579.php.

QUE PEUT L'ÉTAT ?

Entretiens avec...

- **Louis GAUTIER,** *Secrétaire général de la défense et de la sécurité nationale*
- **Thierry MATTA,** *Directeur général adjoint de la sécurité intérieure – DGSI*

Des mesures de soutien pour l'entreprise

- Le ministère de l'Économie et des Finances aux côtés des entreprises
  Christian DUFOUR, *HFDS adjoint, Ministère de l'Économie et des Finances*
- La cybersécurité, une priorité nationale et européenne
  Guillaume POUPARD, *Directeur général de l'ANSSI*
- Terrorisme, cybersécurité et modernisation
  Thierry DELVILLE, *Délégué ministériel aux industries de sécurité , Chargé de la lutte contre les cyber menaces*
- L'apport de l'Union européenne à la protection des infrastructures critiques
  Grégoire DEMEZON, *Chargé de mission, Cabinet du ministre de l'Intérieur et* **Franck PEINAUD,**
  Conseiller à la Délégation de l'Union européenne en Tunisie

Vers un accroissement des pouvoirs des acteurs privés de la sécurité ?

- *Interview de* **Patrice LATRON,** *Préfet, Directeur de Cabinet du Préfet de Paris Île-de-France*
- La sécurité privée dans la sécurité intérieure
  Cédric PAULIN, *Directeur de cabinet du CNAPS*
- Refonder la sécurité privée
  Claude TARLET, *Président de l'ANAPS*
- Une mobilisation irréversible des agents privés de sécurité contre la terreur, mais à quelles conditions ?
  Daniel WARFMAN, *Directeur délégué de Trigion Sécurité, Groupe Facilicom*
- La sécurité privée en chiffres - zone europe géographique, **LPN Group**
- Discours de **Bernard CAZENEUVE,** *Ministre de l'Intérieur – 4e Assises de la sécurité privée*

Entretien avec
LOUIS GAUTIER

Secrétaire général de la défense et de la sécurité nationale

Dans le contexte de crise de sécurité nationale que nous connaissons depuis janvier 2015, les périmètres d'activité des services de l'État en charge de la sécurité sont en pleine redéfinition. La place des armées sur le territoire national a aussi passablement évolué. Pouvez-vous nous donner une vision globale de ces évolutions ?

La crise que nous connaissons s'inscrit dans une évolution amorcée dès 2001 et qui s'est accélérée à partir de 2012 et de l'affaire Mérah. L'ancienne distinction entre sécurité intérieure et sécurité extérieure s'est progressivement brouillée au profit d'une problématique nouvelle, celle de la sécurité nationale. La menace terroriste est devenue plus fluide, se jouant des frontières et des appartenances. Elle s'est aussi faite plus brutale, privilégiant les attentats-suicides et les tueries de masse qui placent nos forces devant l'impératif d'une réaction rapide, anticipée et parfaitement coordonnée.

Face à des adversaires toujours enclins à se jouer des frontières géographiques, techniques ou morales, prévention, protection et intervention doivent donc être combinées au plus juste dans tous les domaines : aériens et terrestres – où nous sommes plus avancés –, mais aussi maritime – où d'importants efforts restent à mener. À l'opposé des anciennes logiques de partage des tâches entre départements ministériels et entre forces, l'heure est par ailleurs au décloisonnement. Il faut moins d'éparpillement des efforts et plus de concentration.

D'importantes dispositions ont été prises dans ce sens. Dans le domaine du renseignement, *la direction générale de la sécurité intérieure* (DGSI) a été désignée, en 2016, comme référent de tous les autres services dans la lutte antiterroriste sur le sol national. Le partage de l'information et des tâches opérationnelles avec la *direction générale de la sécurité extérieure* (DGSE), chargée de la détection et de l'entrave de la menace à l'étranger, résulte par ailleurs désormais d'une étroite synergie entre ces deux directions. S'agissant des forces de sécurité intérieure, une collaboration nouvelle a été établie entre les différentes unités (RAID, GIGN, BRI) et leur organisation géographique a été repensée afin de couvrir au plus près l'ensemble du territoire. Ces évolutions ont abouti à la présentation, le 19 avril 2016, d'un nouveau schéma national d'intervention des forces de sécurité qui les autorise en particulier, en situation de gravité extrême, à s'affranchir de leur zone habituelle de compétence territoriale.

Mais la mesure la plus visible de l'année 2015 fut sans aucun doute le déclenchement de l'opération *Sentinelle*. À la suite des attentats de *Charlie Hebdo*, le contrat opérationnel de protection des armées a été déclenché, entraînant le déploiement dans la durée de 8000 soldats en moyenne. Il n'y a pas là une révolution. La protection du territoire national a toujours constitué une mission des armées, à laquelle contribuent d'ailleurs quotidiennement la marine nationale pour la surveillance de nos côtes et l'armée de l'air pour le contrôle de notre espace aérien. Cette mission de protection avait néanmoins perdu de son ampleur depuis la fin de la guerre froide et la montée en puissance des interventions extérieures qui avait progressivement conduit la France à adopter un modèle d'armées de projection au risque d'être de plus en plus «hors-sol». Aujourd'hui, la sécurisation du théâtre national est redevenue un objectif dimensionnant pour nos militaires en termes de disponibilité et de moyens.

Ces multiples évolutions impliquent des adaptations de notre droit, récemment portées par différents textes législatifs, un important effort financier dont les dernières actualisations de la loi de programmation militaire ont notamment pris acte, une redéfinition de nos doctrines. Elles exigent également que soit conforté le contrôle démocratique exercé sur l'action des pouvoirs publics. C'est cette ambition qui a conduit, par exemple, à la création de la *commission nationale de contrôle des techniques de renseignement* (CNCTR) qui vient contrebalancer les moyens renforcés accordés aux « services » par les lois du 24 juillet et du 30 novembre 2015.

La protection à laquelle travaillent les pouvoirs publics est celle de nos concitoyens. Elle est également celle des installations critiques, et notamment des opérateurs d'importance vitale. Quelle est l'état de la politique menée en la matière ?

La protection des installations qui fournissent les services et les biens indispensables à la vie de la Nation constitue bien évidement une priorité pour les pouvoirs publics. Définie par l'ordonnance du 29 décembre 1958, une politique existe de longue date en la matière. Au début des années 2000, ses orientations, non révisées, avaient néanmoins perdu de leur pertinence en raison de la disparition de la menace soviétique et du renforcement de la menace terroriste. Une redéfinition de la nature et du nombre de cibles à défendre était donc devenue indispensable. Au début des années quatre-vingt-dix, près de 7000 sites figuraient alors au catalogue des installations à protéger.

L'actualisation du dispositif a conduit, dès 2005, à l'adoption de deux modifications importantes, l'obligation de prendre en compte « *toute menace, notamment à caractère terroriste* » et le remplacement de la notion d'entreprise par celle d'« opérateur », plus large, puisqu'elle englobe à la fois les acteurs publics et privés. En un demi-siècle, nous sommes effectivement passés d'une économie marquée par une forte présence étatique à une logique de privatisation qui a placé les entreprises privées au cœur des activités d'importance vitale. Un an plus tard, le décret du 23 février 2006 complétait ce travail de réforme en établissant le dispositif de *sécurité des activités d'importance vitale* (SAIV).

Ce dispositif qui repose sur des bases juridiques solides, le code de la défense, se veut pragmatique en tenant compte des réalités économiques des entreprises. Face à une menace ancrée dans la durée, l'objectif est de parvenir à un équilibre entre le coût des mesures et les besoins de protection. Aujourd'hui, 249 *opérateurs d'importance vitale* (OIV) répartis dans douze secteurs d'activité sont ainsi responsables de 1358 *points d'importance vitale* (PIV). Placés au centre du dispositif SAIV, ces OIV disposent d'un statut particulier, et ce, à plusieurs titres. La désignation d'un *délégué à la défense et à la sécurité* (DDS) leur permet de bénéficier d'un accès privilégié aux décisions prises par les pouvoirs publics, en particulier en matière de posture VIGIPIRATE. La procédure, dite de « criblage », leur offre la possibilité de demander à l'autorité administrative de vérifier que les caractéristiques de la personne souhaitant accéder à un de leurs PIV ne sont pas incompatibles avec la sécurité du site concerné. Le *plan de protection externe* (PPE), élaboré sous l'autorité du préfet de département, complète enfin le dispositif de protection de leur PIV en planifiant les capacités humaines et matérielles que l'État peut déployer en cas de besoin ainsi qu'en prévoyant les mesures de surveillance des zones périphériques.

Le dispositif SAIV a ainsi permis d'élever le niveau de sécurité dans les secteurs d'activité d'importance vitale, non seulement par les mesures de protection mises en œuvre, mais aussi par une élévation de la culture de la sécurité favorisée par la prise de conscience des menaces et des vulnérabilités. Aujourd'hui, nous pouvons nous féliciter de l'existence d'un cercle d'opérateurs de confiance, conscients de leurs responsabilités au titre de la stratégie de sécurité nationale et capables de se mobiliser en cas de crise.

Vous évoquiez la question du criblage. Aujourd'hui, les entreprises souhaitent pouvoir mieux répondre face à des comportements à risques. Le SGDSN mène une réflexion sur les demandes d'enquêtes administratives dont peuvent faire l'objet les salariés ou futurs salariés. Qu'en est-il de ce procédé désigné par « criblage administratif » ?

Le criblage désigne une opération de consultation d'un fichier nominatif de souveraineté (police, justice ou renseignement) réalisée dans le cadre de procédures administratives aujourd'hui prévues par plusieurs dispositions législatives du code de la sécurité intérieure et du code de la défense, destinées à vérifier la compatibilité du comportement de personnes physiques (ou morales) avec l'accès à un lieu, une information ou l'exercice d'un emploi.

Jusqu'au début de l'année 2016, le criblage précédait nécessairement une décision administrative relative à l'accès à certaines zones, en particulier les sites d'importance vitale, les zones de sûreté des aérodromes et des ports et les zones intéressant la défense nationale. Il précédait également l'exercice de certaines fonctions, notamment les emplois publics

participant à l'exercice des missions de souveraineté de l'État et les emplois publics ou privés relevant du domaine de la sécurité ou de la défense.

La loi dite SAVARY du 22 mars 2016 a étendu la possibilité de recourir au criblage pour les emplois en lien direct avec la sécurité des personnes et des biens au sein d'une entreprise de transport public de passagers ou de transport de marchandises dangereuses. Le criblage a également été rendu possible par la loi dite URVOAS du 3 juin 2016 pour contrôler l'accès aux grands événements des personnes qui ne sont ni spectateurs, ni participants.

Les décisions prises à l'issue de ces procédures peuvent revêtir d'importantes conséquences. Dans le domaine des transports, ce sont ainsi 185000 personnes qui sont potentiellement concernées par ce nouveau dispositif. Elles posent plusieurs questions, à commencer par la valeur de l'avis formulé par l'administration et les modalités de sa contestation. Dans la mesure où il revient ultimement à l'opérateur de décider d'un éventuel licenciement, quel fondement juridique donner par ailleurs à sa décision ? Ces questions ont été prises en compte par le décret d'application rédigé par le ministère de l'Intérieur, qui est actuellement en cours d'examen au Conseil d'État.

L'extension de la procédure de criblage à d'autres secteurs d'activité et à d'autres emplois que ceux visés pour le secteur nucléaire ou le secteur du transport, est envisagé. L'attentat commis le 26 juin 2015 dans une usine de production de gaz de Saint-Quentin-Fallavier a notamment souligné toute l'importance de la protection des sites industriels sensibles ou sites SEVESO. Il convient dès lors d'identifier les secteurs et les conditions dans lesquels le criblage pourrait être étendu, de clarifier les conséquences juridiques des décisions administratives individuelles et des employeurs privés et, enfin, de repenser préalablement l'organisation administrative du criblage afin de lui permettre de répondre à un nouvel afflux de demandes.

Le secrétariat général de la défense et de la sécurité nationale est fortement mobilisé sur ce dossier délicat afin de faire du criblage un outil efficace de réponse à des menaces précisément identifiées dans un cadre juridique solide qui se doit de préserver les libertés individuelles.

La protection des principaux acteurs économiques de notre pays constitue un enjeu pour les pouvoirs publics, mais les entreprises sont également appelées à jouer un rôle dans la lutte contre le terrorisme, en particulier celles qui travaillent dans le domaine de la sécurité. Que pouvez-vous nous dire à ce sujet ?

Face à des menaces nouvelles, comme par exemple les drones malveillants, et pour assurer dans le temps la soutenabilité financière de notre politique de sécurité, nous avons besoin de solutions innovantes qui reposent sur le développement au meilleur coût et dans des délais restreints de solutions technologiques capables de compléter la vigilance humaine ou d'y suppléer.

Avec plus de 300000 emplois et un chiffre d'affaires de 30 milliards en 2013, le secteur français de la sécurité est bien positionné pour répondre à ce besoin. Toutes les conditions ne sont cependant pas encore réunies pour amener les technologies nécessaires à maturité et les développer à des coûts satisfaisants.

C'est pour relever ce défi que le comité de la filière industrielle de sécurité (CoFIS), qui associe pouvoirs publics et acteurs privés, a été fondé avec une double ambition. Soutenir, d'une part, l'industrie nationale sur un marché porteur où la France est très bien positionnée – elle compte plusieurs leaders mondiaux –, mais où elle est soumise à une très vive concurrence. Garantir, d'autre part, aux forces de sécurité et aux opérateurs d'importance vitale (OIV) le libre accès, au meilleur coût, à des solutions de sécurité adaptées et fiables.

Depuis janvier 2014, des groupes de travail ont ainsi été constitués, une étude du marché national de la sécurité a permis de mieux connaître son poids économique et ses acteurs, des actions concrètes et coordonnées en matière de promotion de la filière ont été menées à l'échelle européenne et internationale et une première expression de besoin mutualisé a pu être produite.

Il s'agit, dorénavant, de consolider ces acquis et, pour la filière, de construire collectivement les bases d'une politique industrielle de sécurité au service de tous ses acteurs. Dans ce but, une nouvelle feuille de route de la filière a été validée le 1er décembre 2015 à l'occasion du comité directeur du CoFIS présidé par le ministre de l'Intérieur et le ministre de l'Industrie. La sécurité a par ailleurs été prise en compte dans le second volet du programme d'investissement d'avenir (PIA) qui vient d'être lancé. Cela nous permettra de lancer cinq nouveaux démonstrateurs sur la ville intelligente et sécurisée, l'identité numérique, la sécurisation des lieux publics dans les transports intermodaux, la cybersécurité des systèmes industriels et la protection des sites SEVESO contre les actions malveillantes.

Il existe ainsi une dynamique particulièrement porteuse dans ce domaine dont témoigne, au demeurant, le vif succès rencontré par les premières assises des industries de sécurité qui se sont tenues le 20 septembre 2016 à Paris. ■

Entretien avec
THIERRY MATTA

Directeur général adjoint de la sécurité intérieure

Quelle est votre analyse de l'évolution de la menace terroriste ? L'État, la société civile et les entreprises sont-elles préparées à répondre à ces nouveaux modes opératoires ?

La France demeure l'un des pays les plus menacés du monde occidental, notamment du fait de Daech qui a commandité et inspiré plusieurs attentats sur le territoire national, qui ont fait 238 morts. Pour rappel, l'un des numéros de la revue francophone de Daech Dar al Islam titrait en Une « Qu'Allah maudisse la France ». De leur côté, Al-Qaïda au Magreb islamique (AQMI), en tant qu'organisation héritière du groupe islamique armé (GIA) des années 1990, considère toujours la France comme l'ennemi numéro un et Al-Qaïda dans la péninsule arabique (AQPA) nous stigmatise de la même façon. Par conséquent, la menace est aujourd'hui particulièrement forte.

Depuis les premiers attentats en 2015, l'État s'appuie sur une étroite coopération internationale et a déployé d'importants moyens humains, juridiques et techniques afin de répondre efficacement à ce péril. La prolongation de l'état d'urgence, l'élévation du plan Vigipirate au niveau alerte attentat, le dispositif militaire sentinelle, le renfort et le redéploiement des effectifs de police, notamment dans le renseignement, participent à la stratégie globale de lutte contre la menace terroriste. Aussi, de nombreux dispositifs de prévention et de détection de la radicalisation ont été mis en place, comme, par exemple, la plateforme d'appels du centre national d'assistance et de prévention de la radicalisation (CNAPR).

Enfin, les entreprises ont pleinement conscience des nouveaux enjeux sécuritaires et s'adaptent à ce nouveau contexte de menace terroriste en repensant leurs dispositifs de sûreté et la prise en compte du fait religieux dans leur société. Elles bénéficient à ce titre d'un accompagnement des services de la DGSI.

Au cœur du dispositif de lutte anti-terroriste, quelle est la spécificité de l'action de la DGSI et la nature de ses coopérations avec les autres services impliqués dans la lutte ?

Succédant à la Direction centrale du renseignement intérieur (DCRI) depuis le 12 mai 2014, la DGSI a vu ses missions et son organisation fixées par le décret du 30 avril 2014, lequel la charge, sur l'ensemble du territoire de la République, de rechercher, centraliser, exploiter le renseignement intéressant la sécurité nationale ou les intérêts fondamentaux de la Nation. Dans un contexte où la menace terroriste est aujourd'hui une priorité nationale, la DGSI concourt à la prévention et à la répression des actes de terrorisme ou portant atteinte à la sûreté de l'État, à l'intégrité du territoire ou à la permanence des institutions de la République.

En matière de lutte antiterroriste, tandis que le Service Central du Renseignement Territorial (SCRT) suit les

CHRONOLOGIE

(Allemagne) 22/07/2016
*Un réfugié syrien, débouté de sa demande d'asile, se fait exploser dans le centre d'**Ansbach** à proximité d'un festival de musique en plein air. 15 blessés. Le lendemain, on apprend que l'auteur avait « **fait allégeance** » au groupe Etat islamique.*

Saint-Etienne du Rouvray (France) 26/07/2016
***Prise d'otage dans une église.** Les deux assaillants, ayant prêté allégeance à Daesh, égorgent le prêtre et blessent trois personnes.*

2016

Fort Myers (Floride - USA) 25/07/2016
Fusillade dans une boîte de nuit. 2 morts. 17 blessés.

(Belgique) 06/08/2016
***Deux policières sont blessées à la machette** par un homme « criant Allah akbar ».*

FIN

individus radicalisés ou en voie de radicalisation, les individus suspectés de préparer des actes terroristes ou de partir en zone syro-irakienne relèvent du périmètre de la DGSI. Les objectifs prioritaires sont les filières syriennes, les dossiers signalés par les services partenaires ainsi que l'environnement et la surveillance d'objectifs potentiellement violents de la mouvance dite endogène. Si l'islam radical alimente ainsi majoritairement la menace terroriste, celle-ci peut également provenir d'autres mouvances (ultra droite, ultra gauche et séparatismes). Rappelons également qu'en matière judiciaire, la DGSI œuvre en coordination et/ou cosaisine avec les services de police judiciaire compétents (Direction centrale de la police judiciaire-Sous-direction antiterroriste/DCPJ-SDAT, Direction de la police judiciaire de la préfecture de police-Section antiterroriste/PJPP-SAT).

La DGSI suit plusieurs milliers d'objectifs répertoriés par le fichier des signalements pour la prévention de la radicalisation à caractère terroriste, en coopération étroite avec le SCRT notamment, dans le cadre d'un processus clairement établi (signalements, évaluations et traitements dans le cadre des états-majors de sécurité (EMS) départementaux placés sous l'autorité des préfets). L'action du service en matière de lutte antiterrorisme repose sur les trois composantes cardinales que sont l'anticipation, l'entrave et la neutralisation :

- L'action de renseignement est essentielle. Elle repose sur la mobilisation des capteurs humains et techniques, des moyens de surveillance de l'internet notamment, et des coopérations nationales et internationales. La Loi renseignement de juillet 2015 permet et encadre un certain nombre d'opérations techniques dans le domaine de la lutte anti-terroriste.

- Une action d'entrave administrative qui permet aux services de solliciter la mise en œuvre d'un éventail assez large de mesures : interdiction du territoire (entrée et sortie), retrait et refus de délivrance de passeports, gel des avoirs, blocage de sites internet, dissolution d'associations, expulsions d'étrangers du territoire national.

- Une action judiciaire essentielle de démantèlement des réseaux et de neutralisation des projets d'attentats. De nombreux projets d'attentats sur le territoire national ont été déjoués depuis 2013. Plus de 200 mesures de garde à vue ont été prises depuis le début de l'année 2016, et plus de 300 dossiers judiciaires sont en cours qui concernent plus d'un millier d'individus, ce qui permet de déjouer régulièrement des actions terroristes. Le choix du parquet de Paris de criminaliser l'incrimination d'association de malfaiteurs en lien avec un projet terroriste dès lors que des vies humaines étaient en jeu ou que des substances explosives étaient susceptibles d'être utilisées, contribue à accroître l'effectivité et l'efficacité des sanctions.

La coopération avec les services partenaires s'avère fondamentale en matière de lutte anti-terroriste. Ainsi, rappelons qu'en réponse à un impératif opérationnel, le décret n° 2015-1807 du 28 décembre 2015, consécutif à la loi n°2015-912 du 24 juillet 2015 relative au renseignement, a ouvert l'accès au traitement d'antécédents judiciaires aux agents des services de renseignement. Avec la DGSE, la coopération est complémentaire et s'effectue tant sur le plan opérationnel que technique.

? Quelle est la nature de votre coopération avec les entreprises et quel accompagnement concret pouvez-vous leur apporter?

Dans le cadre de sa mission de sécurité économique, la DGSI est un interlocuteur privilégié des directeurs de sécurité et de sûreté des entreprises. Le dialogue porte sur la détection, l'évaluation et l'analyse des menaces auxquelles sont confrontées les sociétés, au premier rang desquelles les ingérences économiques émanant d'acteurs étrangers, les cybermenaces et les phénomènes de radicalisation préparatoire à une action terroriste.

Bien que des événements plus anciens aient déjà alerté sur le caractère prégnant de la menace, les événements de Saint-Quentin-Fallavier (Isère) du 26 juin 2015 ont mis en exergue l'exposition de l'entreprise au terrorisme islamique sur le territoire national. Les risques encourus par l'entreprise sont protéiformes et multiscalaires :

– Le risque exogène porte sur les éléments relatifs à une menace terroriste étrangère à l'entreprise.

– Le risque endogène concerne les menaces provenant du personnel interne à l'entreprise (salariés mais aussi stagiaires, intérimaires…). Il s'agit des individus en mesure d'agir plus facilement au cœur de l'entreprise, compte tenu de leurs facilités de circulation dans les bâtiments.

– Le risque voyage concerne les expositions liées aux trajets quotidiens domicile-bureau tout comme celles des missionnaires (déplacement de délégation, mission ponctuelle, participation à un salon professionnel…), et des expatriés.

Dans ce domaine, l'accompagnement de la DGSI porte notamment sur une analyse de la menace, un dialogue sur les mesures à prendre en interne et une offre de sensibilisation spécifique des cadres ou des comités exécutifs. La DGSI reçoit ainsi un certain nombre de signalements et/ou est interrogée sur des individus suspectés de radicalisation, voire de velléités de passage à l'acte, qui font l'objet d'un traitement pouvant conduire à terme à l'ouverture d'une enquête judiciaire. Déjà perceptible depuis plusieurs mois, ce phénomène s'est amplifié suite aux attentats de janvier 2015 et celui de Saint-Quentin-Fallavier et, plus encore, depuis les évènements du 13 novembre 2015.

? Le décret du 28 mai 2010 interdit toute transmission des Fiches « S » aux maires comme aux employeurs en dehors des officiers de police, des militaires et des autorités judiciaires… Quelles solutions

sont envisageables pour satisfaire cette attente des entreprises et des collectivités locales ?

Les fiches «S» concernent les personnes qui peuvent, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'État et à la sécurité publique par, entre autres, le recours ou le soutien actif apporté à la violence, ainsi que celles entretenant ou ayant entretenu des relations avec de telles personnes. Je rappelle qu'une fiche «S» est un moyen d'enquête, un indicateur parmi d'autres, permettant d'évaluer le potentiel et la personnalité d'un individu donné. Ainsi, les différentes catégories de fiches S renvoient à la conduite à adopter lors d'un contrôle et en aucun cas à un degré de dangerosité. Elles excèdent largement la matière terroriste et les porter à la connaissance du plus grand nombre aboutirait à réduire leur efficacité.

Il semble important de rappeler que les entreprises peuvent signaler tout processus de radicalisation d'un individu à leurs correspondants habituels du SCRT ou également via le Centre National d'Assistance et de Prévention de la Radicalisation (CNAPR) et alerter les services de l'État compétents, et notamment la DGSI, en cas de risque de passage à l'action terroriste. ■

POUR ALLER PLUS LOIN

Garde nationale

Conformément à l'annonce faite par le Président de la République, le 28 juillet 2016, le ministre de la Défense et le ministre de l'Intérieur ont présenté un projet de décret créant une garde nationale destinée à concourir, le cas échéant par la force des armes, à la défense de la patrie et à la sécurité de la population et du territoire.

Lire la suite :

http://www.gouvernement.fr/conseil-des-ministres/2016-10-12/garde-nationale

COM TN

Expert du milieu territoire national, le COM TN, crée en juin 2016, assure l'engagement optimal, cohérent et performant des forces terrestres aux côtés des forces de sécurité intérieures et civiles. Force d'appui agissant au profit des unités et organismes de l'armée de Terre impliqués sur les sujets de sécurité sur le territoire national, son rôle d'anticipation et de conseil stratégique sera déterminant pour faire face aux défis futurs. Doté d'une composante opérationnelle, il pourra aussi renforcer dans l'urgence, en cas de crise majeure, les états-majors interarmés chargés de conduire et de contrôler les opérations sur le TN.

Pour en savoir plus :

http://www.defense.gouv.fr/terre/actu-terre/creation-du-com-tn-federer-les-forces

LE MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES AUX CÔTÉS DES ENTREPRISES

Christian DUFOUR
Haut fonctionnaire de défense et de sécurité adjoint,
Ministère de l'Économie et des Finances

L'économie repose sur des échanges qui ne peuvent fonctionner sans confiance. Face au développement de nouvelles formes de malveillance et de terrorisme, l'État a développé un ensemble de politiques publiques tournées vers le secteur concurrentiel, visant à maintenir ou rétablir rapidement cette confiance, gage de la résilience de la Nation en cas de crise.

Pour illustrer l'engagement du ministère de l'Économie et des Finances, en particulier à l'occasion des récents attentats, seront abordées successivement les relations avec des entreprises spécifiques, porteuses de « risques critiques », puis, de manière plus globale, la réponse possible à l'ensemble des entreprises d'un secteur, d'une zone d'activité, voire à l'échelon national lors d'événements mettant en jeu leur survie ou la continuité de leur activité.

L'accompagnement des entreprises critiques

Le dispositif de sécurité des activités d'importance vitale (SAIV), défini autour de douze secteurs d'activité[1], et coordonné par le Secrétariat général de la défense et de la sécurité nationale (SGDSN), s'attache à la protection et à la résilience des installations qui contribuent, de façon essentielle, à la préservation du potentiel de guerre et économique, de la sécurité et de la capacité de survie de la Nation.

La responsabilité de chacun de ces secteurs relève d'un ministre coordonnateur, chargé d'élaborer une directive nationale de sécurité (DNS) et de veiller à la mise en œuvre du dispositif dans un dialogue permanent avec les entités concernées.

À lui seul, le ministre de l'Économie et des Finances (MEF) est responsable de trois secteurs d'activités d'importance vitale : finances ; industrie ; communications électroniques - Internet-audiovisuel et information. Ceux-ci sont constitués d'entreprises et de services de l'administration, tous qualifiés alors d'« opérateur d'importance vitale » (OIV), leurs installations les plus sensibles étant désignées « points d'importance vitale » (PIV).

Le dispositif SAIV repose sur un travail collaboratif entre l'État et les entreprises. Il a succédé, depuis une dizaine d'années, à la réglementation dite des « points sensibles ». L'ensemble des dispositions est couvert par le secret de la défense nationale. Ces impératifs de confidentialité

(1) Les douze secteurs de la SAIV – ***Secteurs étatiques*** : activités civiles de l'État ; activités militaires de l'État ; activités judiciaires ; espace et recherche. ***Secteurs de la protection des citoyens*** : santé ; gestion de l'eau ; alimentation. ***Secteurs de la vie économique et sociale de la nation*** : énergie ; communications électroniques, audiovisuel et information ; transports ; finances ; industrie.

expliquent le peu d'information publique disponible, malgré l'important travail qu'il recouvre pour les différents acteurs.

Les règles fixées par le ministre coordonnateur sont définies en concertation avec les OIV eux-mêmes, placés dans une relation partenariale. Car l'entreprise, qui dispose d'un savoir-faire reconnu, parfois internationalement, connaît et mesure les enjeux stratégiques de la sécurité. C'est elle qui fait face régulièrement aux menaces et à leur évolution. Il est donc important qu'elle puisse apporter son expérience en complément de l'expertise des pouvoirs publics.

Enfin, cette concertation permet aussi d'appréhender de façon pragmatique les enjeux financiers soulevés en matière de sécurité. Un point d'équilibre entre le développement de la valeur ajoutée et celui de la sécurité peut ainsi être trouvé. Un équilibre pour lequel des méthodes d'analyse de risques sont indispensables, afin que le coût des mesures de protection ne soit pas, ou ne devienne pas, insupportable. Les mesures de sécurité sont ainsi passées au crible d'une série de scénarios, que les OIV doivent prendre en compte pour maintenir leur capacité de résilience, et celle de la Nation tout entière.

La SAIV est confiée, à l'échelon central des ministères, aux Hauts fonctionnaires de défense et de sécurité (HFDS). Ainsi, quotidiennement, le service du Haut fonctionnaire de défense et de sécurité (SHFDS) de Bercy travaille avec une quarantaine d'OIV, sur les 250 désignés pour l'ensemble des secteurs d'activités.

Les récents attentats ont pu montrer que des vagues de cyber-attaques, ciblant entreprises et administrations, pouvaient accompagner la perpétration d'actes terroristes. Les services de l'État doivent donc s'attacher à travailler ensemble à la coordination des réponses, en vue d'une prise en compte globale de la sécurité, c'est-à-dire tournée tant vers la sécurité physique, que cybernétique, développant des dispositifs de continuité d'activité et de résilience économique.

La révision récente de l'ensemble des DNS a permis de mieux prendre en compte certains risques en développement, dont le risque cybernétique. Ainsi, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dépendante du SGDSN, a confirmé son rôle d'acteur incontournable dans le domaine de la cybersécurité, en s'attachant à définir à cette occasion des règles spécifiques aux différents secteurs d'activité, en concertation avec les ministères coordonnateurs et toujours, bien entendu, les OIV eux-mêmes.

Le SHFDS de Bercy, par l'intermédiaire de son département dédié à la sécurité des systèmes d'information (DSSI), apporte ainsi désormais aux OIV, comme à d'autres entités sous tutelle du MEF, un soutien dans l'accompagnement en matière de cybersécurité. Il se prête à des séances de sensibilisation sur la sécurisation des données et des systèmes, pratique des « audits à blanc », ou encore, aide à l'appropriation de guides de bonnes pratiques.

Ces travaux s'inscrivent dans la démarche d'établissement d'un environnement de confiance large, initiée par l'ANSSI à travers différentes réglementations (référentiel général de sécurité (RGS), politique de sécurité des systèmes d'information de l'État (PSSI-E)). Le MEF réalise ainsi des guides et standards de sécurité qui précisent les mesures de protection nécessaires à chaque type de système d'information, et fournissent la démarche pour l'homologation des systèmes d'information, en permettant de prendre en compte les enjeux métiers et l'état de l'art des technologies utilisées. Les thématiques de la sécurisation des courriels, des applications web ou des postes de travail ont ainsi déjà fait l'objet d'une analyse documentée.

Le dispositif de continuité des activités économiques mobilisé suite aux attentats du 13 novembre 2015

Les attentats qui ont frappé Paris et Saint-Denis le 13 novembre 2015 revêtent une ampleur exceptionnelle au regard de leurs impacts immédiats et de plus long terme.

Cette crise majeure[2], avec une menace terroriste durable et à son plus haut niveau, a aussi affecté simultanément plusieurs secteurs d'activité économiques, en particulier ceux du commerce, du tourisme, de l'événementiel et des loisirs. Les pouvoirs publics ont alors mis en œuvre une véritable démarche de résilience nationale, comportant des mesures touchant aussi bien à la protection de la population et du territoire, qu'au maintien du fonctionnement de l'État et de la continuité de la vie de la Nation.

Ces attentats ont suscité une réponse immédiate, en particulier des services d'urgence et de sécurité (police, gendarmerie, sécurité civile, douanes), fortement appuyés par les moyens de la Défense. Mais, face à une crise de cette ampleur, c'est l'ensemble des politiques publiques qui concourt à assurer la sécurité nationale. Cette « réunion » se manifeste en particulier au sein de la cellule interministérielle de crise (CIC), convoquée sans délai par le Premier ministre, pour coordonner l'action des services de l'État, et ce, aussi longtemps que nécessaire.

Responsable de la préparation et de l'exécution de la politique de sécurité économique, le ministre de l'Économie est chargé d'assurer la protection des intérêts économiques de la Nation. Dans ce cadre, il est de sa responsabilité de

(2) Au sens de la circulaire du Premier ministre n°5567 du 2 janvier 2012 relative à l'organisation gouvernementale pour la gestion des crises majeures.

déterminer les mesures permettant de garantir la continuité de l'activité économique du pays. Au-delà de la protection des infrastructures critiques et de la sécurité des activités d'importance vitale, déjà évoquées, son action vise plus globalement à préserver la capacité de production de la Nation en organisant sa résilience économique.

Bien entendu, cette responsabilité ne peut valablement s'exercer qu'à la condition qu'État et acteurs du secteur privé soient en mesure d'échanger et de coopérer pour élaborer, dans un contexte d'urgence, une analyse commune de la situation et de ses conséquences, et des mesures pour en pallier les effets.

C'est ainsi qu'au regard de la gravité de la situation, le ministre de l'Économie a décidé de réunir la cellule de continuité économique (CCE), dont le secrétariat est assuré par le SHFDS. Cet organe, non permanent, et à la composition adaptable, constitue la clé de voûte du dispositif de gestion de crise du MEF qui s'intègre lui-même dans la gestion interministérielle de crise. La CCE réunit directions et services d'administration centrale concernés (y compris d'autres ministères) et représentants des secteurs d'activité les plus affectés par la crise. Elle constitue une enceinte «sur mesures» d'échange et de réflexion qui, à un rythme soutenu, élabore un diagnostic économique sur les plans macroéconomique, sectoriel et géographique.

Les fédérations professionnelles ont, d'emblée, exprimé le besoin d'informations sur la situation, les perspectives d'évolution, et sur l'action envisagée des services de l'État. En réponse, les pouvoirs publics ont pu fournir régulièrement des éléments d'information aux représentants professionnels, permettant à leurs adhérents de mieux analyser la situation, d'anticiper les conséquences et d'être informés des mesures sectorielles d'urgence prises par le Gouvernement.

À cette occasion, la CCE a pu proposer au ministre la réalisation d'un guide pratique destiné aux entreprises les plus impactées, qui regroupait l'ensemble des mesures prises (activité partielle temporaire, étalement d'échéances fiscales et sociales, crédits de trésorerie, délais de remboursement, mobilisation de fonds exceptionnels sectoriels) et précisait les procédures à suivre dans une logique de guichets uniques (n° d'appel unique) mis en place au niveau de chaque département.

Ces événements ont, en outre, amené le ministre de l'Économie à décider de la mise en œuvre d'une feuille de route pour le renforcement du dispositif de sécurité et de continuité des activités économiques, afin d'en accroître la réactivité et l'efficacité. Il est, en effet, nécessaire d'intégrer le fait que la gestion de crise, dans le domaine de la sécurité économique, se distingue d'autres domaines de la sécurité nationale par une temporalité singulière : les conséquences économiques doivent être anticipées d'emblée et gérées dans la durée.

En 2016, ce dispositif a de nouveau été mobilisé après l'attentat terroriste du 14 juillet à Nice. Il a été également activé pour faire face aux conséquences des crues, intervenues en mai et juin 2016, dont les effets s'étaient cumulés avec ceux de mouvements sociaux, le tout à une période où l'impact des attentats de novembre 2015 était encore perceptible. ■

POUR ALLER PLUS LOIN

CELLULE INTERMINISTÉRIELLE DE CRISE (CIC)

Trois cellules, décision, situation, communication, forment le Centre interministériel de crise. Placé sous l'autorité du ministre de l'Intérieur, il est l'outil de gestion interministérielle des crises et coordonne ainsi l'ensemble des centres opérationnels.

CELLULE DE CONTINUITÉ ÉCONOMIQUE (CCE)

La cellule de continuité économique est activée par le ministre de l'économie lorsque l'impact économique d'une crise est susceptible d'être important. Elle est en relation avec le ministre de l'économie et des finances et la Cellule interministérielle de crise à qui elle transmet les informations et expertises nécessaires au pilotage en temps réel de la situation économique et à la prise de décisions.

TERRORISME ET ENTREPRISE

Service de l'information stratégique et de la sécurité économiques – SISSE

Institué par le décret n°2016-66, en date du 29 janvier 2016, le Commissaire à l'information stratégique et à la sécurité économiques (CISSE) conduit la politique publique en matière de protection et de promotion des intérêts économiques, industriels et scientifiques de la Nation, en lien avec les ministères concernés. Il s'appuie pour cela, sur un service à compétence nationale, le SISSE (Service de l'information stratégique et de la sécurité économiques), rattaché au Directeur général des entreprises du ministère de l'Économie et des Finances. Le SISSE dispose d'un réseau régional de délégués, placé au sein des DIRECCTE[1].

Dans le cadre de ses attributions, le SISSE recense, en lien avec la communauté du renseignement, les différentes menaces affectant le tissu économique, scientifique et industriel. La menace terroriste s'inscrit bien évidemment dans ce spectre et doit donc être prise en compte par tous les acteurs économiques dans une approche de sécurité économique globale.

Hors secteurs spécifiques ou activités d'importance vitale, qui sont soumis à un risque terroriste spécifique et avéré, les entreprises françaises ne constituent pas directement, à ce jour des cibles de premier rang pour le terrorisme. Pour autant, indirectement, ce terrorisme profite, et le cas échéant exploite, des failles de sécurité présentes dans les entreprises.

La cybercriminalité en particulier, au même titre que les autres formes de criminalité organisée, peut notamment participer au financement des organisations terroristes (rançongiciel, escroqueries dites au président, etc.), ou promouvoir leurs actions (actions cyberdjihadistes comme le défacement de sites d'entreprise). Au-delà des conséquences purement économiques qu'engendrent de telles attaques (perte d'activité, indisponibilité temporaire ou perte définitive des données dont celles des tiers, etc.), le risque d'atteinte à l'image est élevé, tant vis-à-vis des fournisseurs que des clients. D'autres formes de délinquance à l'encontre des entreprises peuvent également participer à la menace, en particulier celles qui sont susceptibles de permettre à des terroristes d'usurper des identités ou des fonctions professionnelles ou celles qui les amèneraient à s'approprier certains biens (matières ou matériels dangereux notamment).

Pour les entreprises, la réponse à la menace terroriste passe donc par une démarche de sécurité économique globale, au quotidien, impliquant l'ensemble du personnel, et visant à assurer une protection optimale de son patrimoine humain, immobilier et informationnel. C'est notamment sur cette dernière part que l'effort doit être concentré aujourd'hui (protection des systèmes d'information). ■

POUR ALLER PLUS LOIN

CONSULTER

- *Le compte-rendu du Conseil des ministres du 27 janvier 2016*.
- *Décret n°2016-66 du 29 janvier 2016 instituant un « service de l'information stratégique et de la sécurité économiques »*.

(1) Directions régionales des entreprises, de la concurrence, de la consommation, du travail et de l'emploi.

LA CYBERSÉCURITÉ, UNE PRIORITÉ NATIONALE ET EUROPÉENNE

Guillaume POUPARD
Directeur général de l'Agence nationale de la sécurité des systèmes d'information

Suite aux attaques informatiques qui ont touché la France et d'autres pays ces deux dernières années, la sécurité du numérique est au cœur des débats et exige de l'État une réponse adaptée aux nouveaux enjeux nés des évolutions des usages numériques et des menaces qui y sont liées.

Pour que le numérique demeure un espace de liberté, d'échanges et de croissance, il est nécessaire que la confiance et la sécurité y soient établies et défendues. La stratégie nationale pour la sécurité du numérique, présentée en octobre 2015 par le Premier ministre français, a posé les bases d'une réflexion commune et surtout d'une responsabilité partagée entre l'État, les acteurs économiques et les citoyens dans l'exercice de leur vie numérique.

Ce nouveau « contrat social » met la confiance et la sécurité du numérique au cœur des actions entreprises par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), autorité nationale en ces domaines depuis sa création en 2009.

Protéger les infrastructures critiques : une ambition nationale

Ces dernières années, des attaques réussies contre des systèmes de contrôle de processus industriels ont mis en évidence la réalité des menaces qui pèsent sur nos infrastructures critiques et les conséquences potentiellement destructives qu'une attaque informatique, par exemple d'origine terroriste, pourrait avoir.

Ainsi, porté par la loi, l'un des défis majeurs relevés par l'ANSSI est la mise en place effective d'un dispositif efficace de cybersécurité des opérateurs d'importance vitale (OIV), publics et privés, basé sur la confiance et les échanges d'informations.

Pendant près de deux ans, des groupes de travail réunissant les opérateurs, l'ANSSI et les autorités compétentes pour chaque secteur d'activité, ont élaboré des règles de sécurité organisationnelles et techniques, destinées à élever le niveau de sécurité des systèmes d'information les plus critiques des OIV, les systèmes d'information d'importance vitale. Les premiers arrêtés fixant pour chaque secteur les règles de cybersécurité applicables aux OIV sont entrés en vigueur au 1er juillet 2016 et au 1er octobre 2016.

Chargée d'assurer la défense des systèmes d'information de l'État des OIV, l'agence met aussi ses experts au service de la recherche afin d'anticiper et de détecter de plus en plus efficacement et rapidement les éventuelles attaques.

Afin d'assurer la réussite de ce dispositif, l'ANSSI travaille aux côtés des petits et grands acteurs de la filière industrielle de la cybersécurité afin de construire, ensemble, une offre de produits et de services de qualité et de confiance.

… et européenne

Une approche nationale de la cybersécurité est cependant insuffisante : la France promeut l'autonomie stratégique de l'Europe en matière de sécurité du numérique. Là encore, la confiance est essentielle pour garantir l'émergence d'une « Europe du numérique » souveraine, confiante et ouverte sur le monde.

La directive européenne NIS (*Network and Information Security*) adoptée en 2016 conforte les orientations choisies par la France. En effet, des opérateurs fournissant des services essentiels au maintien d'activités économiques ou sociétales critiques, appelés opérateurs de services essentiels (OSE), seront désignés par les États membres de l'Union européenne. Transposé dans le droit national d'ici mai 2018, ce nouveau cadre va permettre d'élargir le dispositif français de cybersécurité des opérateurs d'importance vitale à de nouveaux acteurs, exposés aux menaces d'origine informatique.

Aux côtés de ses partenaires européens, la France a également participé à l'élaboration du règlement e-IDAS, applicable depuis le 1er juillet 2016, qui a pour ambition d'accroître la confiance dans les transactions électroniques sécurisées entre les citoyens et les autorités publiques, et plus largement avec les entreprises.

La sécurité du numérique : une responsabilité partagée

L'ANSSI n'agit cependant pas seule : chacun est responsable de ses actes face au développement croissant du numérique. La prise de conscience individuelle des risques liés à la croissance du numérique reste aujourd'hui insuffisante. Des secteurs d'activité ou des collectivités locales, jusque-là peu numérisés, rattrapent leur retard et doivent être soutenus sur le plan de la sécurité, y compris au regard d'éventuelles spécificités.

L'ANSSI accompagne au niveau national cette prise de conscience en intervenant régulièrement auprès des professionnels pour promouvoir les bonnes pratiques informatiques auprès des dirigeants de grandes entreprises mais aussi, depuis peu, auprès du tissu économique et des institutions à l'échelle régionale.

Le déploiement en régions de référents ANSSI a débuté en décembre 2015 : chaque préfecture de région accueillera d'ici 2017 un expert de l'agence afin de sensibiliser les acteurs locaux du public et du privé aux bonnes pratiques informatiques, animer un réseau des acteurs de la sécurité du numérique en local et apporter l'expertise de l'agence au plus près des entreprises et des écosystèmes locaux.

Agir ensemble pour la sécurité du numérique

Si l'État et les professionnels ont un rôle fort à jouer, il ne faut pas non plus négliger l'implication nécessaire du citoyen dans la prise en compte, au quotidien, de la sécurité dans ses usages numériques. Dès notre plus jeune âge, nous avons un rôle à jouer, chacun à notre niveau. L'ANSSI encourage tous ses publics à relayer les messages de sensibilisation et recommandations techniques, quel que soit leur niveau d'expertise.

Ainsi, les développements récents et simultanés de nouveaux usages et de nouvelles techniques de stockage et de traitement des données favorisent l'émergence de risques de déséquilibre économique et d'atteinte à la sécurité individuelle des personnes ainsi qu'à celle des nations. La captation massive ou illicite de certains types de données personnelles et leur traitement peuvent en effet entraîner des atteintes à la vie privée, voire à la sécurité individuelle ou collective, ou une exploitation commerciale abusive.

Le citoyen numérique a un rôle d'alerte à jouer également : signaler une vulnérabilité est désormais encouragé et facilité par une simple connexion au site internet de l'ANSSI. Le futur dispositif d'assistance aux victimes de cybermalveillance, mené conjointement avec le ministère de l'Intérieur, permettra d'aller encore plus loin en créant des passerelles de proximité entre les citoyens et les acteurs de l'écosystèmes de la cybersécurité.

Porteuse d'innovation et de croissance, la transition numérique engendre aussi des risques pour l'État, les entreprises et les citoyens allant de la cybercriminalité à l'espionnage et passant par de la propagande ou du sabotage. Aujourd'hui la cybersécurité n'est plus une option : elle est la condition même de la confiance et gage de réussite de la transition numérique. ■

POUR ALLER PLUS LOIN

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

Rattaché au Secrétaire général de la défense et de la sécurité nationale, l'ANSSI a un triple rôle à jouer en tant qu'autorité nationale en matière de sécurité des systèmes d'information :

- *détection des attaques informatiques*
- *prévention de la menace*
- *conseil et soutien aux administrations et aux OIV ainsi qu'information du public sur les menaces*

https://www.legifrance.gouv.fr/eli/loi/2016/3/22/INTX1524877L/jo/texte

TERRORISME, CYBERSÉCURITÉ ET MODERNISATION

Thierry DELVILLE
Délégué ministériel aux industries de sécurité, chargé de la lutte contre les cyber menaces

En 2015 et 2016, la France a été très durement touchée par la barbarie terroriste. Jamais, jusqu'alors, nous n'avions connu sur notre sol des attaques terroristes d'une telle nature et d'une telle ampleur. Depuis de nombreux mois, l'ensemble des forces de sécurité se mobilisent, sans ménager leur temps ni leur énergie, pour protéger les Français et défendre nos libertés fondamentales. Nous savons qu'à l'aube de 2017 rien n'est encore gagné sur ce terrain, que la menace sera tout aussi élevée et qu'il nous faudra par là même continuer à faire preuve d'une vigilance et d'un engagement de chaque instant.

Le combat contre le terrorisme se livre également dans le cyberespace. L'organisation Daesh se sert en effet de l'Internet et des réseaux sociaux comme de puissants vecteurs de propagande et de recrutement. La plupart des néo-djihadistes qui ont rejoint ou qui cherchent à rejoindre la Syrie ou l'Irak, se sont pour la plupart radicalisés sur l'Internet.

Le caractère inédit et la force réticulaire de nos ennemis résident dans le croisement entre deux phénomènes concomitants dont ils ont su tirer le meilleur parti : une évolution stratégique d'une part – l'avènement d'un terrorisme de proximité qui recrute ses activistes dans les sociétés mêmes qu'il entend frapper – et une évolution technologique d'autre part, le développement à partir du milieu des années 2000 de l'Internet 2.0 qui permet la constitution de communautés numériques, lesquelles peuvent représenter autant de lieux où se structure l'identité même des individus qui les fréquentent.

La lutte contre le terrorisme et la radicalisation sur le plan juridique

Nous devons adapter nos procédures et nos outils juridiques traditionnels au caractère mondialisé et ubiquitaire du terrorisme et de la cybercriminalité. Les procédures d'entraide judiciaire doivent ainsi être simplifiées afin de permettre aux enquêteurs de recueillir plus rapidement, auprès des acteurs numériques étrangers, les données nécessaires à la poursuite des investigations.

Notre premier objectif consiste à entraver l'action et la diffusion de la propagande terroriste. Car, si nous agissons sans relâche pour empêcher la commission d'actes terroristes, il est également nécessaire, au-delà de ce volet sécuritaire, que nous intervenions en amont, notamment sur l'Internet, pour briser les « continuums de radicalisation » qui peuvent conduire à un passage à l'acte violent. C'est la raison pour laquelle nous nous sommes dotés, depuis plus d'un an, des moyens juridiques nécessaires, avec l'adoption de la loi antiterroriste de novembre 2014, la loi sur le renseignement de juillet 2015, et la prolongation de l'état d'urgence par la loi du 21 juillet 2016. Ce dernier texte tient compte notamment des moyens numériques pouvant apporter des éléments de preuve, par exemple, lors des perquisitions administratives.

Dès la publication, en février 2015, des décrets d'application de la loi du 13 novembre 2014, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) a ainsi mis en œuvre les procédures de retrait et de déréférencement de contenus illicites par les moteurs de recherche sur l'Internet, et, le cas échéant, de blocage des sites qui n'avaient pas procédé

au retrait. L'année dernière, le ministère de l'Intérieur a ainsi traité plus de 1000 demandes de retrait et de déréférencement, et 283 blocages de sites ont été réalisés.

Par ailleurs, sur les 188000 signalements reçus en 2015 par la plateforme PHAROS exploitée par les services de police et les unités de gendarmerie, près de 32000 concernent des contenus de propagande ou d'apologie du terrorisme, dont une grande partie a été reçue dans les jours qui ont suivi les attentats du mois de janvier. Si ce phénomène ne s'est pas reproduit avec une telle ampleur en novembre dernier, il n'en illustre pas moins l'influence et la malignité de nos ennemis.

Les procédures que nous avons mises en place ont donc d'ores et déjà prouvé leur efficacité : c'est la raison pour laquelle nous devons les généraliser à l'échelle européenne. La Commission européenne a mis en place, depuis juillet 2015, un dispositif analogue à celui en vigueur en France : « l'Unité européenne de référencement de l'Internet », susceptible de décupler considérablement notre force de frappe et faciliter ainsi notre travail de repérage et, le cas échéant, de suppression des contenus illicites sur l'Internet et sur les réseaux sociaux.

Plus largement, pour vaincre la menace djihadiste, il faut aussi la coopération des pouvoirs publics avec les acteurs de la société numérique dans laquelle nous vivons. Ainsi, en 2015, près de 90 procédures judiciaires visant des activités terroristes ont pu être initiées sur la base de signalements PHAROS, grâce aux réponses transmises par les opérateurs aux réquisitions des services de police et des unités de gendarmerie.

Enfin, la lutte contre le crime organisé et son financement, ainsi que l'efficacité et les garanties de la procédure pénale, intègrent des dispositions visant à faciliter le travail des enquêteurs, notamment dans le cas d'enquêtes complexes comme celles qui concernent le cyberespace. En particulier, l'adoption d'un nouveau critère de compétence territoriale permet désormais à la justice française de connaître des faits commis en dehors du territoire national, dès lors que la victime de cyber malveillance réside en France.

L'aide des opérateurs de l'Internet

Les attentats du 13 novembre 2015 ont été l'occasion de faire la démonstration de l'aide précieuse que les grands opérateurs de l'Internet pouvaient nous apporter en situation de crise majeure. Des services ont été mis en place spontanément sur les réseaux sociaux, qui ont permis à des millions de citoyens de se signaler auprès de leurs proches pour les rassurer.

Les opérateurs ont su se mobiliser à nos côtés en ces heures tragiques pour le pays. La promptitude et la pertinence avec lesquelles ils répondent aux demandes que leur soumettent régulièrement les services du ministère de l'Intérieur, le prouvent. Cette coopération vertueuse mise en place doit être encouragée car, contre le terrorisme, nous avons besoin de tous les talents, de toutes les énergies et de toutes les responsabilités.

C'est la raison pour laquelle M. Bernard CAZENEUVE s'est rendu en Californie, pour y rencontrer les représentants des grands opérateurs du numérique afin d'explorer avec eux les voies d'une coopération renforcée face à la menace terroriste. Dans le respect du droit existant, un accord sur une plateforme de bonnes pratiques est intervenu collectivement, le 23 avril 2015.

Le premier objectif a consisté à améliorer le contenu des demandes que nous adressons aux opérateurs, qu'il s'agisse de demandes de retrait de contenus ou bien de demandes concernant des enquêtes en cours. Nous avons adapté nos logiciels et nos circuits de validation pour tenir compte des besoins exprimés par les opérateurs. Avec eux, nous avons formé au bon usage de ces nouvelles procédures les formateurs numériques de la police et de la gendarmerie.

Réciproquement, au sein des grandes entreprises du Net, la tâche des services en charge des obligations légales a été simplifiée. Ces services sont désormais davantage en mesure d'assurer un traitement spécifique de nos demandes ainsi « labellisées ».

Cet accord a marqué le début d'un partenariat particulièrement fructueux, qui se développe à travers un « groupe de contact permanent ». Le premier objectif assigné à ce groupe est de réunir régulièrement les opérateurs et les représentants du ministère de l'Intérieur, du ministère de la Justice et du secrétariat d'État au Numérique. Il constitue désormais une instance de dialogue libre et efficace, fondée sur la confiance mutuelle, entre l'État et les opérateurs.

La France a donc été pionnière en la matière. Aujourd'hui, les États-Unis ont à leur tour affirmé vouloir travailler avec les opérateurs pour contrecarrer l'activité des terroristes sur l'Internet. Notre audace a contribué à garantir au mieux notre sécurité collective.

Les plans et la modernisation de la sécurité intérieure

Outre le renforcement de notre arsenal juridique et la mise en œuvre de coopérations inédites, l'adoption, en janvier 2016, du plan de lutte antiterroriste (PLAT) a fourni les moyens humains, matériels et technologiques pour lutter contre toutes les cybermenaces.

À titre d'exemple, la sous-direction de la lutte contre la cybercriminalité, qui intègre la plate-forme PHAROS et l'OCLCTIC, a vu ses effectifs augmenter de façon significative. De même, au sein de la gendarmerie nationale, le Centre de lutte contre les criminalités numériques (C3N) et l'Institut de recherche criminelle (IRCGN) rassemblent 60 enquêteurs de haut niveau placés à la tête du réseau CYBERGEND qui regroupe désormais plus de 2000 enquêteurs, répartis sur l'ensemble du territoire national.

Cet effort de renforcement s'inscrit dans un cadre plus large : le plan de modernisation pour la sécurité (PMSI) mis en

œuvre pour le ministère de l'Intérieur. Ce plan vise à moderniser les moyens des forces de sécurité, mais aussi à proposer de nouveaux services numériques à nos concitoyens. Il représente un budget très conséquent : 108 millions d'euros investis sur trois ans, de 2015 à 2017. [Le PMSI]

Ces projets sont conçus dans une démarche collaborative impliquant tous les acteurs ministériels – particulièrement les forces de police et de gendarmerie – voire interministériels. À l'heure de la révolution numérique, l'intégration numérique ne doit plus se heurter au cloisonnement des forces. Au moment où, face aux défis auxquels nous sommes confrontés, la coopération internationale et le partenariat avec les grands acteurs privés sont nécessaires, il est plus que temps de faire tomber les cloisons internes qui n'ont plus lieu d'être.

C'est dans cet esprit que travaille la délégation ministérielle aux industries de sécurité et la mission pour la lutte contre les cybermenaces, qui constituent un point d'entrée unique et un interlocuteur bien identifié. Les décisions annoncées lors de la réunion du Comité de la filière des industries de sécurité (COFIS), le 1er décembre dernier, ont trouvé, pour la plupart, une application concrète, notamment pour faciliter les coopérations entre l'État et les industriels en cas de crise. L'action du ministère de l'Intérieur s'inscrit pleinement dans le cadre des 5 objectifs définis par la stratégie nationale de sécurité du numérique annoncée le 16 octobre 2015 par le Premier ministre. Par ailleurs, la France soutient toute initiative de la Commission européenne et des acteurs concernés pour développer un marché européen de taille critique suffisante.

S'agissant du plan de modernisation proprement dit, deux défis majeurs ont d'ores et déjà été engagés.
Le premier concerne la mobilité des forces. Piloté par les directions générales de la police nationale et de la gendarmerie nationale, et conduit techniquement par le service des technologies et des systèmes d'information de la sécurité intérieure, il a bénéficié également du concours technique de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pour la solution de transmission sécurisée. Il s'agit de doter les policiers et les gendarmes d'un outil sécurisé de mobilité opérationnelle, qui leur permette de disposer des informations nécessaires à l'accomplissement de leur mission et de conduire un certain nombre de procédures depuis le terrain. L'expérimentation NEOGEND, menée par la gendarmerie dans le département du Nord depuis le mois de septembre 2015, démontre la pertinence et l'efficacité du système. Après une seconde phase d'expérimentation à plus large échelle dans le courant de 2016, plus de 60 000 équipements de mobilité opérationnelle auront été déployés d'ici la fin 2017 sur l'ensemble du territoire.

Le second défi concerne l'utilisation d'outils décisionnels. Il s'agit d'exploiter, dans le strict respect des libertés individuelles, les grands volumes de données disponibles et accessibles, dans le cadre de l'open data notamment, ou bien dans les systèmes d'information propres au ministère. Il s'agit d'un axe particulièrement important pour les forces de sécurité dans leurs différentes composantes. Une phase de recherche et d'expérimentation permettra de mettre au point des applications spécifiques, notamment en matière de police judiciaire.

La lutte contre la criminalité numérique

Si la lutte contre le terrorisme est une priorité absolue, le ministère de l'Intérieur ne se consacre pas moins à la lutte contre toutes les formes de criminalité numérique. Cet effort s'inscrit dans la « stratégie nationale de sécurité pour le numérique » présentée le 16 octobre 2015 par le Premier ministre. Le ministère de l'Intérieur y joue un rôle actif et est force de proposition dans l'élaboration de cette nouvelle stratégie. Le traitement des victimes de cyber malveillance – notamment les particuliers et les petites et moyennes entreprises, qui ne disposent pas toujours des compétences et des moyens nécessaires – va être significativement amélioré sur l'ensemble du territoire. En la matière, l'information des victimes est une véritable nécessité.

Outre le renforcement de nos dispositifs d'information, l'autre priorité qui nous mobilise réside dans la modernisation et l'adaptation de notre cadre juridique et réglementaire. Une telle exigence, valable contre le terrorisme, l'est aussi contre les autres formes de cybercriminalité. L'évolution rapide et la diversification des menaces nous imposent, en effet, de permettre aux enquêteurs de disposer en permanence de capacités technologiques à l'état de l'art. ■

POUR ALLER PLUS LOIN

OFFICE CENTRAL DE LUTTE CONTRE LA CRIMINALITÉ LIÉE AUX TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION (OCLCTIC)

Créé en 2000, l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) met ses compétences techniques et opérationnelles au profit de la lutte contre les infractions spécifiques liées aux nouvelles technologies.

PLATEFORME PHAROS

PHAROS est la plate-forme d'harmonisation, de recoupement et d'orientation des signalements dédiée au traitement des contenus illicites de l'Internet.

PLAN DE LUTTE ANTITERRORISTE (PLAT)

Le plan de lutte antiterroriste comporte des mesures visant le renforcement des moyens pour la prévention et la lutte contre la radicalisation.

RÉSEAU CYBERGEND

Le Réseau CyberGend regroupe des gendarmes et des correspondants N-TECH, enquêteurs spécialisés en technologie numérique, chargés de lutter contre la cybercriminalité.

NEOGEND

Le projet NEOGEND vise à équiper les gendarmes de tablettes ou smartphones afin de rendre leurs applications « métiers » plus opérationnelles sur le terrain.

L'APPORT DE L'UNION EUROPÉENNE À LA PROTECTION DES INFRASTRUCTURES CRITIQUES

Grégoire DEMEZON
Chargé de mission au sein du Cabinet du ministre de l'Intérieur

Franck PEINAUD
Conseiller à la Délégation de l'Union européenne en Tunisie

De nombreuses infrastructures constituent de possibles cibles d'attaques terroristes compte tenu de leur caractère essentiel au fonctionnement des sociétés modernes et elles sont ainsi considérées comme critiques. Il est possible de les définir comme l'ensemble des installations dont le sabotage, l'arrêt ou la destruction aurait un impact grave sur la santé, la sécurité et le fonctionnement des économies ou des institutions. Peuvent ainsi être considérées comme infrastructures critiques, les installations et les réseaux dans le secteur de l'énergie, les technologies de communication et de l'information, les transports, l'eau, la production, le stockage et le transport des produits et matières dangereux, le secteur de la santé ou encore celui de la finance. Tout l'enjeu est donc, après la conduite d'une solide étude de risques, de réduire leur vulnérabilité[1].

Cette question se pose avec d'autant plus d'acuité que les actions recommandées par Daech depuis septembre 2016, disponibles en sources ouvertes, sont les suivantes :

- le **terrorisme de sabotage** (*Irhab takhribi*) : actions de sabotage contre les infrastructures de pétrole, gaz, ressources minières ; eau (barrages, canaux, réserves), électricité (infrastructures) ;
- le **terrorisme d'arrimage** (*Irhab tasalluli*) : infiltration non seulement des manifestations et des grèves mais aussi des institutions et des administrations, pour y mener des actions de sabotage ou de sabordage de l'intérieur ;
- le **terrorisme d'abattage** (*Irhab adh-dhabh*) : menaces contre les personnalités et diffusion de décapitations à grande échelle ; décapitation systématique des victimes pour semer la terreur.

Pour chaque type d'attentat, une médiatisation maximale est explicitement recommandée par Daech pour tenir les médias en haleine dans la durée, occuper l'espace médiatique, notamment en laissant plusieurs indices et caches d'armes, tout en suscitant de nouvelles vocations.

Les dispositions prises par l'Union européenne (UE) constituent la réponse la plus adaptée à la première menace décrite *supra*.

Dès 2006, l'UE s'est dotée d'un programme de protection des infrastructures critiques (EPCIP) pour améliorer leur sécurité active et passive[2]. Une déclinaison concrète de ce programme s'est matérialisée, en 2008, par l'adoption d'une

(1) CROS Michel, GAULTIER-GAILARD Sophie, HARTER Hélène et PECH Pierre, *Catastrophes et risques urbains*, Cachan, Tec & Doc Lavoisier, coll. « Sciences du risque et du danger », 2010, 273 p.

(2) Commission européenne, *Communication de la Commission au Parlement européen et au Conseil sur un programme européen de protection des infrastructures critiques*, COM 2006/786, 12 décembre 2006.

directive portant sur le recensement et la protection des infrastructures critiques. Celle-ci, révisée en 2013, classe les infrastructures critiques en deux types : les infrastructures critiques nationales (ICN) et les infrastructures critiques européennes (ICE). La sécurité des premières est de la responsabilité partagée des propriétaires-exploitants et des États où elles se situent. La directive impose aux États membres (EM) d'identifier ces infrastructures critiques, de formaliser un dialogue avec les propriétaires-exploitants et d'établir, en lien avec eux, un plan d'intervention spécifique. Les secondes sont les infrastructures qui ont une importance telle que leur arrêt ou leur destruction aurait un impact sur plusieurs États membres. Le recensement, le classement et la protection de ces infrastructures relèvent, dès lors, d'une responsabilité partagée entre les propriétaires-exploitants, plusieurs EM et les instances européennes.

L'UE a assuré, dans ce domaine, le financement d'un certain nombre de projets pour un montant de 140 millions d'euros, sur la période 2007-2013, dans le cadre du programme « prévention, préparation et gestion des conséquences en matière de terrorisme et d'autres risques liés à la sécurité ». Elle a également développé des outils techniques pour améliorer la coordination entre EM, comme le « *Critical Infrastructure Warning Information Network* » (CIWIN), qui constitue à la fois un réseau d'alerte en matière de protection des infrastructures sensibles et une plateforme sécurisée d'échanges de bonnes pratiques concernant les menaces et les vulnérabilités communes.

Enfin, au-delà des infrastructures physiques, l'UE s'est également intéressée à la protection du cyber-espace et aux vulnérabilités spécifiques des EM de l'UE dans ce domaine. Le risque est ainsi aujourd'hui bien réel que la fourniture de services de première nécessité puisse être perturbée par une cyber-attaque. Apparaît ainsi un risque de cyber-terrorisme dont les conséquences pourraient être considérables. En 2013, à l'initiative de la Commission européenne, l'UE a adopté une stratégie de cyber-sécurité portée par Catherine ASHTON, alors haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité. Confrontées à cette dimension transnationale, les forces de sécurité doivent, en effet, se coordonner entre elles et échanger des renseignements pour agir efficacement. C'est pour cela que le Parlement et le Conseil ont adopté, en 2013, une directive relative à la protection des systèmes d'information qui a permis d'harmoniser les incriminations et les poursuites pénales concernant les infractions dans le cyber-espace. D'autres initiatives peuvent être citées comme la création en janvier 2013 de l'« *European Cyber-Crime Center* » (EC3) au sein d'Europol. L'objectif de ce centre est de partager l'expertise entre les forces de police des EM dans ce domaine.

L'UE estime, en outre, « *qu'il est important de protéger les infrastructures critiques étant donné qu'une attaque non conventionnelle, par des auteurs de menaces hybrides, pourrait entraîner de graves perturbations de l'économie ou de la société* »[3], qu'il s'agisse d'acteurs étatiques ou non étatiques.

À travers les transports, l'énergie ou le cyber-espace, c'est donc bien l'ensemble des infrastructures, qu'elles soient physiques ou immatérielles, et qui représentent pour elle une vulnérabilité particulière, que l'UE entend contribuer à protéger face à la menace terroriste. ■

POUR ALLER PLUS LOIN

PROGRAMME DE PROTECTION DES INFRASTRUCTURES CRITIQUES (EPCIP)

Programme européen pour la protection des infrastructures critiques. Lancé par le Conseil européen en 2004, ce programme est conçu pour identifier et protéger les infrastructures critiques, contre les catastrophes naturelles, le crime et plus spécifiquement, le terrorisme.

EUROPEAN CYBER-CRIME CENTER » (EC3) AU SEIN D'EUROPOL

L'EC3 s'occupe des affaires de cybercriminalité en apportant un soutien technique, financier, ou encore, humain, concernant l'attaque contre les systèmes informatiques, la fraude en ligne et l'exploitation sexuelle des enfants via Internet.

(3) Commission européenne et haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, *Communication conjointe au Parlement européen et au Conseil sur un cadre commun en matière de lutte contre les menaces hybrides, Une réponse de l'Union européenne*, JOIN (2016) 18 final, 6 avril 2016.

Les attentats, depuis janvier 2015, ont impacté l'image et la réputation de la France.

**Les chiffres du tourisme en baisse illustrent sa perte d'attractivité.
Luxe, restauration, hôtellerie, etc.. en sont aussi victimes.
Le gouvernement réagit pour relancer l'économie .**

PLAN DE RELANCE ÉCONOMIQUE

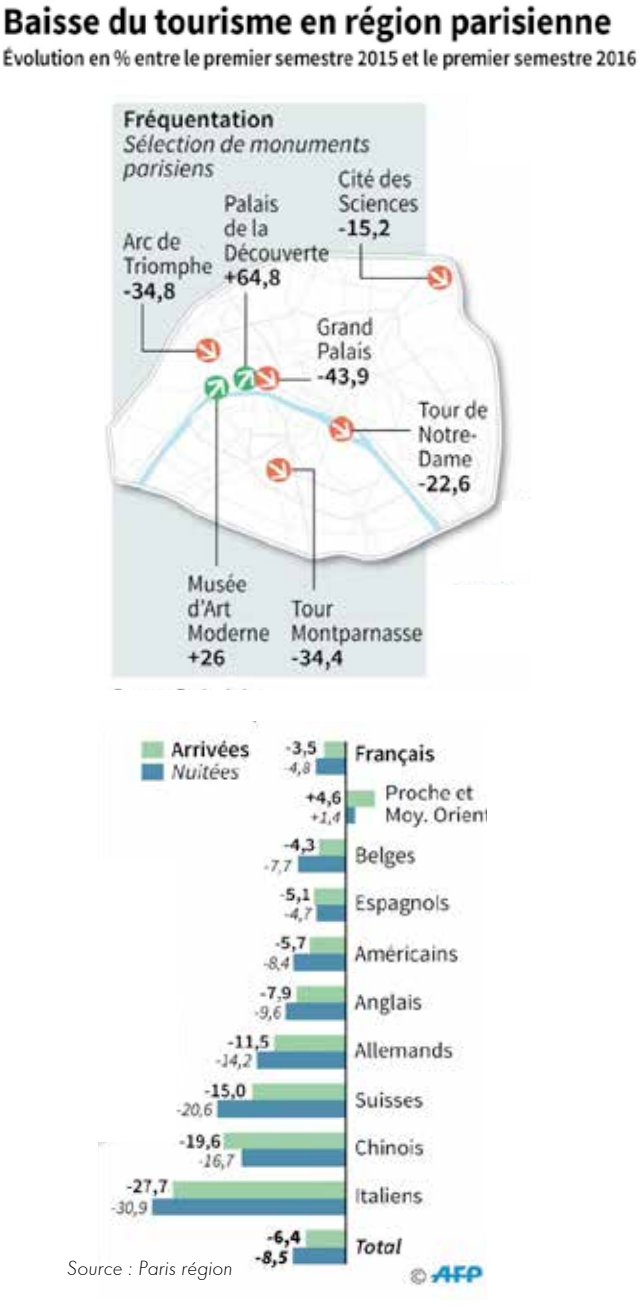
Plan ORSEC

Alors que Frédéric VALLETOUX, président du Comité régional du tourisme (CRT), déplore 1,8 million de touristes en moins entre janvier et août 2016, soit une baisse de 7% de l'affluence touristique par rapport à la même période en 2015, le gouvernement a dévoilé lundi 7 novembre, un an après les attentats de novembre 2015, un plan ORSEC (Organisation de la réponse de sécurité civile) pour le secteur du tourisme.

Face à l'impact des attentats terroristes sur les chiffres du tourisme, Manuel Valls a annoncé simultanément lors du Comité interministériel du tourisme et sur son compte Twitter une enveloppe de 42,7 millions d'euros pour défendre ce secteur, qui représente 7,5% du PIB de la France et maintenir l'Hexagone à sa place de 1ère destination touristique au monde.

Sur cette enveloppe, 15,5 millions d'euros seront ainsi consacrés à la sécurité des touristes, puisque c'est majoritairement le risque sécuritaire qui préoccupe ces derniers, en majorité les asiatiques, et qui les poussent à déserter la France (*- 39% de touristes Japonais en moins depuis janvier, - 23% pour les Chinois*). La vidéo-surveillance des lieux touristiques, salles de spectacles, transports publics sera renforcée, ainsi que les équipements de sécurité dans les sites culturels les plus fréquentés, comme les grands musées parisiens. Des commissariats mobiles pourront se rendre dans les hôtels ou sur les sites touristiques afin que les touristes n'aient plus à se déplacer pour porter plainte, lors d'un vol ou d'une agression. Enfin, les aéroports parisiens seront munis de nouveaux modules Parafe [1] pour faciliter le contrôle automatisé d'identité.

Cependant, si le volet sécuritaire est bien pris en compte par ce plan ORSEC, il ne suffira pas à attirer les touristes. D'autres mesures sont ainsi mises en avant, comme des aides accordées aux hôteliers et aux restaurateurs afin qu'ils puissent notamment se moderniser et s'équiper en Wi-Fi, ou encore apportées aux retraités modestes, pour leur permettre de partir en vacances. Enfin, un budget de 10,5 millions d'euros servira aux campagnes de communication qui viseront à la promotion de la destination France, avec le tournage de films ou de séries dans la capitale, la création d'événements associés à des offres promotionnelles, « pour créer – selon l'adjoint au tourisme, Jean-François Martins – un sentiment d'urgence de la visite à Paris », ou encore l'installation d'un nouvel espace d'accueil sous la tour Eiffel... ■



Source : Paris région

(1) Le module Parafe, acronyme de Passage Rapide Automatisé aux Frontières Extérieures à Schengen, permet aux voyageurs, entre l'espace Schengen et son extérieur, de gagner du temps lors du passage aux frontières, grâce au contrôle biométrique.

Interview de
PATRICE LATRON

Préfet, Directeur du cabinet du Préfet de police

Comment percevez-vous l'évolution de la menace, en termes d'occurrence, de gravité, de conséquences... La coproduction de sécurité est-elle aujourd'hui suffisante et adaptée au contexte ?

Les menaces évoluent, croissent, se diversifient, et ce, en matière de terrorisme mais pas uniquement. Les entreprises sont également concernées par le piratage informatique, le vol de données ou encore la défiguration des sites pour des raisons économiques, politiques et idéologiques. Les modes opératoires évoluent pour s'adapter aux technologies de plus en plus perfectionnées, en détourner les utilisations et en exploiter les failles. A titre d'exemple, concernant les vols de véhicules haut de gamme, les malfaiteurs ont mis au point des dispositifs permettant d'empêcher le verrouillage de la voiture et de prendre le contrôle de ces véhicules avec des cartes électroniques qu'ils fabriquent à cette fin.

En matière de coproduction, il paraît plus que jamais essentiel de la renforcer entre les différents services de l'État et les entreprises. A commencer par les liens qui doivent encore être consolidés entre les chefs des entreprises et le préfet de leur département.

Les entreprises ne peuvent plus considérer que leur sécurité est à la seule charge de l'État. Avec les directions sûreté, elles doivent organiser leurs dispositifs et mobiliser leurs propres compétences, en interne ou en externe, pour assurer la sécurité de leurs salariés, de leurs données et de leurs infrastructures. Dans ce contexte sécuritaire, les PME doivent aussi s'interroger sur la prise en compte du risque.

Quelle adaptation des forces de l'ordre à cette menace en termes d'effectif et de mode d'intervention et de coopération avec la sécurité privée ?

Les forces de l'ordre voient leurs effectifs augmenter depuis les attentats. Nous avons désormais intégré la nécessité d'associer la sécurité privée à la sécurité globale. Le Gouvernement en a pris acte en créant, il y a quelques années, le Centre National des Activités Privées de Sécurité (CNAPS), qui garde un rôle important dans l'organisation de la politique de sécurité du Ministère et dans la labellisation des entreprises de sécurité. L'Euro 2016 est un exemple abouti de coopération et de complémentarité. Considérant le besoin de plusieurs milliers de gardes privés, nous avons agi de concert pour la préparation de cet événement majeur. Il a donc fallu développer, très en amont, une politique de mobilisation et d'accompagnement des entreprises privées de sécurité. Nous nous préparons désormais au championnat du monde de handball, qui aura lieu en janvier 2017.

Ces événements sont d'ordre privé. Ils sont soumis au régime de la concurrence. Le choix du prestataire de sécurité incombe donc à l'entreprise. Cependant, l'entreprise doit être agréée par le CNAPS et les agents, eux-mêmes, sont agréés individuellement.

L'intervention de la sécurité privée est-elle légitime et nécessaire ?

Elle est indispensable. Les niveaux d'intervention des forces publiques et des forces privées doivent être dis-

tingués et s'organiser en fonction des besoins du terrain : les grands évènements ne demandent pas la même mobilisation ni le même niveau d'intervention que la gestion de la sécurité au quotidien dans une entreprise.

Dans le cas d'un évènement d'ampleur, la force publique envoie des patrouilles sur la voie publique. Elle est en mesure de répondre, en cas d'urgence, à une attaque armée. Son rôle n'est pas de sécuriser les locaux des entreprises ou de gérer les accès aux manifestations sportives ou culturelles. Cela relève de la sécurité privée, dont le périmètre d'intervention s'étend de plus en plus. La menace terroriste oblige désormais à mettre en œuvre de nouveaux procédés de sécurité tenant compte de la sensibilité et de la vulnérabilité des infrastructures qu'il convient de protéger. Les opérateurs privés de sécurité sont mandatés par les directions sûreté ou les directions générales pour assurer la sécurité des salariés, des infrastructures et des accès. Le rôle de la police est de sécuriser la voie publique, de contrôler les abords par des passages et des rondes. Il est également d'informer les services de l'État et d'intervenir en cas de menace avérée.

Concernant l'armement, les demandes de la part des entreprises restent exceptionnelles. C'est pourtant une possibilité réelle, mise en œuvre depuis peu dans quelques entreprises.

Par ailleurs, une intervention de ce type doit être comprise dans la durée. Le préfet autorise l'acquisition des armes par l'entreprise, laquelle doit ensuite trouver un opérateur privé de sécurité qui, lui-même, doit demander au préfet des autorisations individuelles de détention d'armes sur le site de l'entreprise bénéficiaire. L'achat des armes et leur stockage est à la charge de l'entreprise. Elle doit donc faire l'acquisition d'un système de sécurisation des armes.

L'entreprise ne peut-elle pas faire directement appel à un opérateur privé de sécurité avec ses propres gardes armés ?

Ça n'existe pas en France. En effet, ce n'est pas une accréditation que l'on donne à l'entreprise de sécurité. Le préfet l'attribue, individuellement, à chacun de ses agents, et prend fin à la rupture du contrat. Cette précision est mentionnée dans le permis de port d'arme. Par ailleurs, le droit du travail s'appliquant, lorsqu'il y a un changement de prestataire, l'entreprise qui reprend le marché a l'obligation de conserver les salariés s'ils l'exigent. C'est une règle qui s'applique à tous les prestataires, que ce soit une entreprise de nettoyage ou d'armement.

Des formations particulières sont-elles exigées ?

Nous avons créé à la Préfecture de Police une forme de jurisprudence locale sur les critères attendus des gardes qui se présentent. Mais la loi va être complétée en matière de formation. C'est le préfet qui, en dernier ressort, a le pouvoir d'appréciation sur la fiabilité de l'intéressé (extrait de casier judiciaire, enquête de moralité, maîtrise de l'arme, expérience professionnelle, inscription en club de tir, etc.).

Les entreprises, salariés, public et visiteurs qui participent aux grands évènements organisés dans la capitale sont exposés aux risques d'attentats. L'état d'urgence justifie-t-il la mobilisation systématique de gardes armés ?

Les moyens de l'État sont adaptés et suffisants pour sécuriser ces évènements ponctuels. Pour le moment, l'armement d'agents privés sur ce type de mission n'est pas possible.

La Préfecture de Police est structurée pour faire face à cette demande de sécurité, qui se concrétise par la mise en place de patrouilles dynamiques, réparties par secteurs , dédiées à cette mission, et formées pour intervenir en cas d'urgence et de menace avérée. Ces patrouilles, visibles, ont le double avantage de rassurer la population et de rester imprévisibles pour des personnes malveillantes qui auraient étudié le dispositif en amont.

Nous avons réduit drastiquement le nombre des sites placés sous surveillance statique, cette dernière étant davantage déléguée aux opérateurs privés de sécurité sur une longue durée.

En dehors des OIV et Seveso, dont la sécurisation fait déjà l'objet d'un dispositif spécifique, percevez-vous des zones plus particulièrement exposées au risque d'attentat ?

L'évolution des modes opératoires et la diversification des cibles rendent potentiellement tous les secteurs d'activités, économique ou humaine, vulnérables. Des efforts particuliers sont faits pour sécuriser les sites religieux, les espaces de transports, les grands centres commerciaux, les sites touristiques et les institutions. À titre d'illustration, des exercices d'ampleur sont régulièrement organisés par la Préfecture de Haute Seine. La BRI réalise des exercices d'entraînement de nuit dans de grands centres commerciaux parisiens. Quant aux transports, nous entretenons des liens extrêmement privilégiés avec la SNCF et la RATP.

Concernant ces sites, des équipes dédiées patrouillent dans Paris avec une densité supérieure à la moyenne. Des unités de force mobile (CRS et gendarmes) viennent encore renforcer le dispositif. Une force d'intervention rapide, en système d'astreinte, permettant d'intervenir rapidement sur un attentat équipée avec des armes de guerre, est également prévue en relais avec l'intervention de la BRI.

La Préfecture a-t-elle un rôle dans la prévention de la radicalisation qui touche ces secteurs d'activités ?

Le dispositif national CNAPR met à disposition un numéro vert que tout citoyen, salarié, ou chef d'entreprise, peut appeler pour signaler des comportements sensibles. Une réunion régulière étudie, cas par cas, nominativement, les signalements. Elle associe les services de renseignement et de police, en présence d'un haut fonctionnaire chargé de la prévention de

la radicalisation, du Parquet de Paris et d'un représentant de l'administration pénitentiaire. Ce travail est réalisé en partenariat avec l'Éducation nationale, la ville et les caisses d'allocation pour le soutien des familles de radicalisés qui sont dans la détresse.

Ces sujets sont extrêmement sensibles et ça ne se règle pas d'un trait de plume ou d'une décision administrative dans un bureau. C'est pourquoi la Préfecture de Police prend en compte chaque cas et déploie un dispositif adapté à chaque niveau de menace, que ce soit dans une démarche préventive ou de traitement de la radicalisation. La campagne de communication autour de ce numéro vert doit être relayée auprès des entreprises qui ne savent pas encore toujours à qui s'adresser.

Est-ce le rôle de l'État que d'assurer la protection des entreprises sur le territoire national ?

Nous cherchons à être extrêmement proactifs vis-à-vis des entreprises. Le renseignement joue, en la matière, un rôle fondamental, tant au niveau de la prévention que de la répression. La direction du renseignement de la Préfecture de Police, aux côtés de la DGSI, travaille au quotidien sur un certain nombre de risques ou de menaces.

Les contacts entre les directions de sûreté et la Préfecture sont établis à plusieurs niveaux. Les responsables sûreté des grands groupes, situés à Paris et dans la petite couronne, ont des relations régulières avec la direction du renseignement. Concernant les PME, nous proposons un audit de sécurité par un service spécialisé – le Service Information Sécurité – lorsque l'on a connaissance d'une menace particulière. Ce service, généralement en charge des grands groupes, s'attache aussi à auditer les cas les plus sensibles. Il est composé de policiers mandatés par le préfet de police, pour amorcer des préconisations permettant aux entreprises de se mettre à niveau en termes de sécurité technique et humaine.

La Préfecture de Police intègre, dans un dispositif original placé sous l'autorité unique du préfet de police Michel Cadot, l'ensemble des compétences concourant à la sécurité : renseignement, prévention, sécurité au quotidien assurée par les commissariats d'arrondissement, patrouilles sur les sites sensibles, polices de l'immigration et de l'hygiène, police judiciaire et unités spécialisées comme la BRI, unité d'intervention dédiée à la protection de Paris.

Paris est aujourd'hui une ville rayée des destinations de voyages proposées par certains tour-opérateurs. Son image, dans les médias étrangers, est celle d'une ville hostile, voire en guerre. Cette perception est-elle fidèle à la réalité de la menace ?

Paris est le coeur de la France, le siège des institutions et le lieu de grands évènements internationaux. Nous avons eu deux évènements d'ampleur mondiale cette année : la COP 21 et l'Euro 2016. Paris, c'est aussi la première destination touristique au monde. Pour beaucoup, elle est le voyage d'une vie. Elle est donc naturellement exposée, compte tenu de la fréquence des évènements, des flux importants de populations et de son fort rayonnement.

C'est un sujet dont s'est emparé le Gouvernement, lequel organise des concertations régulières, notamment sous l'autorité du premier ministre et du ministre des affaires étrangères, en lien avec le ministre de l'Intérieur, pour déterminer comment améliorer l'image de Paris et mieux sécuriser la ville.

Nous travaillons étroitement avec les acteurs économiques pour renforcer leur protection. A ce sujet, la Tour-Eiffel, Notre-Dame, Le Louvre ou encore le Sacré-Coeur sont des correspondants réguliers de la préfecture de police. Les Champs Elysées disposent également d'un dispositif de sécurité spécifique, renforcé par une brigade dédiée à cette zone.

Un plan dédié au tourisme, élaboré depuis 2013 et comportant 26 mesures, vise à améliorer la sécurité des touristes à Paris. Il comporte notamment un système de partenariat avec l'INALCO qui nous permet de bénéficier, pour les mois les plus visités, juillet et août, d'étudiants interprètes en chinois, coréen et japonais.

À qui incombe la décision d'élever un niveau de sûreté sur une zone ou un site ?

La sécurité de la voie publique relève du préfet de police.

En fonction des mesures à adopter pour renforcer la protection de manifestations commerciales ou festives, la loi prévoit la possibilité de facturer les prestations de sécurité publique. Ceci se fait sur la base d'un barème national établi par le Ministère de l'Intérieur. La mise en oeuvre de moyens importants et significatifs par l'État pour sécuriser un évènement d'ordre privé, que ce soit par exemple pour un salon ou l'anniversaire d'un groupe.

Compte tenu de l'investissement en dispositifs de sécurité, les entreprises n'ont-elles pas intérêt à faire appel à un opérateur privé de sécurité ?

Le choix des moyens publics à mettre en oeuvre relève de la responsabilité du préfet. C'est pour le moment tout le paradoxe de ce système. Cependant, il convient de lever une ambiguïté sur l'intérêt de l'Etat aurait à facturer : la somme facturée par le préfet alimente directement le budget de l'Etat.

La demande d'installation de vidéosurveillance s'est intensifiée depuis janvier 2016. Comment s'effectuent les transmissions et l'exploitation des informations ?

Les captations d'images sur la voie publique sont transmises et traitées par un centre de supervision d'une collectivité ou de l'État. Le Préfet de police, conscient de l'utilité de cette technologie pour le traitement de la délin-

quance et la prévention du terrorisme, a dégagé un budget pour financer le développement de la vidéo protection avec de nouvelles caméras, dans Paris, petite et grande couronne.

Des évènements majeurs, comme a pu l'être l'Euro 2016, bénéficient de ce principe de raccordement. Les images des vidéos des hôtels qui ont hébergé les équipes de l'Euro 2016 nous ont été transmises. Concernant les transporteurs, nous assurons le raccordement des images au centre de supervision de la Préfecture de Police afin d'avoir accès aux vues de la RATP et de la SNCF.

Le raccordement des captations entre certaines entreprises et la Préfecture est une garantie de sécurité que les organisateurs offrent à leurs clients à la fois en temps réel – les fonctionnaires de police du commissariat d'arrondissement concentrent leur attention sur tel ou tel évènement – mais également à titre judiciaire, si une menace survient pendant l'événement.

Par ailleurs, les drones sont un moyen efficace pour couvrir les grands évènements parisiens. La Préfecture de Police a développé un système anti-drone mis en oeuvre pour la première fois le 8 mai 2015, pour protéger les cérémonies patriotiques sur les Champs-Elysées. Un décret, en cour de signature, devrait autoriser les services publics à utiliser les drones en ville pour le suivi des foules. Cette technologie s'ajoutera aux moyens développés en parallèle par la DGGN et la DGPN pour couvrir les grands évènements parisiens.

? La Préfecture a-t-elle une démarche prospective quant aux moyens à développer au bénéfice de la sécurité ?

La Préfecture de Police a une réelle démarche prospective concernant le développement de technologies susceptibles de répondre à l'ensemble des menaces. C'est à ce titre que la Direction Opérationnelle des Services Techniques et Logistiques, chargée du soutien logistique et matériel des fonctionnaires de police, a développé le premier système de lutte anti drone mis en oeuvre en France en 2015. Le laboratoire central de la Préfecture de Police (LCPP) est également très en avance dans le domaine de la recherche sur les causes d'incendie ou le déminage. ■

LA SÉCURITÉ PRIVÉE DANS LA SÉCURITÉ INTÉRIEURE

« à chacun sa place mais une place connue de chacun »

Cédric PAULIN
Directeur de cabinet du directeur du Conseil national des activités privées de sécurité (Cnaps)

La sécurité privée participe de la sécurité intérieure. C'est un fait… Un fait d'autant plus prégnant, depuis deux ans, dans un contexte d'attentats et de menaces terroristes jusqu'alors inconnu en France. Avant d'approfondir cette relation particulière entre la sécurité privée et le terrorisme – qui ne va pas nécessairement de soi –, il est essentiel de comprendre les évolutions plus traditionnelles de la sécurité privée et de sa régulation.

Profession réglementée, forte de 160000 agents de sécurité privée et de 9000 établissements, la sécurité privée fournit désormais plus d'un tiers des personnels de sécurité dans notre pays. Certes, elle ne dépasse pas les effectifs de la police et de la gendarmerie nationales, comme cela est le cas dans la majorité des autres États de l'Union européenne, mais la tendance est à la croissance. C'est même cette croissance forte, dans les années 2000, qui a incité l'État à reprendre la main sur cette relation nécessaire entre les forces publiques et la sécurité privée, en créant un instrument destiné à mieux contrôler ce secteur d'activité stratégique. Le Conseil national des activités privées de sécurité (CNAPS), établissement public administratif sous tutelle du ministère de l'Intérieur et créé par la LOPPSI 2 du 14 mars 2011, est entré en fonction en janvier 2012. Il a en charge la régulation du secteur, à travers la délivrance des autorisations de l'accès à la profession et du contrôle de l'activité, pouvant aboutir à des sanctions.

Si le CNAPS voit les régulés participer à ses différentes instances décisionnelles nationales et locales (Collège, Commission nationale d'agrément et de contrôle, Commissions locales d'agrément et de contrôle) et leur offre ainsi une certaine reconnaissance, il n'en demeure pas moins que, par cette régulation rénovée, l'État entend maîtriser l'évolution du cadre global de la sécurité intérieure. Le CNAPS est le garant de la confiance accordée aux entreprises et agents de sécurité privée et permet d'envisager, à l'avenir, de possibles extensions de compétences, de missions, de périmètre. Il revient aux responsables politiques de décider de ces évolutions.

Où en sommes-nous aujourd'hui ? L'*EURO 2016*, qui a vu la mobilisation de 13000 agents de sécurité, a de ce fait été utile pour évaluer la situation de la sécurité privée : elle a su répondre présente et cela grâce à un maillage territorial fort et une préparation bien anticipée de l'ensemble des acteurs publics et privés. En revanche, il est possible de s'interroger sur la qualité des prestations fournies, s'agissant particulièrement des palpations de sécurité. Cette image synthétique – présence humaine effective mais qualité de prestation parfois douteuse – est probablement ce qui caractérise globalement la sécurité privée aujourd'hui et ce qui montre le chemin qui lui reste à parcourir.

La formation apparaît comme le préalable essentiel à une plus grande professionnalisation du secteur, et notamment des agents eux-mêmes. L'année 2016 sera, dans cette

optique, nouvelle puisque les organisations de formation aux métiers de la sécurité privée seront désormais contrôlées par le CNAPS : la réalité des formations et des examens, le sérieux des formateurs et des jurys seront sous l'œil du régulateur, et sous le coup de sanctions en cas de manquements.

Professionnalisation et moralisation restent des facteurs d'évolution significatifs pour la filière de la sécurité privée. De longue date, certains créneaux, comme le conseil et l'audit en sûreté, l'installation et la maintenance de dispositifs électroniques de sécurité, plus récemment l'auto-surveillance, et les plates-formes collaboratives en sécurité privée, sont envisagés comme pouvant, ou devant, rejoindre le périmètre réglementé, et donc contrôlé, de la sécurité privée. Des discussions sont en cours sur ces sujets ; ils ont tous en commun d'interroger indirectement les frontières du périmètre réglementé. Défi pour le législateur et le régulateur, cet élargissement possible du périmètre force à interroger le principe d'exclusivité, principe issu de la loi fondatrice du 12 juillet 1983, que l'on peut résumer ainsi : une entreprise de sécurité privée ne peut réaliser que des activités de sécurité privée et pas d'autres. S'il est vrai que des exceptions légales existent (en sécurité incendie, en installation d'alarmes, etc.), il est également vrai que nous élargissons rarement la réflexion à ce principe jusqu'au prisme de la compétitivité économique et de la capacité de l'offre française de sécurité privée à proposer des solutions plus globales et incluant de nouveaux services.

Par ailleurs, il faut le reconnaître, le contexte induit par les actes terroristes depuis deux ans a donné à certains questionnements une acuité plus forte encore. Du point de vue de la coproduction de sécurité, la hausse de la demande de sécurité à partir de janvier 2015, observée tant pour les forces publiques que pour la sécurité privée, a remis sur la table la problématique de leur articulation et de leur complémentarité. Qui fait quoi et où ? Cette question, naturelle, logique, ne doit néanmoins pas en occulter une autre, plus complexe encore, car plus sociologique que juridique : qui sait où est l'autre ? En effet, si le transfert de missions et de compétences devenues moins régaliennes peut s'envisager, dans certaines limites, le transfert d'informations paraît plus déterminant encore pour atteindre une coproduction efficiente.

Ainsi, l'armement des agents de sécurité privée, pour certaines missions, pour certains lieux, avec une formation adéquate et une autorisation spécifique, est désormais envisagé – la question n'aurait pas pu se poser avant janvier 2015. Cependant, il conviendra de bien prévoir l'information mutuelle des différents acteurs concernés, tant publics que privés : il faut que les forces de l'ordre sachent précisément où se trouvent les agents de sécurité renforcée sur leur zone de compétence, tout comme il faut nécessairement que les agents de sécurité renforcée aient la capacité de prévenir, en temps réel, les forces de l'ordre d'un événement particulier.

De même, une plus grande présence d'agents de sécurité privée sur la voie publique, mais toujours pour réaliser une mission, même itinérante, de surveillance et de gardiennage d'un ou de lieux privés, peut s'envisager, mais encore faut-il s'assurer que les forces publiques en soient informées et maîtrisent cette extension périmétrique.

Vont également dans le sens d'un plus grand partage d'informations, des développements qui concernent directement les agents de sécurité privée. Étant les premiers présents en cas d'attentats ou d'autres événements graves, les agents de sécurité privée ont désormais des capacités professionnelles adaptées : chaque formation en sécurité privée inclura bientôt un module de « sensibilisation au terrorisme », d'environ 20 heures. De même, rappelons le lancement en début d'année 2016 de l'Observatoire des atteintes aux agents de sécurité privée, en partenariat avec l'INHESJ et l'ONDRP : il s'agit d'un dispositif de déclaration en ligne, sur la base du volontariat, des agressions physiques et morales dont sont victimes les agents de sécurité privée dans l'exercice de leurs missions. Cet Observatoire vise à mieux connaître les réalités, parfois risquées, des métiers de la sécurité privée.

Une doctrine de coproduction de la sécurité privée est désormais accessible et conceptualisable : « *A chacun sa place mais une place connue de chacun* » : c'est à ce prix que la coproduction sera efficiente, davantage que par un simple transfert d'une mission ou d'une compétence d'une structure (publique) de sécurité à une autre (privée). ■

POUR ALLER PLUS LOIN

LE CONSEIL NATIONAL DES ACTIVITÉS PRIVÉES DE SÉCURITÉ (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.*

http://www.cnaps-securite.fr/

REFONDER LA SÉCURITÉ PRIVÉE

Claude TARLET
Président de l'Alliance nationale des activités privées de sécurité (ANAPS)

Un nouveau contexte géopolitique

La France est au premier rang des pays occidentaux victimes du terrorisme (avec plus de 230 morts et 800 blessés depuis les attentats de janvier 2015 contre Charlie Hebdo).

Un fait majeur tend à modifier sensiblement l'environnement géopolitique : le Brexit, qui risque d'entraîner un éloignement des Britanniques.

Toutefois, si l'Union européenne peine encore à adopter des positions communes sur de nombreux sujets, force est de constater que la sécurité fait – heureusement – figure d'exception. Citoyens et gouvernements estiment en effet unanimement que la sécurité (intérieure et extérieure) est une priorité. Soyons à la hauteur !

Est-il besoin de rappeler l'impérative nécessité de créer une « Europe de la sécurité » ? L'Union des entreprises de sécurité privée (USP) l'avait d'ailleurs appelée de ses voeux dès 2008. Souvenons-nous du premier Sommet européen de la sécurité privée, à Paris, et du Livre Blanc édité en coopération avec l'INHES.

Aujourd'hui plus que jamais, nous souhaitons nous associer aux militaires, aux policiers et aux gendarmes qui demandent une coopération européenne toujours plus forte.

Des attentes fortes à l'égard de l'État

Tout a basculé depuis les attentats. Nous avons besoin d'un État au plus près des préoccupations des citoyens, au plus près du concret, plus dans l'opérationnel et moins dans le jargon administratif.

Les attentes sont grandes. Nous sommes prêts (comme nous l'avons déjà démontré à plusieurs reprises) à soutenir et accompagner l'État dans ses démarches.

Des attentes fortes (et non encore satisfaites) existent notamment en matière de *benchmark* (et de transposition de solutions efficaces dans nos pratiques) et à l'égard de notre système législatif. Le droit français est souvent à la traîne.

Concernant la transposition de solutions qui ont fait leurs preuves, je prendrai l'exemple des principaux services de sécurité qui ont évolué dans les aéroports, notamment israéliens ; ils utilisent beaucoup de physionomistes et moins d'équipements techniques ou technologiques.
Les deux sont parfaitement complémentaires.

Concernant les avancées technologiques, c'est souvent le droit qui en ralentit l'usage. C'est le cas pour l'utilisation des technologies de reconnaissance faciale et des LAPI.

La loi tendant à encadrer juridiquement l'utilisation de la reconnaissance faciale dans les enquêtes terroristes et à la prévention des attentats se fait attendre… L'identification de Mohamed ABRINI, « l'homme au chapeau » des attentats de Bruxelles, a été rendue possible grâce à un logiciel de reconnaissance faciale développé par le FBI. Dans le contexte de la lutte contre le terrorisme, pourquoi se priver d'une telle méthode ?

De nombreux pays, soucieux des libertés individuelles de leurs ressortissants, ont déjà expérimenté les dernières technologies en matière de sécurité et de biométrie faciale à des fins de lutte antiterroriste.

La lecture automatisée de plaques d'immatriculation (LAPI) est un procédé technique consistant à permettre la lecture aléatoire des plaques d'immatriculation. Ce procédé est notamment utilisé dans le cadre de la sécurité intérieure par les services de police et de gendarmerie nationale, ainsi que par les douanes.

Un incompréhensible éparpillement

Si les Européens ont bien compris que l'efficacité de la sécurité repose sur une coopération poussée et une réponse collective, cela ne suffit pas et la prise de conscience n'est pas encore suivie des faits attendus. La dimension nationale est fondamentale.

Mais comme le souligne Nicolas BAVEREZ à propos des services de renseignement, «*la France ne peut échapper à une profonde réorganisation*». Cette réorganisation vise notamment «*l'élaboration d'une stratégie globale de sécurité, aujourd'hui défaillante*».

Il rappelle l'intérêt de faire travailler ensemble le million de personnes qui coproduisent la sécurité en France, soulignant la nécessité de «*renforcer la formation et la déontologie des agents de sécurité privée*».

Agir et non subir

Je partage les propos de Nicolas BAVEREZ. Ces différents constats nous incitent à agir rapidement. Et je considère que la sécurité privée doit également procéder à une profonde réorganisation.

Une réorganisation qui repose sur deux mots d'ordre: confédération et excellence. L'excellence, qui doit animer notre démarche en matière de formation recrutement et de formation. C'est dans ce cadre que j'appelle à la création d'un Institut national de la Sécurité privée dans une concertation avec tous les acteurs concernés.

En contrepoint, il s'agit de proposer une nouvelle approche pour que les entreprises de sécurité privée puissent faire face aux nouvelles missions qui leur sont confiées. L'USP[1] (mais au-delà c'est toute une profession) demande notamment la création d'un cadre réglementaire précis.

La Confédération, aussi, s'impose désormais. Aujourd'hui, plus de 15 organisations «animent» notre secteur. Cet éparpillement est largement contreproductif.

Nous avons besoin d'une stratégie opérationnelle, efficace et exemplaire, incompatible avec les querelles de chapelle stériles.

Le temps de l'action collective est venu. L'Alliance Nationale des Activités Privées de Sécurité (Anaps) est un laboratoire qui a permis de fédérer 14 organisations et de réfléchir ensemble à la création d'une approche globale de la sécurité privée. Nous devons continuer encore et sortir de nos schémas anciens. Nous devons désormais renforcer encore cette démarche en créant cette Confédération de la sécurité privée. Un lieu unique de partage des idées et des compétences, un espace central qui permette la mutualisation des moyens de tous les acteurs en préservant les identités des métiers.

On doit être à la hauteur, c'est-à-dire lancer un plan stratégique opérationnel qui crée la différence, qui fait la démonstration à nos adhérents, à nos agents, à nos clients et à l'État, que dans les prochaines années, grâce à ce nouvel engagement, les acteurs de la sécurité privée pourront relever un certain nombre de défis, notamment en matière économique, d'emploi, de professionnalisation, et offrir des solutions intégrées et prédictives.

Cette exigence unitaire ne s'impose pas seulement aux acteurs de la surveillance humaine.

En clair, elle s'impose à tous. Alors, métier par métier, construisons cette unité de représentation que tout le monde appelle de ses vœux sans oser le dire.

Pourquoi? Parce que plus vite nous avancerons unis, plus vite nous serons connus et reconnus comme des acteurs à part entière. Or, en dépit des progrès réalisés ces dernières années, ce n'est pas encore le cas.

Tous attendent que nous nous comportions, aujourd'hui, avec responsabilité pour protéger nos infrastructures et nos concitoyens, en appui de la puissance publique.

La menace terroriste a changé la société française et ouvert le chemin à une nouvelle conscience collective.

Alors, nous aussi, bougeons les lignes et osons nous libérer de nos blocages pour nous transformer, collectivement, dans l'intérêt national, créer le lien de confiance avec l'opinion publique et tous les acteurs de la filière de la sécurité. ■

POUR ALLER PLUS LOIN

L'ANAPS

Créée le 17 janvier 2013, l'Anaps, Alliance nationale des activités privées de sécurité, regroupe quatorze organisations représentatives du secteur, toutes activités confondues: surveillance humaine, sécurité électronique, télésurveillance, transports de fonds et de valeurs, sûreté aéroportuaire, enquêtes privées, protection de personnes, conseil, formation.
http://www.anaps-securite.org/

UNE MOBILISATION IRRÉVERSIBLE DES AGENTS PRIVÉS DE SÉCURITÉ CONTRE LA TERREUR, MAIS À QUELLES CONDITIONS ?

Daniel WARFMAN
Directeur délégué de Trigion Sécurité - Groupe Facilicom

Les attentats du 13 novembre 2015 perpétrés en île-de-France ont eu une répercussion plus grande sur le sentiment d'insécurité dans la population que ceux du 7 janvier 2015, parce qu'ils n'ont pas visé une cible clairement identifiée (comme Charlie Hebdo) mais ont touché « tout le monde », sans distinction de religion, de race ou d'opinions.

Depuis l'attentat du 14 juillet 2016 à Nice, on a le sentiment que le terrorisme est désormais aveugle.

Alors que les services de sécurité de l'État (Police, Gendarmerie, Armée) et des collectivités (polices municipales), abondamment déployés pour rassurer la population, sont saturés et que beaucoup de leurs personnels sont « épuisés », le recours massif aux services de sécurité privée est apparu comme la solution d'évidence.

Décharger les services de l'État de tâches « indues » pour qu'ils puissent se recentrer sur des missions régaliennes n'est pas un slogan mais une réalité tangible. Le mot d'ordre en avait déjà été tenu, en son temps, par Charles PASQUA, alors ministre de l'Intérieur et de Robert PANDRAUD, ministre délégué à la Sécurité Publique, après la série d'attentats terroristes de septembre 1986 (bureau de poste de l'Hôtel-de-ville, *Pub Renault*, Préfecture de Paris, rue de Rennes), devant les représentants de la profession. C'est dans ce contexte que les décrets d'application de la loi fondatrice du 12 juillet 1983 (aujourd'hui le titre VI du Code de la Sécurité Intérieure) réglementant les activités privées de gardiennage, surveillance et transport de fonds, avaient été promulgués (les 26 septembre et 10 octobre 1986).

Et trente ans plus tard, dans un contexte identique, ce discours s'est imposé comme une évidence. On redécouvre la contribution de la sécurité privée à la sécurisation des cibles vulnérables. Mais, entre temps, ce secteur de services s'est largement structuré. L'évolution de la profession depuis les années 1980, sa structuration autour d'organisations professionnelles, le dispositif du CNAPS et la gestion des cartes professionnelles, la focalisation sur les besoins de formation, tendent à laisser encore plus de place à la sécurité privée générale, comme des segments spécifiques se sont structurés dans les services de sécurité aéroportuaire en 2001, après les attentats du 11 septembre.

C'est, sinon à cause du désengagement de l'État, mais de son incapacité à répondre exponentiellement aux besoins de sécurité en fonctionnaires, que de nouveaux postes privés se sont créés, fournissant ainsi des emplois de plus en plus pérennes.Cependant, malgré l'encadrement de ces activités spécifiques de surveillance, contrôle et filtrage, des dérives et des manquements ont été révélés.

On aurait pu penser que les aéroports, lieux particulièrement sécurisés où les contrôles sont multiples et possibles, et où les forces de l'ordre ne sont jamais loin, auraient été épargnés par les dérives et les manquements. Que dire alors des sites culturels, commerciaux, sportifs, cultuels, où des terroristes ayant changé de pratiques en font des cibles comme les autres, puisque de

l'attentat à la bouteille de gaz des années 1980, on est passé au kamikaze qui n'hésite pas à faire sauter sa ceinture d'explosifs. Dans ces conditions, et face à ce genre de menace, le service de veille et de vigilance assuré par des agents privés peut-il être dissuasif? Lors de la loi du 12 juillet 1983, comme lors de la discussion qui a donné naissance au CNAPS, à la carte professionnelle et au titre VI du Code de la Sécurité Intérieure, un mot d'ordre s'est imposé, celui des deux 2 piliers de la moralité et de la compétence.

- Les contrôles sur la «moralité» des agents restent une prérogative des services de l'État. Ils pourraient être plus « approfondis » comme ceux qui permettent de délivrer un badge d'accès aux zones réservées dans les aéroports.
  Ce contrôle, qui est assuré lors de l'obtention de la carte professionnelle, ou de l'entrée dans un organisme de formation, devrait être renouvelé systématiquement de manière périodique.

- En termes de compétence, la réglementation sur la formation et les organismes qui la dispensent évolue, mais c'est à l'évidence l'un des points sur lesquels il faut s'engager résolument beaucoup plus loin, dans la mesure où le «manque de compétence» des agents n'est souvent dicté que par une apparence de sécurité. Combien de fois a-t-on ouvert son sac devant un agent de sécurité qui a fait une «inspection visuelle» sans rien voir? Et à supposer qu'il ait vu quelque-chose de suspect, aurait-il pu l'identifier? Et à supposer qu'il ait vu et identifié quelque-chose, qu'aurait-il fait alors?

Une formation adéquate doit permettre à l'agent d'identifier le risque ou la menace et de réagir dans le cadre de procédures prédéfinies, qui doivent devenir des réflexes afin d'atteindre un niveau de sûreté acceptable.

Encore faut-il que les dispositifs de protection mécanique (portes, grilles,…) soient judicieusement implantés et opérationnels dès la survenance d'une attaque. Il est évident que la moralité et la compétence des agents de contrôle ne sont pas seules en cause, car plus problématiques encore sont celles de leurs encadrants directs.

Le *middle-management* des entreprises de sécurité privée n'est pas soumis à l'obtention d'une carte professionnelle. Pourtant, dans la période récente, on a vu des «encadrants» procéder eux-mêmes aux palpations de sécurité. De quel droit? Avec quel contrôle? Avec quelle formation? Ce personnel d'encadrement devrait être soumis aux mêmes critères que les agents: moralité et compétence.

Il est d'ailleurs troublant de constater que des étudiants inscrits en «licence professionnelle des métiers de la sécurité» ou en master «risques», s'ils acquièrent bien une certaine compétence, ne sont soumis à aucun contrôle de moralité, si ce n'est *a posteriori* de leur formation, s'ils décident d'obtenir l'agrément du dirigeant délivré par le CNAPS.

Du côté de l'exploitation et des services «de terrain», les «stocks» d'agents de sécurité dans les entreprises privées ne sont pas «inépuisables», d'autant que le contingent d'heures supplémentaires est limité et très coûteux.

Dans un contexte politique ayant décrété l'état d'urgence, où la mobilisation des forces se fait dans la précipitation, les entreprises de sécurité privée ne savent pas «recruter». Bien entendu, elles peuvent toujours trouver des candidats «en règle», détenteurs de la carte professionnelle attestant leurs compétences dans le domaine, mais la question se pose pour ceux qui les mobilisent de savoir sous quel statut ils les embauchent ? Cela ne va pas de soi. En CDI? Mais on ne sait pas jusqu'à quand ça va durer, et après… En CDD? Mais là non plus, on ne connaît pas la fin… Face à de telles incertitudes, et en l'absence d'une notion de «contrat de chantier» ou de «contrat de mission», les entreprises prestataires sous-traitent. Pourquoi est-ce possible et peut-on s'en accommoder? Les salariés des sous-traitants travaillent dans une entreprise qui est leur employeur principal et de fait, ils effectuent leurs 35 heures (en fait 36 heures = 3 services de 12 heures) en 3 jours. Il leur reste 4 jours pour aller travailler ailleurs… ils vont donc trouver un emploi complémentaire dans cette autre entreprise sous-traitante.

Cette dernière emploie ces salariés dans le cadre de contrats de travail, en heures normales, et non pas en heures supplémentaires…

Quand la demande du donneur d'ordres diminue ou s'arrête, l'entreprise de sécurité privée met un terme au contrat commercial avec le sous-traitant, charge à ce dernier de trouver une solution avec ses salariés. Mais comme beaucoup de ces derniers ont déjà un double emploi, ils se contentent de leur emploi principal dans l'attente de nouvelles missions complémentaires. Ce problème de volume fluctuant de prestations, qui impacte le prestataire en termes financiers (montée ou baisse du chiffre d'affaires, besoin en Fonds de Roulement) et en termes de gestion des ressources humaines (effectifs), perturbe également la gestion des donneurs d'ordres.

Il faut bien rester conscient que la montée en puissance du passage d'un palier à l'autre, dicté par l'État (du « Temps de Paix » [qui n'existera certainement plus] à «Vigipirate Vigilance»; de «Vigipirate Vigilance » à «Vigipirate Attentat»; de «Vigipirate Attentat» à «Vigipirate État d'Urgence»), représente un coût souvent difficilement supportable pour les entreprises. Or, la décision de redescendre de niveau est également très difficile à prendre. Car la prise de responsabilité est douloureusement ressentie comme un dilemme: en effet, que se passerait-il si, le lendemain d'une «baisse de vigilance», survenait un nouvel attentat?

C'est alors que de nouvelles fonctions ou «solutions» apparaissent dans les métiers de la sécurité privée. Les conditions d'emploi des agents de surveillance renforcée (gardes armés) sont déjà autorisées. Les sites «protégés» vont devoir faire l'objet d'aménagements…

Les conditions «techniques» de l'armement des agents vont se différencier de celles des convoyeurs de fonds (stockage des armes, équipements… et se posera la question de savoir si cela aura lieu chez le client?).

Aujourd'hui, plus que jamais, les entreprises de sécurité privée ont un vrai rôle de conseil et de mise en place de prestations qui sont en réelle cohérence avec la typologie des lieux, des personnels, des visiteurs, des activités, et des procédures. C'est au *middle management* responsable qu'il revient d'anticiper, en concertation avec les donneurs d'ordre et les pouvoirs publics, de toutes les implications du partage des responsabilités dans la mise en protection des sites et des hommes dans des stratégies anti terroristes… ■

LA SÉCURITÉ PRIVÉE EN CHIFFRES – ZONE EUROPE GÉOGRAPHIQUE

Source : Les données sont extraites d'une étude en cours, conduite par la société LPN,
réalisée et complétée sur la base des études menées par la CoESS (Confédération européenne des services de sécurité)
LPN est la première société en France à avoir été autorisée à déployer des agents de surveillance renforcée depuis juin 2015.
Les données ne sont pas encore disponibles concernant les pays suivants :
Chypre, Finlande, France, Grèce, Lituanie, Macédoine, Portugal, Slovaquie, République Tchèque.

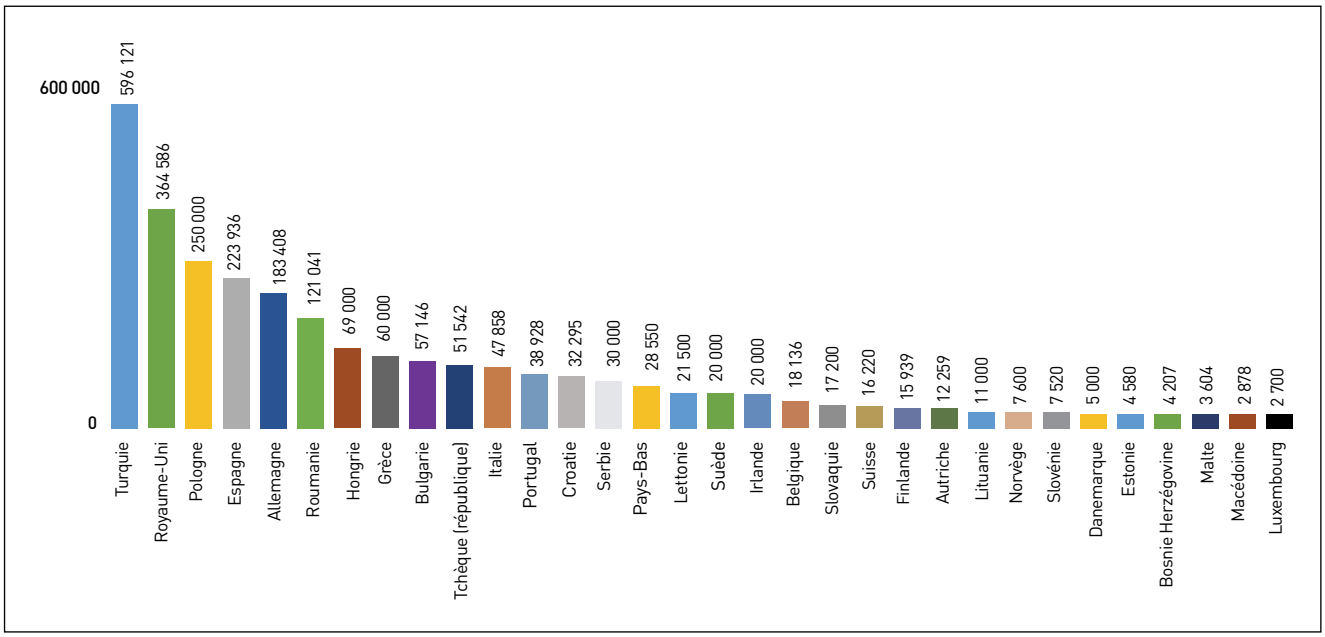
www.securite-protection-risque.com

Le recours à la sécurité privée est en nette augmentation en France depuis janvier 2015. Au premier semestre de 2016, l'INSEE a ainsi noté une augmentation de 3,9 % des activités liées aux systèmes de sécurité et de 3,3 % des activités de sécurité privée, pour un chiffre d'affaire qui s'élève à 8,3 milliards d'euros pour le secteur en 2015[1]. Les enjeux d'avenir pour ce secteur portent notamment sur l'armement des agents. Cette question est aujourd'hui une des priorités de l'État : des textes devraient aboutir à des clarifications concernant l'armement des agents privés de sécurité en France.

Le CNAPS joue un rôle déterminant concernant la formation spécifique de ces agents. Il a notamment travaillé sur la création d'un nouveau statut d'«Agent de Surveillance Renforcée». Certains agents font déjà l'objet d'autorisations de port d'arme délivrées par la Préfecture, dans le cadre de la protection des sites les plus exposés.

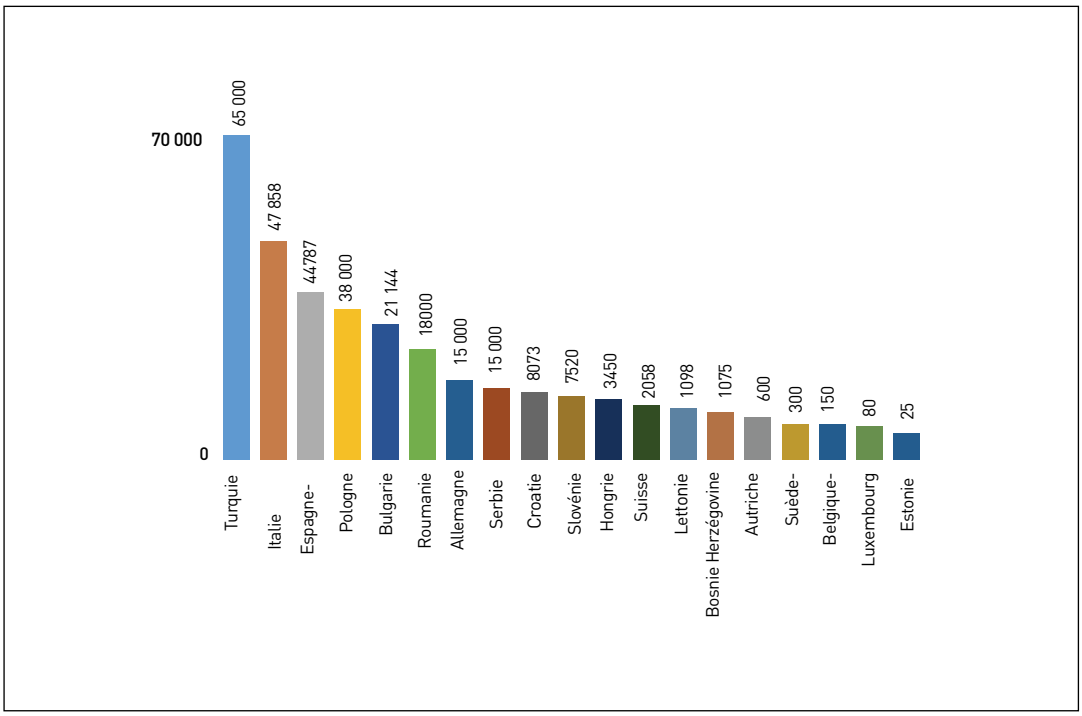
D'autres pays ont recours aux services d'agents de sécurité armés. L'observation des chiffres ci-dessous permet d'avoir une lecture comparée, entre pays de l'Europe géographique, sur le nombre d'agents privés de sécurité armés (APSA) et non armés».

NOMBRE TOTAL DES AGENTS PRIVÉS DE SÉCURITÉ DANS CHAQUE PAYS



(1) Source INSEE : http://www.insee.fr/fr/themes/document.asp?ref_id=if66#inter2

NOMBRE D'AGENTS PRIVÉS DE SÉCURITÉ ARMÉS (APSA) DANS LES PAYS EUROPÉENS



Les ASPA ne sont pas autorisés dans les pays suivants: Danemark, Irlande, Malte, Norvège, Pays-Bas, Royaume-Uni.

Parmi les pays référencés, c'est la Turquie qui possède le plus d'agents privés de sécurité, soit, 591 121. 65 000 d'entre eux sont autorisés à porter une arme.

L'Italie compte 47 858 agents de sécurité privés. L'intégralité des agents sont autorisés à porter une arme. Elle est le seul pays avec la Slovénie, parmi les pays référencés, à posséder 100 pour-cent d'ASPA.

En Espagne, 20 % des 223 936 agents de sécurité sont des ASPA. Ces derniers sont au total 44 787.

L'Allemagne seuls 8,17 % d'entre eux sont des ASPA (15 000). Sur les 18 136 agents de sécurité Belges, les ASPA sont au nombre de 150, soit 0,82 %.

Discours de
BERNARD CAZENEUVE

*ministre de l'Intérieur**

Le lundi 5 décembre 2016 - école militaire - PARIS

Quatrièmes Assises de la sécurité privée

* Premier ministre depuis le 06 décembre 2016

Messieurs les Préfets,

Messieurs les directeurs, Mesdames les directrices,

Mesdames et Messieurs,

Il y a deux ans, j'ai eu le plaisir d'inaugurer, dans ce même amphithéâtre, les troisièmes Assises de la sécurité privée. Nous savions alors que d'importants chantiers devaient être menés à bien. Beaucoup ont abouti ou sont en voie de l'être. Mais surtout, depuis deux ans, notre pays a été confronté à la barbarie terroriste, qui a modifié en profondeur la conception que les Français se font de la sécurité.

Comme tous nos concitoyens, je ne pourrai jamais oublier les vies brisées et les familles déchirées des victimes de ces attentats odieux. Mais j'ai aussi pu admirer l'extraordinaire résilience du peuple français, qui, face au fanatisme et à l'horreur, reste fidèle à ses valeurs.

Dans ce contexte de crise, l'État a apporté des réponses immédiates. Je fais évidemment allusion à la mise en œuvre de l'état d'urgence, au soir du 13 novembre 2015, qui mobilise l'ensemble des services du ministère. Je pense aussi aux efforts budgétaires exceptionnels en faveur des forces de sécurité, pour les doter en équipements nouveaux, et à la rapide montée en puissance des dispositifs de recrutement et de formation de la Police et de la Gendarmerie nationales.

La sécurité privée a elle aussi assumé ses responsabilités, dans les domaines qui sont les siens. Elle a eu ses héros : ces agents du Stade de France qui, au péril de leur vie, ont barré la voie aux terroristes ; cet employé du Bataclan – DIDI - qui a porté secours aux spectateurs, en courant sous les balles pour ouvrir l'issue de secours et dont j'ai eu le plaisir de présider la cérémonie de naturalisation à l'Hôtel Beauvau en mai dernier.

Ces drames nous ont enseigné que pour protéger les Français, les différents acteurs de la sécurité devaient s'engager résolument dans la voie de la coopération. Cela exige d'eux une très grande rigueur dans la répartition des rôles, car la coproduction de sécurité n'est en rien une confusion des sécurités. Chaque acteur, Police et Gendarmerie nationales, polices municipales et sociétés de sécurité privée, doit intervenir dans son champ de compétences spécifique, en tendant vers davantage de complémentarité et des échanges d'informations toujours plus fluides.

La sécurisation du marché de Noël de Strasbourg, dont Robert HERMANN, Président de l'Eurométropole, vous parlera cet après-midi, est menée dans cet esprit.

Mesdames et Messieurs, les exigences qui pèsent sur nous sont très élevées. Quelles que soient les difficultés que nous pourrions être amenés à rencontrer, le souci de l'intérêt général doit prévaloir sur toute autre considération.

* * *

Les résultats d'exercice des deux dernières années traduisent ainsi une forte hausse de l'activité de vos entreprises, qui ont bénéficié de deux mesures phares : le CICE et la taxe dite CNAPS, qui a notablement renforcé cet opérateur.

Au-delà de ces résultats comptables, les entreprises de sécurité privée ont su relever un défi qualitatif, en contribuant à la sécurisation de l'Euro 2016. Ce sont pas moins de 13 000 agents qui ont été déployés sur les différents sites de la compétition. La France a ainsi fait la preuve qu'elle disposait d'un haut niveau de compétence dans le domaine de la sécurisation des grands événements, ce qui sera pris en compte, je l'espère, lors de la sélection du pays d'accueil des JO 2024 et de l'Exposition universelle de 2025.

Plus généralement, votre secteur a su répondre ces derniers mois aux besoins de nouveaux clients, notamment des collectivités territoriales, qui vous ont sollicités en urgence pour sécuriser des événements publics. J'avais évoqué ici la nécessité de créer des outils destinés à vous aider sur ce type de déploiements. Avec la circulaire du 5 janvier 2016, relative aux **conventions locales de coopérations de sécurité**, c'est chose faite. Ce dispositif souple et pragmatique facilite les échanges d'informations, dans le strict respect des compétences de chacun.

Ces deux dernières années, vous avez aussi mené d'importants chantiers d'amélioration des conditions de travail. Je pense tout particulièrement à l'**accord de branche**, signé par l'ensemble des partenaires sociaux, et au **développement de la formation des agents**. Ces dispositions participent à l'accroissement de l'attractivité de votre secteur auprès de candidats de qualité.

Vous savez par ailleurs que **la formation est désormais strictement contrôlée**, dans le cadre d'un régime introduit par la loi du 17 août 2015, qui a aussi créé une obligation de formation continue. En contrepartie, les sociétés de formation à la sécurité

privée ont été soumises aux mêmes exigences que les entreprises prestataires, ce qui écarte de fait du marché les officines douteuses. L'actualisation de cinq des certifications de qualification professionnelle et la définition d'étapes obligatoires de formation continue ont contribué elles aussi à cette dynamique globale de professionnalisation.

Je me félicite aussi que vous ayez mis sur pied un **système de contrôle des profils** de vos agents, qui vous a permis d'examiner, sur la seule année 2015, les situations individuelles de plus de 3 500 salariés. L'accès au fichier TAJ accordé à votre autorité de contrôle a porté ses fruits et ne soulève plus de contestations, pas plus que la possibilité donnée au CNAPS d'échanger des informations avec les services en charge de la lutte contre le travail illégal. Ce sont là des exigences incontournables pour assurer votre légitimité aux yeux des Français.

J'insiste en revanche sur la nécessité, pour les services de police et de gendarmerie, de pouvoir vérifier en toute circonstance l'appartenance professionnelle d'un individu qui se revendiquerait d'une de vos sociétés. Cela devrait être facilité par la **dématérialisation des cartes professionnelles**, préparée actuellement par le CNAPS, en vue d'en faire un outil rapidement actualisable.

Outre ces avancées importantes, je constate que vous travaillez activement à anticiper les exigences de demain, en investissant dans **les nouvelles technologies de sécurité**. Avec le développement des caméras intelligentes et des algorithmes prédictifs, de nouveaux défis technologiques se présentent constamment à nous. J'entends donc que le ministère de l'Intérieur continue à soutenir les *start-ups* françaises innovantes dans toutes ces spécialités, via la Délégation ministérielle aux industries de sécurité et aux cyber-menaces (DMSIC), et en s'appuyant sur le réseau de professionnels du Conseil des industriels de la confiance et de la sécurité (CICS).

À ce titre, je tiens à saluer les efforts des **professions les plus exposées**, notamment des transporteurs de fonds, des bijoutiers et des buralistes, qui se trouvent souvent en première ligne face à des actions de plus en plus déterminées de grande délinquance. Les réflexions collectives de ces professionnels – et je pense en particulier à l'association PERIFEM -, leur recherche constante de produits de défense ou de marquage des produits, qui rendent de grands services aux enquêteurs, contribuent incontestablement à la lutte contre l'insécurité.

Par ailleurs, nombre d'entre vous avez investi à juste titre dans **la vidéo-protection**. L'État s'y emploie lui aussi, en soutenant, par le biais du FIPDR, les demandes d'équipements des collectivités territoriales, et en déployant les réseaux de surveillance des établissements scolaires et des zones touristiques.

* * *

Mesdames, messieurs, d'importants progrès ont été accomplis depuis notre dernière réunion. Cependant beaucoup reste à faire.

Il nous faut pour cela dépasser la temporalité de l'action immédiate et mener des réflexions de fond sur nos enjeux communs. C'est à cet effet que j'ai installé au mois d'octobre, au sein du ministère, un **Conseil de la stratégie et de la prospective**, où praticiens et universitaires évaluent les politiques publiques de sécurité, pour que nous préparions ensemble notre efficacité de demain.

Parmi ces enjeux d'avenir, la **question de l'armement de certains de vos agents doit être étudiée sérieusement, en prenant en compte les enjeux opérationnels mais également les conséquences en termes de choix de société**. C'est pourquoi alors que, vous le savez, des textes sont en préparation et que d'autres sont prêts, j'estime qu'il doit revenir à la représentation nationale d'en débattre et de se prononcer sur leur adoption. C'est une obligation démocratique qui n'en légitimera que plus les choix ainsi opérés.

Une chose est certaine : ces différentes mesures, dont il faut aujourd'hui envisager l'adoption sont le fruit des efforts que vous avez consentis en matière de formation et de professionnalisation de vos agents. C'est un très grand succès, dont vos représentants doivent être vivement remerciés.

Je crois d'ailleurs qu'ils ont raison de vouloir améliorer encore la formation et l'information de vos personnels.

C'est ainsi que j'ai récemment entendu des appels à la création d'un « **Institut National de la Sécurité Privée** ». Je conçois tout à fait l'utilité d'un tel projet. Vos métiers ne peuvent travailler en vase clos, ils ont besoin d'une plateforme qui soit aussi bien un lieu d'échanges entre professionnels qu'une source d'informations sur les faits sociaux et économiques qui régissent votre activité.

Toutefois, cette maison que vous appelez de vos voeux se doit d'être la vôtre, et donc d'être conçue en premier lieu par des représentants de votre profession. Aussi, je souhaite qu'au cours du premier semestre 2017, ils dessinent les grandes lignes de ce projet, en décident le lieu d'implantation et le mode de financement, et déterminent s'il faut ou non l'adosser à une structure déjà existante. À mon sens, un tel Institut devrait s'engager sur le volet pédagogique de la formation, mais aussi oeuvrer à l'émergence d'un véritable encadrement intermédiaire. Je demande à la Délégation aux Coopérations de Sécurité d'effectuer un suivi de ces travaux et de m'en adresser régulièrement la synthèse.

Je veux d'ailleurs souligner l'importance que j'attache au développement de la formation continue, qui conditionne l'indispensable montée en compétence de la sécurité privée. C'est pourquoi j'ai souhaité que le renouvellement de la carte professionnelle soit lié à **l'obligation de suivre un cycle de formation continue,** qui pourrait se composer d'un module commun à tous les agents, complété par des modules spécialisés en fonction de leur cursus. Je souhaite notamment qu'un module de sensibilisation aux menaces terroristes soit accessible à tous, ainsi qu'un module consacré au sauvetage et au secourisme au travail (SST). J'entends que d'ici le 15 décembre, une solution prenant en compte les situations individuelles des agents soit proposée, conformément aux engagements pris devant les organisations professionnelles. En ce qui concerne la nécessité d'accompagner les efforts de formation à moyen terme, j'ai bien entendu le souhait de mettre en place un fond de modernisation dont le financement pourrait être assis sur une fraction de la taxe qui finance le CNAPS. Je demande à ce que les parties prenantes, la profession, le CNAPS et la délégation étudient avec le ministère du budget les modalités de sa création et surtout arrêtent ses orientations.

Toujours au titre de cette exigence de formation, vous avez raison de vouloir être informés de l'**évolution des menaces** qui pèsent sur notre pays. Je souhaite donc que chaque responsable de société de sécurité ait, au sein de la Police ou de la Gendarmerie, un interlocuteur attitré qui puisse répondre à ses interrogations. En outre, j'ai demandé à mes services de construire des modules de sensibilisation à la détection des signaux faibles, à l'intention des cadres de votre secteur.

Dans le même esprit, vous êtes sans doute informés de la mise en place, à titre d'expérimentation, du **dispositif Vigie** dans le quartier de La Défense. Ce dispositif associe, à travers différents modules d'information, les personnels de sécurité privée à la lutte contre le terrorisme, de manière à ce que tous les acteurs de la sécurité développent des réflexes et un langage commun. Je demanderai sous peu à la DGPN et à la DCS de dresser un premier bilan de cette expérience intéressante à plus d'un titre.

J'entends aussi vos inquiétudes sur le cadre juridique futur de vos activités. Je sais notamment que vous vous interrogez sur l'évolution de votre **périmètre d'action sur la voie publique**. Je n'évoque pas là vos missions de filtrage-palpation à l'occasion d'événements sportifs ou culturels, car celles-ci s'inscrivent dans un cadre juridique clair, celui de la privatisation temporaire de la voie publique. En revanche, il serait nécessaire de passer par la loi pour repenser votre périmètre d'action autour des bâtiments dont vous avez la garde. Les services de la DLPAJ se sont saisis de cette problématique et me rendront un premier rapport d'étape sur cette question en début d'année prochaine.

Par ailleurs, j'entends vos préoccupations face à une possible **ubérisation de la sécurité privée**, rendue possible par la mise en contact directe, sur des plateformes numériques, de demandeurs de prestations de sécurité et d'agents susceptibles d'y répondre. Le CNAPS a récemment consacré un très intéressant colloque à ce sujet.

Il faut bien constater qu'un nouveau marché de services de **sécurité privée sollicitée en urgence** est en train de se dessiner. Je n'y suis pas hostile *a priori*, mais ma position est très claire : aucun intervenant nouveau dans le champ de la sécurité privée ne doit pouvoir s'affranchir des dispositions réglementaires propres à cette activité, et il n'est pas envisageable d'autoriser une course au moins-disant, qui favoriserait le travail clandestin. Je souhaite, sur ce point aussi, que le CNAPS et la délégation puissent formuler des propositions d'ici la fin du premier trimestre 2017.

Enfin, je pense qu'il est temps de tirer tous les enseignements de votre implication quotidienne dans la sécurité de notre pays, telle qu'elle a été définie par la loi d'orientation et de programmation du 21 janvier 1995. Opérateurs publics et privés travaillent désormais en confiance. Il me paraît donc très naturel d'instaurer l'**obligation de signalement** pour un agent de sécurité privé témoin d'un acte délictueux violent, que j'appelais déjà de mes voeux il y a deux ans. Mon intention n'est pas de détourner vos agents de leurs missions, mais de leur donner la place qui leur revient dans notre dispositif de sécurité. En contrepartie, je souhaite qu'ils puissent **bénéficier d'un régime de circonstances aggravantes** particulières, dans le cas où ils seraient victimes d'une agression.

* * *

Mesdames et Messieurs, vous n'adhérez sans doute pas tous à chacune des mesures que je viens d'évoquer, mais vous reconnaissez, je pense, qu'elles constituent un ensemble cohérent. Sachez en tout cas que je ne dévierai pas de ma position concernant l'apport de la sécurité privée à la politique globale de sécurité de notre pays.

La sécurité reste bien évidemment en premier lieu **une compétence de l'état**, qui ne peut se défausser de ses responsabilités sur les acteurs privés.

En revanche, je crois plus que jamais à **la nécessité d'un décloisonnement des cultures** entre les différents cercles de la sécurité. Je n'oublie pas, à ce propos, le rôle du citoyen, dont l'implication vigilante nous est de plus en plus précieuse.

Enfin, j'ai la conviction que **la démarche entreprise depuis cinq ans est la bonne**. En mettant en place un mécanisme d'agrément et de contrôle, l'État pousse les entreprises de sécurité privée à s'organiser. Je sais que d'autres professions intervenant dans la sphère de la sécurité souhaitent à leur tour être éligibles à un tel processus. J'invite le délégué aux Coopérations de Sécurité à me faire des propositions sur ce point avant la fin du prochain trimestre.

Mesdames, Messieurs, les Français attendent beaucoup de nous. Ils veulent que nous assurions leur sécurité, dans le strict respect de l'État de droit, et que nous nous organisions en conséquence face aux nouvelles menaces qui pèsent sur eux. Avec vos 160 000 agents, je sais que vous serez à la hauteur de ces attentes.

Je vous souhaite une très bonne journée de travaux et vous remercie. ■

IMPACTS ET RÉPONSES

Quelles responsabilités pour l'entreprise?

- La responsabilité de l'employeur face à la menace terroriste
  Olivier HASSID, *Directeur chez PwC, Expert en sécurité & sûreté*
- Menace terroriste : quel est le risque pour l'entreprise en droit du travail et comment le limiter ?
  Christine PELLISSIER, *Avocat en droit du travail – Directeur associé, Cabinet FIDAL*
- L'entreprise et les salariés victimes d'attentats
  Général Louis CROCQ, *Médecin Général (CR) , psychiatre des armées, créateur du réseau national des cellules d'urgence médico-psychologique*

Fait religieux et radicalisation djihadiste : le tabou est-il brisé ?

- La « radicalisation » en entreprise
  Mustapha BENCHENANE, Docteur d'État en Science Politique, Conférencier au Collège de Défense de l'OTAN
- L'entreprise n'est ni laïque ni religieuse mais commerciale
  Éric MANCA, *Avocat associé August and Debouzy*
- Quel est le meilleur endroit en France pour réussir le « vivre-ensemble » ?
  Thomas BOUVATIER, *Psychanalyste*
- La charte de la laïcité et de la diversité
  Claude SOLARZ, *Vice-Président du Groupe PAPREC*
- De la délinquance à la radicalisation djihadiste
  Entretien avec **François PUPPONI**, *Député Maire de Sarcelles*

Témoignages... Maintenir les activités : à quels prix ?

- **Alain ZABULON,** *Directeur de la Sûreté, du Management des Risques et de la conformité – ADP*
- **Stéphane GOUAUD,** *Directeur de la Sécurité – RATP*
- **Jean-Louis FIAMENGHI**, *Directeur de la sûreté – VEOLIA*
- **Patrick ESPAGNOL,** *Préfet, Directeur sûreté et IE – EDF*
- **Ziad KHOURY,** *Ex-directeur de la sûreté – Euro 2016 SAS*
- **Jean-Claude CATHALAN,** *Président du Comité MONTAIGNE*
- **Franck CHARTON,** *Délégué général – PERIFEM*
- **Sophie HUBERSON,** *Déléguée générale – SNELAC*

Technologie et sécurité

- La protection des données personnelles, un atout pour les entreprises
  Edouard GEFFRAY, *Secrétaire général de la CNIL*
- Sécurité publique et protection des données
  Béatrice OEUVRARD, *Juriste Senior chez Microsoft France, responsable des affaires BtoC*
- Les entreprises : victimes de la consumérisation des cyberattaques
  Nicolas ARPAGIAN, *Directeur scientifique du Cycle « Sécurité des usages numériques» de l'INHESJ*
- #terrorisme. L'entreprise face au terrorisme à l'heure de Twitter
  Emma VILLARD, *Regional Security Advisor at ANDRITZ*

LA RESPONSABILITÉ DE L'EMPLOYEUR FACE À LA MENACE TERRORISTE

Olivier HASSID
Directeur chez PwC, Expert en sécurité & sûreté

La menace terroriste en France est à la fois élevée, polymorphe et non discriminante. Élevée, cela ne semble faire guère de doute. Dans son rapport paru en juillet 2016, Europol note que les services de police français ont arrêté en un an plus de suspects de cas de terrorisme que tous les services de police de tous les autres pays de l'Union européenne cumulés (366 personnes arrêtées en 2015 contre 75 en Espagne, 21 en Allemagne…) 1. Elle est polymorphe, car elle peut se traduire aussi bien par une attaque à la bombe dans des transports collectifs que par une prise d'otage dans un centre commercial ou une tuerie de masse au siège d'une entreprise. Enfin, la menace terroriste est non discriminante, ou tout du moins le semble-t-elle, car elle peut prendre pour cible aussi bien un prêtre dans une église, que des élèves dans une école ou bien un dirigeant d'entreprise.

Il paraît donc difficile de la prévenir si ce n'est en renforçant nos services de renseignement et en augmentant les moyens de la police et de la gendarmerie nationale. Or, cette logique de moyens croissants à laquelle on assiste depuis des années est-elle vraiment efficace et efficiente ? Dans certains cas, elle l'est. Comme nous le mentionnions plus haut, les services de police français ont réussi la prouesse d'arrêter un grand nombre de suspects avant qu'ils ne passent à l'acte. En revanche, à la question « *pourrait-on collectivement faire mieux ?* », la réponse est indubitablement positive.

Sur la base de constats empiriques et de travaux criminologiques récents, il ressort que le dispositif global français repose encore trop sur une approche en termes de moyens étatiques. Autrement dit, la collectivité attend que l'État puisse régler seul cette question. Or, cette position ne peut plus raisonnablement tenir aujourd'hui. L'idée que l'État aurait le monopole de la sécurité nationale est non seulement fallacieuse, mais elle est aussi dangereuse. Tout décideur, qu'il soit public ou privé, tout responsable d'institution, tout garant de lieux publics ou privés a sa responsabilité dans la sécurité nationale. Un chef d'établissement scolaire, le PDG d'une entreprise ou encore l'organisateur d'une manifestation publique ne peut ignorer qu'il a un rôle à jouer dans la prévention des actes de terrorisme.

En effet, il a pour responsabilité de s'assurer que le ou les sites qu'il gère sont bien protégés face à la menace terroriste, et ce de différentes manières. Premièrement, il doit avoir une bonne connaissance de ses risques et vulnérabilités en s'interrogeant : « *Un terroriste pourrait-il agir dans mon établissement, et si oui comment ?* » Autrement dit, avant de mettre en place des moyens en termes de surveillance humaine et de technologie de sécurité, il convient de réaliser une bonne analyse des risques et de définir les différents scenarii de crises envisageables. Ce travail ne peut se faire sans avoir collecté, au préalable, un minimum de renseignements sur son environnement.

Deuxièmement, après avoir identifié qu'effectivement certains sites pouvaient être vulnérables et exposés à une attaque, il doit se demander comment les protéger de manière adaptée. La meilleure protection d'un site ne se décide pas au sommet de l'État, mais par des professionnels

(1) *European Union terrorism situation and trend report 2016*, 20 juillet 2016.

de la sécurité sur le terrain. Ceux-ci analysent un site, ses vulnérabilités et les risques associés. Puis ils conçoivent un plan de protection auquel ils associent des moyens de prévention (surveillance humaine, système de vidéosurveillance…).

Enfin, il doit s'interroger sur la nécessité de pérenniser une organisation de la sécurité en interne. Si la menace qui concerne ses sites est forte et permanente, il est préférable d'étudier le recrutement d'un directeur de la sécurité et de la sûreté capable de prévenir les risques terroristes qui peuvent les affecter. Précisons que la menace terroriste ne repose pas uniquement sur une attaque terroriste extérieure, elle peut aussi provenir du personnel même de l'entreprise.

GIGN PRISE D'OTAGES A DAMMARTIN EN GOELE 121

Un directeur de la sécurité et de la sûreté doit donc également apprendre à gérer, en collaboration avec le directeur des ressources humaines, le risque de radicalisation de certains employés.

S'il est évident que le risque zéro n'existe pas, la mise en place à la fois d'analyses de risques et des moyens associés permet de limiter ces risques et d'apporter une réponse rapide en cas de crise. Or encore actuellement de nombreux dirigeants, même s'ils ont conscience du problème, restent négligents. Cependant, à nos sens, plusieurs facteurs peuvent amener ces mêmes dirigeants à se responsabiliser.

Tout d'abord, parce que la responsabilité de l'employeur peut être engagée. Dans le cadre des arrêts de la Cour de Cassation du 28 février 2002, la Chambre sociale a défini la faute inexcusable de l'employeur en faisant référence à l'obligation de sécurité découlant du contrat de travail. «*Le manquement à cette obligation a le caractère d'une faute inexcusable, au sens de l'article L 452-1 du Code de la sécurité sociale, lorsque l'employeur avait, ou aurait dû avoir conscience du danger auquel était exposé le salarié, et qu'il n'a pas pris les mesures nécessaires pour l'en préserver*». Dans cette perspective, il ne paraîtrait pas absurde que la responsabilité de l'employeur soit recherchée si ce dernier n'a pas mis de mesures préventives pour faire face à la menace terroriste sur le sol national. Dans un contexte où le plan Vigipirate est maintenu à un niveau élevé (et que tout chef d'établissement ne peut l'ignorer[2]), il pourrait être considéré comme inexcusable qu'un chef d'entreprise n'ait pas mis en place une organisation de la sûreté au sein de son entreprise avec un directeur de la sûreté, des correspondants locaux, des politiques de sûreté, des dispositifs de prévention situationnelle… À ce titre, dans un arrêt du 26 mai 2016, il est rappelé que l'employeur doit protéger la santé physique et mentale des travailleurs, la pénibilité mais également la violence au travail[3]. Or, encore actuellement, de nombreuses entreprises ne disposent pas d'un dispositif de sûreté adapté aux enjeux provoqués par le terrorisme.

Ensuite, un acte terroriste au sein d'un établissement peut impliquer des dommages corporels, il peut également impliquer des dommages matériels extrêmement importants. Rappelons que les frais occasionnés par les attentats du *Word Trade Center* ont entraîné des dizaines de milliards de dollars de coûts. Les préjudices matériels sont dédommagés par les assureurs «habitation» des biens concernés, grâce à la «garantie attentats et actes terroristes». Cette couverture indemnise les victimes des dégradations provoquées par un attentat ou un sabotage. Si aujourd'hui le cas ne s'est pas encore présenté en France, on peut se demander ce que ferait un assureur face à un assuré victime d'un acte terroriste et qui a été négligent face à la menace alors qu'il avait conscience d'être une cible. Outre la responsabilité civile et pénale de l'employeur, ce dernier pourrait se voir refuser par son assureur d'être remboursé des dégâts occasionnés.

En conclusion, la prévention de l'acte terroriste ne repose pas, comme de nombreux chefs d'établissement le pensent encore, sur la seule responsabilité des services de police. Les dirigeants d'entreprise ont une responsabilité et doivent s'engager pour assurer un dispositif de sûreté adapté aux niveaux de menaces auxquels leur entreprise est confrontée. Si cette position paraît évidente, dans la réalité, les choses sont moins simples. Des entreprises qui sont pourtant confrontées à des problématiques de radicalisation ou qui sont visées en raison de leur activité, n'ont pas toujours le dispositif qui convient. Il reste dans ces conditions à espérer que les pressions légales et assurantielles disciplineront certains chefs d'entreprise qui font cavaliers libres… ■

(2) Partie publique du Plan gouvernementale de vigilance et de protection face aux menaces d'actions terroristes, Vigipirate, n°650/SGDSN/PSN/PSE du 17 janvier 2014.

(3) Cour de cassation, chambre sociale, arrêt du 26 mai 2016 : RG n°14-15566.

MENACE TERRORISTE QUEL EST LE RISQUE POUR L'ENTREPRISE EN DROIT DU TRAVAIL ET COMMENT LE LIMITER ?

Christine PELLISSIER
Avocat en droit du travail - Directeur associé - Cabinet FIDAL

Il y a presque quinze ans, le législateur, en intégrant dans le Code du travail l'Article L4121-1 toujours d'actualité, imposait à l'entreprise l'obligation générale de prendre toute mesure en vue d'assurer la sécurité et de protéger la santé physique et mentale de ses salariés. Le manquement à cette obligation entraînait la responsabilité de l'entreprise.

Rapidement, les juges ont qualifié cette obligation de sécurité d'obligation de résultat, signifiant par cela que l'employeur ne pouvait se contenter de fournir ses meilleurs efforts pour préserver la santé des salariés mais devait réussir dans cette entreprise.

Devant les juges prud'homaux, l'obligation de sécurité a connu de multiples illustrations dans les contentieux rendus en matière de harcèlement moral. Le manquement à cette obligation a également été reconnu en matière d'accident du travail[1] sans que toutefois l'existence d'un accident du travail soit une condition nécessaire à la reconnaissance de la responsabilité de l'employeur. Devant les juridictions de sécurité sociale, elle ouvre la porte à la reconnaissance d'une faute inexcusable de l'employeur si les faits faisaient apparaître que ce dernier avait ou aurait dû avoir conscience du danger auquel était exposé son salarié et qu'il n'avait pas pris pour autant les mesures nécessaires pour l'en préserver.

Mais l'obligation de sécurité ne vise pas seulement les risques dont l'auteur est interne à l'entreprise.

Dans un arrêt du 7 décembre 2011[2], mettant en cause un expatrié en Afrique, la Chambre sociale de la Cour de cassation a reconnu la responsabilité de l'entreprise, suite à l'agression de son salarié en relevant que celui-ci se trouvait du fait de son contrat de travail dans un lieu particulièrement exposé au risque et qu'il avait alerté son employeur sur l'accroissement des dangers en lui demandant d'organiser son rapatriement, sans que cette demande ne soit suivie d'effet.

À la lecture de ce type d'arrêt et jusqu'à récemment encore, les entreprises pouvaient être tentées de considérer que l'entreprise ne devenait un lieu à risque que pour le cas très spécifique des expatriés, population hors site et dont l'exposition particulière au risque avait pu donner lieu, dans le passé, à des arrêts emblématiques reconnaissant la responsabilité de l'entreprise, notamment sur le terrain de la faute inexcusable (voir Jurisprudence Karachi ou Sanofi).

(1) *Cass soc 11 avril 2002, n°00-16535*
(2) *Cass soc 7 décembre 2011, n°10.22.875*

Mais l'on sait bien que ce n'est plus le cas aujourd'hui et que **toute entreprise, dans le cadre normal de son activité en France, est susceptible de devenir un «lieu à risque» et d'engager donc à ce titre sa responsabilité vis-à-vis de ses salariés**.

Cette conclusion s'impose pour plusieurs raisons. En premier lieu, parce que la chambre sociale de la Cour de cassation n'a jamais érigé en principe général que l'agression provenant d'un tiers à l'entreprise pouvait exonérer la responsabilité de celle-ci. Ainsi des employeurs ont vu leur responsabilité reconnue dans des dossiers mettant en jeu un acte physique violent commis par des personnes tierces à l'entreprise. Dans un arrêt du 26 septembre 2012[3], la Chambre sociale de la Cour de Cassation a considéré que violait son obligation de sécurité l'employeur qui, face à la multiplication de cambriolages et de braquages dans son magasin, se contentait d'installer des caméras de surveillance et de proposer des mesures de soutien psychologique et de mutation dans d'autres magasins, ce qui ne constituait pas, selon la Cour, des mesures suffisantes et ne tenait pas compte des mesures proposées par le salarié et par le CHSCT. Une telle décision peut se comprendre par la rédaction même de l'Article L 4141-1 du Code du travail qui est très générale et vise toute atteinte à la santé sans distinguer un auteur interne ou externe à l'entreprise. L'on sait par ailleurs que, dans d'autres décisions, l'entreprise a été reconnue responsable de faits commis par des personnes consultants externes qui n'étaient pas placées sous son autorité.

En deuxième lieu, parce que la jurisprudence n'a jamais imposé comme condition que le manquement de l'entreprise ait été la cause déterminante de l'accident[4]. Il suffit que manquant à ses propres obligations elle ait permis que survienne le dommage et en soit donc l'une des causes.

Enfin, parce que dans le cadre d'une menace terroriste, le lieu ordinaire de travail peut exposer le salarié à un risque d'atteinte à sa santé, sans que le risque soit par essence de nature professionnelle. Et même si ce risque ne se concrétise pas, chaque salarié est susceptible de simplement craindre pour sa santé en venant sur son lieu de travail, cette crainte pouvant parfois apparaître plusieurs années après la survenance d'un accident[5]. Or, l'obligation de sécurité inclue bien évidemment la santé mentale. Un sentiment de crainte, un préjudice d'anxiété, si le salarié a déjà connu des incidents dont il craint la réitération, sont autant de moyens qui peuvent fonder une action en responsabilité contre l'employeur. Plus généralement, le sentiment d'insécurité d'un salarié estimant que son lieu de travail n'est pas suffisamment sécurisé peut aboutir à engager la responsabilité de l'employeur, peut important que l'entreprise n'ait commis aucune faute[6]. L'obligation de sécurité relève, en effet, du droit commun de la responsabilité contractuelle qui veut que le contrat de travail comporte des obligations réciproques pour chaque partie et qu'en contrepartie de sa capacité de travail qu'il alloue, le salarié puisse légitimement attendre que son employeur lui garantisse sécurité et santé. Cet argument peut parfois être invoqué en réaction à une décision prise par l'employeur. Ainsi, un salarié licencié pour inaptitude ou pour insuffisance professionnelle pourra être tenté de faire valoir que son inaptitude ou insuffisance ne sont que la résultante de la défaillance de l'employeur qui n'a pas mis en œuvre des mesures de protection efficaces. L'on pourrait même imaginer, même si sa recevabilité serait discutable, que le salarié soit tenté de faire usage de son droit de retrait qui lui permet de cesser spontanément le travail s'il estime qu'il existe un danger grave et imminent pour sa santé.

Pour limiter ce risque de mise en cause de responsabilité, l'entreprise n'a d'autre choix que d'engager une véritable réflexion et de mettre en œuvre, ce que le Code du travail qualifie de «mesures nécessaires» pour prévenir le risque d'une atteinte physique ou mentale, ces mesures devant aujourd'hui intégrer le risque terroriste. De quelles mesures s'agit-il?

Il doit bien évidemment s'agir, en premier lieu, de mesures d'information. Au-delà du contenu même de cette information, chaque entreprise devra réfléchir à son paramétrage en fonction de son organisation interne, de son activité et de son/ses lieux d'implantation. Il peut être opportun de définir un niveau d'information minimal, commun à tous, et un niveau d'information ciblé en fonction des postes et des rôles spécifiques de certains salariés (salariés compétents en protection et prévention des risques professionnels[7], CHSCT, etc). L'information devra envisager assez largement toutes les personnes qui circulent dans l'entreprise: visiteurs internes ou externes, stagiaires et le cas des salariés tant sur leur lieu qu'hors du lieu de travail, dans le cadre de leurs déplacements professionnels. Elle devra aussi envisager toutes les situations liées au travail dans leur diversité: l'accueil, la livraison sont aussi importants que les fonctions relevant de l'activité de l'entreprise elle-même. Elle ne devra pas oublier les situations qui ne sont que la conséquence indirecte du travail, comme la diffusion d'une information spontanément par les salariés via leur profil sur les réseaux sociaux, par exemple, et qui peut mettre en risque l'entreprise par la communication en externe de ses projets.

Mais l'information sur le risque lié aux attentats[8] ne peut se concevoir sans une information sur les mesures de prévention du risque. Par exemple, une note d'information sensibilisant le personnel sur la probabilité de survenance d'une attaque, outre son caractère anxiogène, serait inutile et n'exonérerait aucunement la responsabilité de l'entreprise si elle ne s'accompagne pas de consignes pour limiter ce risque

(3) *Cass Soc 26 septembre 2012, n° 10.16307*
4) *Cass soc 31 octobre 2002, n°00-18.359*
(5) *Cass soc 25 novembre 2015, n°14-24.444*
(6) *Cass soc 6 octobre 2010, n°08.22.45609*
(7) *Au sens de l'Article L4644-1 du Code du travail*
(8) *Sur le fondement des principes généraux de l'article R4141-3-1 du Code du travail*

(consignes d'évacuation ou au contraire de confinement, organisation du transport et prise en charge des frais pour chaque salarié vers son domicile, etc).

L'entreprise devra aussi mettre en œuvre des mesures de formation. En parallèle d'une réflexion sur la nature de ces formations[9] et sur leur niveau de mise en œuvre (salarié, «manager», salarié titulaire d'une délégation de pouvoirs, etc.), il faudra aussi commencer par analyser en détail l'existant et son niveau de performance. Combien d'entreprises peuvent, en effet, affirmer sans le moindre doute que leurs salariés sont correctement formés au risque incendie, ont des consignes d'évacuation à jour, que les serre-files sont encore salariés de l'entreprise, etc. ?

Ces actions de formation et d'information sont aujourd'hui considérées comme un moyen incontournable permettant à l'entreprise de démontrer qu'elle a mis en oeuvre tous les moyens nécessaires pour prévenir la survenance du risque et ainsi éviter d'engager sa responsabilité[10].

Au-delà de ces mesures, l'entreprise est également invitée à «mettre en place une organisation et des moyens adaptés» qui pourra aller bien au-delà de la mise en oeuvre de caméras de surveillance ou d'un contrôle des salariés à l'entrée du site. Appliqué au risque attentat, c'est une invitation à repenser l'organisation de l'entreprise à la lumière de cette nouvelle contrainte pour ne pas que cette organisation génère un risque. Faut-il comme certaines entreprises créer une fonction de «risk manager»? Faut-il aller jusqu'à adapter les procédures de recrutement ou de recours à la sous-traitance? Faut-il mettre en place de véritables procédures d'alerte?

Il faudra naturellement veiller à ce que ces mesures n'aboutissent pas à une surveillance accrue des salariés, par exemple par une multiplication des fouilles ou une vidéo surveillance élargie dont la légalité pourrait être remise en cause.

Sur l'ensemble de ces chantiers de réflexion, les représentants du personnel et particulièrement le CHSCT devront être bien évidemment associés mais plus encore, leurs «alertes» ou propositions devront être soigneusement considérées. Il en sera de même des demandes des salariés. Il est notable en effet que, dans la plupart des décisions de justice rendues, la responsabilité de l'employeur est aussi reconnue pour avoir négligé ou ne pas avoir au moins répondu aux messages d'alerte ou aux propositions des salariés ou des représentants du personnel.

L'entreprise est donc invitée à élaborer une véritable démarche de prévention, seul moyen de diminuer son risque juridique. C'est le message clair délivré par la Chambre sociale de la Cour de cassation dans ses arrêts les plus récents en la matière qui font dire que d'une obligation de sécurité de résultat, **le juge tendrait aujourd'hui vers une obligation de moyens renforcée**. Dans une affaire longuement commentée impliquant un chef de cabine qui, témoin des attentats du 11 septembre 2001, va développer plusieurs années après, un syndrome anxio-dépressif dont il imputera la responsabilité à son employeur, cette responsabilité ne sera pas reconnue et le salarié sera débouté de son action. Pour les juges, l'entreprise n'a pas manqué à son obligation de sécurité car elle avait bien mis en place des mesures, en l'occurrence un soutien psychologique et l'intégration du risque post traumatique dans le document unique. L'entreprise peut donc justifier avoir mis en place un arsenal de mesures, ce qui lui permet de s'exonérer de toute responsabilité.

À la lecture de cette décision, l'on voit bien qu'au-delà de ces mesures ponctuelles de prise en charge des salariés, comme la cellule de soutien psychologique, c'est aussi la cohérence du dispositif de prévention de l'entreprise qui est jugée: dans cette affaire, les risques identifiés sont bien intégrés dans le document unique et le salarié a fait l'objet d'un suivi médical régulier comme le relèvent indirectement les juges en constatant qu'il a été déclaré apte pendant toutes les années concernées.

Toute mesure prise par l'entreprise pose donc également la question de la mise à jour de sa documentation interne: les fiches de poste des contrats de travail pour intégrer la mission de prévention de certains salariés, les délégations de pouvoirs, le règlement intérieur pour imposer aux salariés un respect strict des consignes de sécurité, etc.

Outre le fait de limiter le risque juridique pour l'entreprise, **l'ensemble de ces mesures auront aussi pour effet de rendre le salarié lui-même acteur de sa propre santé au travail**. Il ne faut pas oublier en effet que le Code du travail reconnait aussi pour le salarié l'obligation de prendre soin de sa santé et de sa sécurité, ainsi que de celle des autres, et ce conformément aux «instructions» qu'il a reçues de son employeur et en «fonction de la formation» dispensée par celui-ci[11]. Ceci ne signifie pas que l'employeur pourra s'exonérer de sa propre responsabilité en se retranchant derrière une faute du salarié qui, par exemple, n'aurait pas signalé un risque. En effet, la responsabilité du salarié n'a pas d'impact sur celle de l'employeur[12]. En revanche, l'employeur pourra légitimement sanctionner le salarié qui aurait adopté un comportement à risque en ne se conformant pas aux mesures de prévention mises en place par l'entreprise. De la même manière, un refus d'indemnisation par le Fonds de garantie des victimes des actes de terroriste (FGTI) dont les conditions d'indemnisation sont indépendantes de la relation du salarié et son de son employeur, n'aurait aucun effet sur les obligations de l'employeur, qui n'aurait d'ailleurs pas nécessairement accès à cette information.

La menace terroriste concernant aujourd'hui les entreprises dans le cadre même de leur activité, les entreprises ne sauraient considérer que le risque terroriste aurait pour elle la qualification de force majeure exonératoire de responsabilité. Il est donc indispensable pour l'entreprise d'engager une démarche structurée de prévention seule susceptible de l'exonérer d'une éventuelle mise en cause de responsabilité. Il faut aussi y voir, car le risque attentat n'est pas ponctuel, un outil dans une démarche de qualité de vie au travail. ■

(9) *Dans le respect de l'Article R 4141-3 du Code du travail : mesures sur la conduite à tenir, sur les conditions de circulation ou encore sur les conditions d'exécution du travail*

(10) *Cass soc 1er juin 2016, n°14-19.702*

(11) *Article L4122-1 du Code du travail*

(12) *Cass soc 10 février 2016, n°14-24.350*

L'ENTREPRISE ET LES SALARIÉS VICTIMES D'ATTENTATS

Général Louis CROCQ
Médecin Général (CR), psychiatre des armées, créateur du réseau national des cellules d'urgence médico-psychologique

Comment l'entreprise peut-elle accueillir ses salariés qui viennent d'être victimes d'attentat, leur offrir un milieu sûr et un environnement social compréhensif qui les aide à se dégager de l'emprise de leur souvenir obsédant, et des conditions qui leur permettent de s'épanouir dans leur travail ?

Divers cas de figure

Des salariés d'une entreprise peuvent être victimes d'attentats terroristes, attentats à l'explosif, attentats par mitraillage ou attentats par tout autre moyen (camion fou, émission de gaz toxique, etc.).

Il peut s'agir du cas particulier où l'attentat a eu lieu dans les bâtiments ou sur le site de l'entreprise; et le salarié peut être seule victime (par exemple, le cas d'un gardien de nuit), ou une des victimes parmi d'autres. Et il peut être blessé physique ou blessé psychique, ou les deux à la fois (tout blessé physique conscient est aussi un blessé psychique, par les effets du choc émotionnel). Il peut être blessé psychique à un moindre degré, s'il a été seulement témoin à distance de l'attentat, ou intervenant dans les premiers secours. Enfin, son trouble émotionnel peut être plus intense s'il découvre que l'attentat visait des personnes (dont lui) et pas seulement les bâtiments ou le matériel.

Mais il peut s'agir aussi du cas où l'attentat a eu lieu en dehors du site de l'entreprise, par exemple quelque part en ville, dans une gare ou une station de métro; et, dans ce cas de figure, il convient de noter si le salarié victime se rendait à son travail, ou en revenait. Ici encore, on devra spécifier s'il est seule victime, ou victime parmi d'autres; et si, parmi les autres victimes – tuées ou blessées – il y a des membres de sa famille. À signaler aussi le cas, marginal, où des membres de sa famille ont été victimes d'un attentat en dehors de sa présence; *a priori*, son degré de victimisation est moindre, et il peut être endeuillé ou « impliqué », ou même « victime indirecte ». À signaler enfin, le cas où un attentat à l'explosif a détruit son domicile, et il est alors victime et sinistré (s'il était présent à son domicile), ou sinistré seulement (s'il n'y était pas présent).

Que l'attentat ait eu lieu sur le site ou en dehors de l'entreprise, le salarié victime blessé physique ou psychique peut avoir été hospitalisé un certain nombre de jours, et avoir bénéficié ensuite d'un arrêt de travail d'une certaine durée, avec ou sans soins à domicile. Et peut-être va-t-il reprendre son travail grevé d'une inaptitude transitoire à servir, que le médecin de l'entreprise va entériner et évaluer en fonction des avis du médecin traitant et des médecins experts.

État psychique des victimes d'attentat

Phase immédiate (les premières 24 heures)

Au moment de l'attentat, les sujets présents sur les lieux ont réagi par la réaction réflexe de stress. Il peut s'agir (dans 75 % des cas) d'un stress adapté, qui inspire des comportements salutaires de sauvegarde et d'entraide, mais se paie par des symptômes gênants (tachycardie, hypertension, pâleur et spasmes viscéraux) et par une dépense en adrénaline, en cortisol et en glucides. À la

fin de sa réaction de stress adapté, le sujet se sent à la fois soulagé et épuisé. Il va s'en remettre en quelques heures, éventuellement au terme d'un dialogue avec un secouriste ou un soignant. Mais il peut s'agir aussi d'un stress dépassé (25 % des cas), dans une des quatre formes d'inhibition stuporeuse, d'excitation incoordonnée, de fuite panique ou d'action automatique. Alors que le stress adapté se caractérise par la lucidité et le sang-froid, le stress dépassé se traduit par un vécu traumatique (traumatisme psychique) avec frayeur, horreur, désorientation, arrêt de la pensée (« trou noir »), orage neurovégétatif, sentiment d'impuissance et détresse.

Phase post-immédiate (du 2e au 30e jour)

Cette phase recouvre deux éventualités : ou bien tout rentre dans l'ordre dès la première semaine, les symptômes gênants du stress adapté s'effacent, l'esprit du sujet n'est plus accaparé en permanence par les images et souvenirs de l'événement, et il est disponible pour reprendre ses activités d'avant ; ou bien au contraire les symptômes du stress dépassé persistent (surtout les symptômes de déréalisation), l'esprit demeure obnubilé par les images de l'événement (donnant lieu à des ruminations mentales incessantes), et le sujet est incapable de reprendre ses occupations (professionnelles, familiales et loisirs) d'avant, tandis que de nouveaux symptômes – psycho-traumatiques – apparaissent, tels que reviviscences intrusives de l'événement, cauchemars, état d'alerte, sursauts et peurs phobiques liées à l'événement. Nous sommes alors dans la phase de latence ou d'incubation d'une névrose traumatique.

Phase différée-chronique (au-delà du 30e jour)

Dans cette phase, on constate le tableau clinique d'une pathologie psycho-traumatique durable, correspondant au diagnostic de névrose traumatique de la nosographie européenne, ou à son équivalent américain « trouble stress post-traumatique », appellation adoptée – l'hégémonisme de la langue anglo-saxonne y aidant – par la communauté scientifique internationale. Cette pathologie comporte trois volets : *primo*, des symptômes de reviviscence de l'événement (visions hallucinatoires, flash back, impression subite que l'événement va se reproduire, cauchemars) ; *secundo*, des symptômes généraux d'asthénie, de dépression, d'anxiété, de somatisations (algies et troubles psychosomatiques) et des troubles des conduites (boulimie, anorexie, addictions, agressions contre autrui ou contre soi-même) ; et *tertio*, sous-jacente au plan des symptômes, une altération de la personnalité, sans cesse en état d'alerte et luttant le soir contre l'endormissement (car s'abandonner au sommeil c'est risquer d'être attaqué par surprise), ayant perdu son intérêt pour le monde et pour l'avenir, et ayant perdu aussi sa capacité de relation affective équilibrée avec autrui (impression d'être séparé des autres par une membrane invisible, impression de n'être ni compris, ni soutenu). Ce trouble de stress post-traumatique peut se résorber – avec l'aide d'un thérapeute ou spontanément, en fonction des capacités de résilience du sujet - en trois à six mois ; mais il peut perdurer, plus ou moins intense et avec des reviviscences de plus en plus espacées, pendant des années. Il peut connaître aussi des relances à l'occasion d'autres expositions traumatiques ou de nouvelles d'événements violents. Enfin, la mise à la retraite, privant le sujet du dérivatif que lui procurait son activité professionnelle et le laissant seul face à ses souvenirs, peut être l'occasion de rechutes.

Prise en charge thérapeutique et sociale

Instauré au lendemain de l'attentat de la station RER Saint-Michel du 25 juillet 1995, le réseau national des cellules d'urgence médico-psychologique (CUMP), couvrant les 101 départements du territoire, est chargé d'assurer les soins médico-psychologiques aux blessés psychiques des attentats (et catastrophes et incidents à forte répercussion psychosociale) lors des phases immédiate et post-immédiate (et aussi pendant la phase chronique si le dispositif habituel de soins psychiques s'avère insuffisant). Dans l'immédiat, véhiculées sur le terrain par les SAMU, les équipes CUMP de psychiatres, de psychologues et d'infirmiers spécialement formés à la psychiatrie d'urgence, de guerre et de catastrophe, assurent le tri et les soins des victimes psychiques. À cette phase, la procédure de soins est dénommée « *defusing* », mot anglais signifiant déchocage ou désamorçage (préventif des évolutions pathologiques). Il s'agit d'apporter une présence « contenante » (contre toute nouvelle menace d'effraction psychique et contre les débordements émotionnels), et d'inciter le sujet à sortir de son inhibition et de son silence pour exprimer son ressenti, ce qui est déjà récupérer une activité et esquisser une maîtrise de l'événement. On rassure et calme la victime, et on lui remet (en la commentant) une fiche explicative de ses symptômes présents ou à venir, avec invite à contacter la CUMP en cas de besoin, et à participer à une séance de « *debriefing* », ou bilan psychologique d'événement, pendant la phase post-immédiate.

Pendant la phase post-immédiate, les CUMP assurent le suivi des victimes qui ont été vues dans l'immédiat ; et sont même contactées par d'autres victimes qui, dans l'euphorie d'être rescapées, avaient refusé l'offre de soins proposée sur le terrain, mais se sont décompensées ensuite au terme du classique temps de latence. Beaucoup de ces consultants tardifs avaient reçu en mains propres, sur le terrain, la fiche d'information. C'est lors de cette phase post-immédiate, vers le 8e ou 15e jour, qu'est proposée (toute victime peut décliner cette offre) l'opération de *debriefing*. Effectué en individuel ou en

petit groupe (dix sujets ayant été victimes du même événement, au même moment et sur le même lieu), le *debriefing* pratiqué par le personnel des CUMP se distingue des *debriefings* anglo-saxons en ce sens qu'il n'est pas narratif. On demande à chacun des participants, non pas de raconter ce qu'il a vu, mais d'exprimer (d'énoncer) ce qu'il a ressenti. Au cours d'une séance de *debriefing* de groupe, chacun, s'adressant aux autres et au debriefeur, peut s'exprimer plusieurs fois et, riche des propos des autres, peut faire évoluer sa prise de conscience et le sens profond de son expérience traumatique. Le debriefeur encourage l'identification au groupe, invite les participants à résoudre leurs problèmes de sentiment d'impuissance, de honte et de culpabilité et met un point final à la séance lorsqu'il voit qu'elle patine. Après la séance, il peut proposer une prise en charge plus personnalisée à tel ou tel sujet qu'il aura repéré comme fragile.

Le traitement du trouble stress post-traumatique à la phase chronique ne soulève pas de problème particulier. Diverses approches sont possibles: psychothérapie de soutien ou d'inspiration psychanalytique, méthodes cognitivo-comportementales de déconditionnement, recours à l'hypnose ou à la relaxation (ou encore à l'*Eye Movement Desensitization Reprocessing* ou EMDR, qui se rapproche de l'hypnose), et appoint pharmacologique pour réduire l'anxiété, l'inhibition dépressive et l'insomnie. Toutes ces approches relèvent peu ou prou de la méthode cathartique préconisée par Freud pour le traitement de la névrose traumatique: faire revivre au patient l'événement assorti de toute sa charge d'affects, mais en lui demandant d'établir des associations d'idées à son sujet; ainsi, il pourra donner du sens à l'insensé de son expérience traumatique et la réinsérer comme un souvenir construit (et non plus comme une souvenance sensorielle brute) dans la continuité fluide de sa vie.

En général, sur le terrain et même après, la prise en charge thérapeutique assurée par les CUMP et d'autres organismes de soin, se double d'une prise en charge sociale assurée par la Protection Civile, la Croix-Rouge, l'INAVEM et les associations de victimes. Cette prise en charge sociale, par les effets d'empathie et de compassion, a des effets psychologiques qui complètent harmonieusement les soins psychiques assurés par les CUMP.

Rôle de l'entreprise dans la santé mentale de ses personnels victimes ou impliqués

Lorsqu'un personnel victime d'attentat vient reprendre son travail, il est souhaitable qu'il soit accueilli avec compassion et encouragement par la direction ou le DRH de l'entreprise, vu le caractère exceptionnellement agressant de ce qu'il vient de vivre. Le médecin du travail, de son côté, peut doubler sa mission technique (évaluation d'aptitude et recommandation éventuelle d'aménagement du poste) d'un entretien où, sans interférer avec l'action du psychiatre ou généraliste traitant, il peut manifester sa compréhension et son empathie. Enfin, ses collègues, soucieux de ne pas laisser le rescapé face à ses ruminations solitaires, peuvent lui exprimer, dans la conversation, leur sympathie et leur soutien. Le cas échéant, et surtout s'il y a plusieurs victimes rescapées, la direction peut organiser une réunion d'accueil, avec la participation de tout le personnel (s'il s'agit d'une petite entreprise) ou des collègues de l'atelier concerné (s'il s'agit d'une entreprise de grande taille).

L'entreprise peut aussi aménager le poste de travail et les horaires du salarié affaibli par sa récente épreuve et mentalement moins disponible du fait de ses reviviscences. Elle peut aussi lui procurer de l'aide matérielle par l'action de ses services sociaux.

Enfin, dans la conjoncture d'une série d'attentats et du climat d'insécurité qui s'en suit, l'entreprise peut organiser des séances de sensibilisation et de formation de ses personnels, concernant l'évaluation du danger, la vigilance, les mesures préventives à prendre et, en cas de survenue d'un attentat, les comportements-réflexes à adopter pour la sauvegarde, les premiers secours et l'entraide. ■

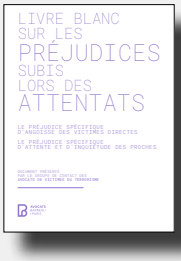
POUR ALLER PLUS LOIN

Après le 13 novembre, premiers résultats de l'enquête Crédoc - juin 2016

Dans le cadre du programme 13 novembre initié par le CNRS, l'Inserm et héSam Université, une série de questions sur les attentats du 13 novembre 2015 a été insérée dans la vague de juin 2016 de l'enquête « Conditions de vie et Aspirations » du CRÉDOC, menée auprès d'un échantillon représentatif de la population française de 2 000 personnes.

http://www.memoire13novembre.fr/sites/default/files/Note%20Cre%CC%81doc%2007-11-2016.pdf

Livre blanc sur les préjudices subis lors des attentats



Présenté par le groupe de contact des avocats de victimes du terrorisme
http://www.avocatparis.org/system/files/editos/barreauparis_livreblanc_victimes.pdf

LA « RADICALISATION » EN ENTREPRISE

Mustapha BENCHENANE
Docteur d'État en Science Politique, Conférencier au Collège de Défense de l'OTAN

À constater la confusion qui prévaut trop souvent dans les esprits depuis quelques mois, on est en droit de se demander si les terroristes ne sont pas en train de gagner, du moins quant à l'aspect psychologique de la confrontation en cours…

Pour mener le vrai combat et se donner les moyens de le gagner, il faut commencer par identifier le problème et, pour y parvenir, utiliser, entre autres, le vocabulaire approprié.

- Le mot « radicalisation » est employé indifféremment à propos de l'homme qui, sur son lieu de travail, refuse de serrer la main d'une collègue, et également pour désigner le processus menant un jeune à partir faire le « djihad » en Syrie ou qui commet un attentat terroriste dans le pays qui est le sien, puisqu'il y est né…

Dans le premier cas, il serait pertinent de parler de « fait religieux » dans l'entreprise. Tout intégriste, fondamentaliste, salafiste, n'est pas fatalement, amené à devenir terroriste. Néanmoins, on peut considérer que c'est un terreau favorable à des dérives extrémistes. Dans la plupart des cas, ceux qui passent à l'acte en devenant terroristes, se « radicalisent » rapidement sans toujours attirer l'attention sur les signes, les indicateurs, de leur transformation. C'est ainsi qu'ils créent l'effet de surprise.

- La formule « guerre contre le terrorisme » ne devrait pas être de mise. En effet, le terrorisme est l'une des formes de la violence et la guerre à mener doit être dirigée contre les terroristes qui ont recours à ce moyen que l'on appelle « terrorisme ».

- La laïcité est un principe, un concept qui se traduit par des relations spécifiques entre le pouvoir temporel de nature politique et les religions. La loi du décembre 1905 est dite « Loi de séparation des Églises et de l'État ». L'article 28 de ce texte évoque les signes d'appartenance à une religion pour les interdire sur les « monuments publics ». Il n'est donc pas question de l'École, de l'hôpital, des entreprises, encore moins de l'espace public. Il a fallu la loi de 2004 pour prohiber, à l'École, les « signes ostensibles » d'appartenance à une religion. Il faut reconnaître que le législateur visait prioritairement l'Islam.

  Actuellement, on utilise le mot « laïcité » avec une légèreté étonnante et, en le galvaudant, on l'affaiblit. Cela mérite quelques précisions qui viendront à la fin de cette analyse.

  Pour revenir à ce qui se passe dans les entreprises, de quoi s'agit-il dans la plupart des cas ?

  C'est soit une inadaptation d'une minorité de salariés parmi les musulmans à la société française qui a sa propre histoire et ses valeurs, soit un refus conscient de s'intégrer à cette même société qui est jugée « corrompue » compte tenu des mœurs permissives, la crise de l'autorité qui commence dans la structure familiale et que l'on retrouve au niveau de l'État, et de l'École, le scepticisme grandissant à l'égard de la démocratie représentative, le « mariage pour tous », etc…

  Dans ce domaine aussi il y a confusion et discorde sur ce qu'on est en droit d'exiger des musulmans : est-ce l'« intégration » ou l'« assimilation » ?

L'individu intégré est celui qui est utile socialement et qui respecte les lois, les valeurs, les normes du pays dans lequel il vit.

L'assimilation que certains expriment sous la forme d'une injonction est d'une autre nature : elle suppose que les personnes concernées procèdent à un « échange de cerveau » afin d'effacer totalement toute mémoire de leurs origines, celles de leurs parents et qu'elles renoncent ainsi à un imaginaire au profit d'un autre : celui du pays d'accueil ; qu'elles « françisent » leur nom et, pourquoi pas, qu'elles abjurent leur religion, donc qu'elles renoncent à l'Islam… Cet objectif est irréaliste à court et à moyen termes. Il ne peut s'envisager que dans le temps long, celui de l'Histoire. Encore que, compte tenu de la mondialisation – qui est aussi culturelle – et du « village planétaire », on peut se demander ce que pèsera, dans quelques décennies, le « récit national » ou le « roman national » que l'on voudrait « injecter » dans les cerveaux avec des méthodes autoritaires…

- À cet égard, le débat sur l'« identité » et les surenchères auquel il donne lieu sont dangereux pour plusieurs raisons. Ils sont d'abord révélateurs d'un trouble, d'un doute sur ce qu'est devenue l'identité de la France. Emmanuel LÉVINAS disait : « *Lorsqu'un peuple s'interroge sur son Identité, c'est qu'il l'a déjà perdue* »… Si tel est le cas en France actuellement, il conviendrait de s'interroger sur les raisons de cette situation anxiogène. Il y a des causes endogènes dans lesquelles l'Islam n'entre pour aucune part : le recul de la Foi chrétienne et la perte des valeurs morales qu'elle induit, l'implosion de la famille, la crise multidimensionnelle de l'autorité, le « pourquoi pas » à propos de tout et qui, sans cesse, recule les limites pour finir par toutes les abolir, le mariage homosexuel etc. ne doivent rien à l'Islam… Mais il semble qu'il n'y ait plus de restriction aux attaques, non pas seulement contre l'« islamisme », mais contre l'islam et les musulmans.

Cela est vécu comme une maltraitance par beaucoup d'adeptes de la deuxième religion de France avec, comme conséquence, chez certains d'entre eux, une vraie « radicalisation ».

Toujours est-il que des entreprises sont confrontées à des difficultés émanant de salariés musulmans. Les cadres ainsi que les responsables des ressources humaines ne savent pas comment y faire face tout en respectant la légalité et l'impératif de bon fonctionnement de leur structure.

Il convient d'essayer de trouver les « bonnes réponses » à la fois dans l'ordre juridique national et dans les conventions internationales signées et ratifiées par la France.

L'ordre juridique en faveur de la liberté

Le droit international et national est clairement en faveur de la liberté : le salarié peut, au sein de l'entreprise privée, exprimer ses opinions politiques et faire état de ses croyances religieuses de façon verbale ou symbolique.

L'article 9 de la Convention Européenne des Droits de l'Homme stipule : « *La liberté de manifester sa religion ou ses convictions ne peut faire l'objet d'autres restrictions que celles qui, prévues par la loi, constituent des mesures nécessaires, dans une société donnée, à la sécurité publique, à la protection de l'ordre, de la santé ou de la morale publique, ou à la protection des droits et libertés d'autrui* ».

La Directive 2000/78/CE du Conseil du 27 novembre portant création d'un cadre général en faveur de l'égalité de traitement en matière d'emploi et de travail interdit les discriminations y compris celles qui seraient fondées sur un motif religieux. Cette Directive a fait l'objet de la procédure de transposition en droit interne français et elle est incorporée au Code du travail.

La Cour Européenne des Droits de l'Homme reconnaît que la liberté religieuse relève d'abord du « For intérieur », mais elle va plus loin en ajoutant : « *elle implique de surcroît, notamment, celle de manifester sa religion* » et donc de l'extérioriser par des signes (Cour EDH, 25 mai 1993).

Dans une autre affaire, cette même Cour a estimé que le droit de manifester ses convictions religieuses devait être apprécié comme un « droit fondamental » car une « société démocratique doit tolérer et encourager le pluralisme et la diversité ». Elle va encore plus loin en affirmant qu'« une personne qui a fait de sa religion un axe majeur de sa vie puisse être en mesure de communiquer ses convictions à autrui » (15 janvier 2013).

Le droit français protège, lui aussi, la liberté religieuse.

La Constitution de 1958 intègre l'article 10 de la Déclaration des Droits de l'Homme et du Citoyen qui énonce : « *Nul ne doit être inquiété pour ses opinions, même religieuses pourvu que leur manifestation ne trouble pas l'ordre public établi par la loi* ».

Cette Constitution reprend l'article 5 du préambule de la Constitution du 27 octobre 1946 : « *Nul ne peut être lésé dans son travail ou son emploi, en raison de ses origines, de ses opinions ou de ses croyances* ».

Le Code du travail reprend ces principes dans son article 1121-1 : « *Nul ne peut apporter aux droits des personnes et*

aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ». Quant à l'article L. 1321-3 2° et 3°, il pose le principe que le règlement intérieur d'une entreprise ne peut apporter de restriction générale et absolue à l'exercice d'une liberté fondamentale, cette restriction doit être justifiée par la nature de la tâche à accomplir et proportionnée au but recherché et ne peut pas comporter de dispositions discriminant les salariés en raison de leurs convictions religieuses.

Le règlement intérieur est « l'ensemble des règles relatives à l'exécution du contrat de travail et aux relations agissant au sein de l'entreprise ». Il est soumis au contrôle de l'administration du travail car il est un acte réglementaire, et il relève du contrôle judiciaire en tant qu'acte de droit privé.

La Commission Badinter a présenté son rapport au Premier ministre au début de l'année 2016, sous le titre : « *Les principes essentiels du droit du travail* ». L'article 6 de ce document disposait : « *La liberté du salarié de manifester ses convictions, y compris religieuses, ne peut connaître de restrictions que si elles sont justifiées par l'exercice d'autres libertés et droits fondamentaux ou par la nécessité du bon fonctionnement de l'entreprise et si elles sont proportionnées au but recherché* ». L'article 2 de la loi n°2016-1088 du 8 août 2016, dite « loi El-Khomri », est inspirée de cette recommandation et donne son contenu à l'article L 1321-2-1 du Code du travail : « *Le règlement intérieur peut contenir des dispositions inscrivant le principe de neutralité et restreignant la manifestation des convictions des salariés si ces restrictions sont justifiées par l'exercice d'autres libertés et droits fondamentaux ou par les nécessités du bon fonctionnement de l'entreprise et si elles sont proportionnées au but recherché* ». Cette « loi El-Khomri » a été adoptée dans un contexte particulier marqué par l'affrontement politique entre les différentes sensibilités hexagonales, mais aussi par le traumatisme provoqué par les attentats terroristes. En dépit de ce contexte, on aurait pu se contenter des dispositions de la « loi Auroux » du 4 août 1982 sur la liberté des travailleurs dans l'entreprise.

Le contentieux relatif à la liberté des travailleurs au sein de l'entreprise, notamment en matière religieuse, a donné lieu à la saisie de l'appareil judiciaire qui a rendu des décisions ou des des arrêts au cas par cas.

Des restrictions à la liberté au sein de l'entreprise

Pour des raisons d'hygiène et de sécurité, le chef d'entreprise est fondé à interdire le port de signes religieux. En effet, dans certains cas, l'équipement de sécurité est obligatoire et il prime sur la liberté religieuse. La restriction est par ailleurs légale au regard de la nature de l'activité que le salarié doit exercer. La Cour d'Appel de Paris a justifié l'interdiction du « foulard islamique » à une vendeuse d'un centre commercial et à une technicienne de laboratoire. Les juges ont considéré que ces deux salariées étaient en contact direct avec la clientèle, donc à un large public de convictions variées. Dans ce cas, le port du « foulard islamique » pouvait nuire à l'image de l'entreprise.

La justice s'est prononcée en cette matière de façon empirique, en traitant le « cas de l'espèce ». Elle a dégagé les critères de pertinence et de proportionnalité. Elle a décidé que la liberté religieuse ne doit pas entraver la bonne exécution du contrat de travail, l'organisation nécessaire et les impératifs d'intérêt commercial.

La liberté d'expression religieuse peut être limitée lorsqu'elle constitue un abus d'expression. Tels que le prosélytisme, des actes de pression ou d'agression à l'égard des autres collègues. La question a été posée s'agissant du « voile islamique » : est-ce qu'il constitue en tant que tel un acte de prosélytisme ? La jurisprudence française et européenne considère qu'une distinction doit être faite entre le comportement prosélyte d'un salarié et le port d'un vêtement ou d'un insigne répondant à une pratique religieuse ou manifestant une appartenance à une religion, à un parti politique ou un mouvement philosophique qui ne constitue pas, en soi, un acte de prosélytisme.

La jurisprudence fonde ses décisions sur la notion de « bonne marche de l'entreprise ». Celle-ci doit l'emporter sur la liberté du salarié. Par exemple, la justice a validé le licenciement d'une salariée musulmane qui quittait son travail à 15h pendant le mois du Ramadan, alors qu'elle bénéficiait déjà d'un aménagement de ses horaires de travail pour quitter l'entreprise à 17h au lieu de 18h.

Dans certains cas, le fait d'être au contact de la clientèle n'est pas en soi une justification légitime pour restreindre la liberté religieuse au travail. A été reconnue comme mesure discriminatoire le licenciement d'une télé-enquêtrice en contact avec la clientèle et qui refusait de

retirer son foulard qu'elle portait depuis l'embauche et «*que sa tenue ne posait pas de problème particulier avec la clientèle*» (C.A Paris 19 juin 2003).

La justice a considéré qu'était illégal le licenciement d'un salarié au motif qu'il avait une «barbe trop longue». Cet entreprise -*Sécuritas*- avait avancé comme motif le «*non-respect du référentiel vestimentaire*».

Dans une autre affaire, le Conseil des Prud'hommes, par ordonnance de référé en date du 17 décembre 2002, a jugé qu'un licenciement en raison de «convictions religieuses» oblige l'entreprise à réintégrer le salarié. Cette décision a été confirmée par la Cour d'Appel de Paris pour laquelle le licenciement était «*manifestement illicite en ce que la restriction sur les vêtements cachait une atteinte à la liberté religieuse*».

La «Ligne rouge» pour le chef d'entreprise, c'est la «discrimination», qui est un délit. Mais il est difficile pour le salarié d'en apporter la preuve.

La Cour de Justice de l'Union européenne connaît actuellement une affaire sur saisine de la Cour de cassation qui, avant de se prononcer, a demandé à cette Cour d'interpréter la Directive du 29 novembre 2000 sur la lutte contre les discriminations en matière d'emploi et de travail. L'avocate générale, Eléonor SHARPSTON, soutient, dans ses conclusions, que «*le règlement d'une entreprise imposant un code vestimentaire parfaitement neutre est susceptible de créer une discrimination indirecte*». La Directive prévoit des exceptions à la non-discrimination si «*en raison de la nature d'une activité professionnelle ou des conditions de son exercice, la caractéristique en cause constitue une exigence professionnelle essentielle et déterminante, pour autant que l'objectif soit légitime et que l'exigence soit proportionnée*». L'avocate générale considère que «*cette dérogation doit être interprétée de manière stricte*». Elle estime que la requérante a été l'objet d'une discrimination directe fondée sur la religion. Elle ajoute: «*Rien n'indique que le fait de porter le foulard islamique empêchait Madame B d'accomplir ses tâches en tant qu'ingénieur d'étude ». Elle précise même que « le risque de préjudice financier pour l'employeur ne peut justifier une discrimination directe*».

Dans une affaire belge cette fois-ci, à propos toujours de «voile islamique», une autre avocate générale écrit dans ses conclusions que l'interdiction du port de signes religieux par l'employeur est possible dans certaines conditions. Elle affirme que doivent être pris en compte «l*a taille et le caractère ostentatoire du signe religieux, la nature de l'activité de la travailleuse, le contexte dans lequel elle doit exercer son activité; ainsi que l'identité nationale de l'État membre concerné*». Les deux affaires n'ont pas encore connu leur épilogue.

Si l'on se réfère à l'affaire *crèche Baby Loup*, la confusion a prévalu du début à la fin. Il s'agissait d'une salariée qui, à l'issue de son congé maternité, revient travailler mais en portant un «voile islamique». La crèche relève du droit privé, le devoir de «neutralité» que l'on doit observer dans les établissements publics ne s'applique donc pas en la matière. Pourtant, l'appareil judiciaire français a traité cette affaire depuis les Prud'hommes jusqu'à la Cour de Cassation siégeant en Assemblée plénière.

1) La salariée est licenciée pour «faute grave» en décembre 2008.
2) Les Prud'hommes confirment le licenciement le 13 décembre 2010.
3) Le licenciement est confirmé par la Cour d'Appel de Versailles le 27 octobre 2011.
4) La Cour de Cassation annule le 19 mars 2013 l'arrêt de la Cour d'Appel de Versailles et renvoie l'affaire devant la Cour d'Appel de Paris.
5) Celle-ci rend un «arrêt de rébellion» le 27 novembre 2013.
6) La Cour de Cassation, de nouveau saisie et siégeant en Assemblée plénière, suit l'arrêt de la Cour d'Appel de Paris, par un arrêt rendu le 25 juin 2014. Cet arrêt reconnaît que le règlement intérieur pouvait, en l'espèce, limiter la liberté d'expression religieuse des salariés de la crèche, justifiant cette restriction par le contexte particulier (public reçu, taille de la structure). En revanche, la Cour de Cassation refuse d'étendre le principe de laïcité et de reconnaître à la crèche le caractère d'entreprise de «conviction» ou de «tendance» (école catholique, parti politique, organisation syndicale).

On constate donc que la jurisprudence n'apporte pas une réponse claire et définitive aux problèmes éventuels auxquels le chef d'entreprise peut être confronté. On lui demande et on exige même de lui le respect de la liberté, en le sanctionnant en cas de «discrimination», tout en ayant à l'esprit le principe de «proportionnalité», la notion de «bon fonctionnement de l'entreprise» ou de l'«intérêt de l'entreprise», toutes notions vagues et pouvant donner lieu à des interprétations diverses et divergentes.

Ce qui est sûr – si l'on veut être rigoureux- c'est que le chef d'entreprise ne doit pas édicter des restrictions à

cette liberté religieuse en se fondant sur le principe de laïcité. En effet, celle-ci signifie : « *l'État neutre entre les religions, tolérant pour tous les cultes et forçant l'Église à lui obéir en ce point capital* » (Ernest Renan 1882) ou encore « *l'État neutre entre tous les cultes, indépendant de tous les clergés, dégagé de toute conception théologique* » (Ferdinand Buisson 1883). Les législateurs qui ont rédigé et voté la loi de décembre 1905 se sont inspirés de ces définitions. La laïcité ne concerne donc pas l'entreprise privée, les piscines ou les hôpitaux, et encore moins l'espace public.

S'agissant des entreprises privées, quand problème il y a, il concerne le « fait religieux » et non la « radicalisation ».

Dans toute la mesure du possible, il faut tout essayer pour trouver une solution à l'intérieur même de l'entreprise car le recours à la justice et, plus encore, la médiatisation, exacerbent les tensions et figent les positions.

On pourrait imaginer, avant le recours à la justice, la possibilité de faire appel à des « consultants-médiateurs » ayant une solide formation en droit du travail et, pourquoi pas, en islamologie. En effet, ce n'est pas au chef d'entreprise de faire de la pédagogie en matière religieuse. Un Conseil Français du Culte Musulman (CFCM), composé de personnalités éclairées et courageuses, indépendantes de toute allégeance étrangère, aurait un rôle déterminant à jouer en cette matière. Exemples : il pourrait expliquer que le Coran n'oblige pas à faire la prière sur le lieu de travail ; que rien dans le Coran n'interdit à un homme de serrer la main à une femme pour la saluer ; que lorsqu'il y a incompatibilité incontestable entre travail efficace et pratique du jeûne à l'occasion du Ramadan, le travail doit avoir la priorité, etc…

En dernière analyse, il faut savoir raison garder car les menaces prioritaires auxquelles les entreprises françaises sont confrontées ne relèvent pas du fait religieux (traduisons : de l'Islam) mais sont sur un autre registre : la compétitivité pour affronter la concurrence dans une économie de marché mondialisé, ce qui signifie la modernisation de leurs méthodes de travail, de leurs équipements, de leur organisation. Dans ce cadre, il y a aussi la vigilance permettant de lutter contre l'espionnage économique. Sans vouloir minimiser les questions relatives au fait religieux dans l'entreprise, force est de constater que trop souvent, elles sont présentées de façon passionnelle, ce qui aboutit à une aggravation des problèmes et à des crispations identitaires. ■

POUR ALLER PLUS LOIN

L'OBSERVATOIRE DU FAIT RELIGIEUX EN ENTREPRISE — ***Étude 2016***

L'Observatoire du Fait Religieux en Entreprise est un programme de recherche développé pour mener des travaux sur les questions liées aux différentes formes du fait religieux en entreprise.

L'ENTREPRISE N'EST NI LAÏQUE NI RELIGIEUSE : ELLE EST COMMERCIALE !

Éric MANCA
Avocat associé August and Debouzy

L'Observatoire du Fait Religieux en Entreprise, en partenariat avec l'Institut Randstad, a livré, le 22 septembre dernier, son étude pour 2016 sur ce qu'il est aujourd'hui commun de dénommer « le fait religieux en entreprise ».

Pour tout praticien et observateur avisé du monde de l'entreprise, ces résultats ne créent pas de véritable surprise. Ils ne font que confirmer une dynamique enclenchée depuis ces dernières années, caractérisée par une montée en puissance du fait religieux au travail (65 % des personnes interrogées ont été témoins de ces faits religieux en 2016, contre 50 % en 2015), et la sollicitation tout aussi grande du management de l'entreprise, prié de gérer les situations en dérivant (selon l'étude, en 2016, 48 % des faits religieux ont nécessité une intervention managériale, contre 24,5 % en 2014).

Le fait religieux dont il s'agit est avant tout celui de l'islam (à 95 % des cas selon M. Lionel HONORÉ, professeur des Universités et directeur de l'OFFRE), et se manifeste notamment par le port du voile.

Le fait religieux s'est donc invité dans l'entreprise. Dont acte. Cette dernière, à la différence de l'entreprise publique, n'est pas un lieu couvert par la neutralité. Elle est ainsi devenue un espace d'expression de plus en plus marqué en ce qui concerne la manifestation des convictions religieuses, et parfois même, comme il le sera exposé, au préjudice de ses intérêts premiers et légitimes, à savoir son objet commercial. Autrement dit, au préjudice de sa raison d'être.

La liberté de religion, liberté fondamentale, ne s'arrête donc pas au seuil de l'entreprise, où elle est plus précisément protégée par le Code du travail, qui proscrit toute discrimination/différence de traitement reposant notamment sur les convictions religieuses, à compter de l'embauche, et ainsi tout au long de la relation de travail.

Est-ce donc à dire que toute contrainte, toute réserve manifestée par l'entreprise à la liberté religieuse, afin de préserver son bon fonctionnement ou de faire cesser un trouble apporté à celui-ci, serait constitutive de discrimination ?

Et la liberté d'entreprendre dans tout cela ? Cette dernière, raison d'être de toute entreprise, devrait-elle s'effacer lorsqu'elle rentre en collision avec la liberté religieuse ?

Le bon sens conduit à répondre immédiatement par la négative. La liberté de religion, toute fondamentale soit-elle, n'en est en effet pas pour autant une liberté absolue. Elle est censée trouver sa limite là où commence le trouble objectif au bon fonctionnement de l'entreprise.

Mais voilà bien tout le problème. Au-delà de cette déclaration de principe, il n'existe pour l'heure aucune norme contraignante venant l'appuyer et, partant,

venant sécuriser l'entreprise dans son approche des problématiques liées à la manifestation du fait religieux au travail.

Alors que le fait religieux constitue un véritable phénomène de société, l'entreprise est invitée à se débrouiller seule dans l'appréciation de la marche à suivre.

Il lui appartient donc, à ses risques et périls, exposée à la censure ultérieure du juge et aux prétoires médiatiques, de concilier liberté d'entreprendre et liberté religieuse, en prenant garde de ne jamais verser dans les travers de l'inégalité de traitement et de la discrimination.

Exercice tout aussi délicat que périlleux. Si bien que, face à cette situation hautement aléatoire, l'entreprise est tentée d'opter entre trois lignes de conduite :

1/ Laisser faire, laisser aller, en pariant sur le fait que les managers / l'encadrement sauront faire « au mieux » ;
2/ Refuser toute concession aux faits religieux, notamment par crainte d'installation du communautarisme en son sein ;
3/ Acquiescer à toutes les revendications et postures religieuses, pour éviter tout risque de discrimination et ses incidences judiciaires, sociales et médiatiques, de nature à impacter durablement les valeurs, l'image et la réputation de l'entreprise. Autrement dit, acheter la paix sociale.

Ces trois postures ne sont assurément pas viables et tenables. Irresponsables pour la première et la troisième, illicite pour la seconde, elles ont toutes trois pour point commun de faire la part belle à la loi du plus fort, et de créer injustices, tensions et incompréhensions chez les salariés qui s'y trouvent exposés, dans un contexte, de surcroît, marqué par la vague d'attentats terroristes que connaît notre pays, qui a exacerbé les sensibilités et passions. Le regard du collectif en entreprise sur la visibilité religieuse s'en trouve donc logiquement modifié.

En cela, le fait religieux est un sujet bien trop sérieux pour se satisfaire d'un traitement au cas par cas, facteur de distorsions.

On ne peut, sur ce point, que difficilement se satisfaire de l'assertion bienveillante selon laquelle l'arsenal juridique à la disposition de l'entreprise se suffirait à lui-même pour permettre à cette dernière de faire face en toutes circonstances.

Si cette analyse s'avère exacte dans la gestion du fait religieux attaché aux demandes d'absences, de pauses, de temps de prière, et plus généralement d'aménagement du temps de travail, il en va tout autrement de la question du port d'un signe religieux en entreprise.

Ainsi, les questions liées à la demande de congés / absences, de temps de pause pour motifs religieux, ne doivent pas être traitées sous l'angle de la religion, mais sous l'angle exclusif de l'organisation du travail.

Le manager peut refuser ce type de demande si celle-ci nuit au bon fonctionnement de l'entreprise. Un problème de sous-effectif, de surcroît de travail, de difficulté à s'organiser différemment, peut être légitimement avancé pour refuser ce type de réclamation.

Il s'agit de raisons objectives tout à fait légitimes, puisque totalement étrangères à toute considération d'ordre religieux.

Il en va de même avec les salles de prières. Pareille revendication ne s'inscrit pas dans l'ADN d'une entreprise. L'entreprise doit, là encore, pouvoir répondre de façon objective : manque de locaux ; absence de moyens pour les entretenir, voire souhait de ne pas créer des distorsions par rapport aux autres salariés. D'autant qu'en cas de réponse positive, l'entreprise se devra de s'assurer, au titre de son obligation de prévention des risques et de sécurité, que la salle de prière mise à disposition ne sert pas de relai à quelque action prosélytiste que ce soit, ou encore à l'expression / diffusion de toutes valeurs contraires ou attentatoires aux lois de la République, à l'ordre social et aux bonnes mœurs. Soit autant d'obligations exorbitantes.

Seul l'intérêt légitime de l'entreprise doit entrer en ligne de compte, à l'exception de toute autre considération. Il faut donc s'attacher exclusivement à répondre au fait religieux par le prisme d'une seule et unique considération : l'existence ou non d'un trouble au bon fonctionnement d'un service ou de l'entreprise. Autrement dit, que l'on bannisse de son jugement toute considération / sensibilité personnelle, par nature étrangère à la notion de bon fonctionnement de l'entreprise.

Dans ce cas de figure, la ligne de conduite est claire. Soit l'entreprise est en mesure de satisfaire la requête de son salarié, sa revendication se révélant sans incidence sur le bon fonctionnement de son service, et plus largement sur le bon fonctionnement de l'entreprise, soit il en va autrement, et le salarié devra alors, une fois parfaitement avisé de la situation, renoncer à sa requête.

Si celui-ci devait malgré tout persister et passer en force, il se placera alors sur le terrain du manquement et s'exposera au pouvoir de sanction de l'entreprise qui

oscillera, en fonction de l'intensité du manquement constaté, de l'avertissement au licenciement pour faute grave (insubordination, abandon de poste).

De la même manière encore, le fait de ne pas vouloir saluer ses collègues de sexe féminin, constitue un comportement discriminant à raison du sexe. L'employeur se doit, dans un premier temps, de sensibiliser le salarié à son comportement et à la qualification qu'il revêt, dans l'espoir que ce trouble cesse. À défaut, ce comportement n'étant pas acceptable, un avertissement pourra être notifié, suivi d'un licenciement pouvant aller jusqu'à la faute grave, dans l'hypothèse où le salarié se refuserait toujours à entendre raison.

Bien souvent, les managers situés en première ligne, entre le marteau et l'enclume, sont dans l'ignorance de ce mode d'appréciation, par manque de formation préalable. Ils se retrouvent alors dans une position délicate pour réserver leurs décisions.

La formation des managers sur l'état du droit applicable et des outils de gestion qu'il offre au soutien de l'intérêt légitime et objectif de l'entreprise, dans le respect de l'individu et de son intimité, est donc incontournable.

En cela, la publication du *Guide Pratique du Fait Religieux dans l'Entreprise privée*, par le ministère du Travail, constitue un bon début de réponse et de soutien à des managers exposés, trop souvent dépassés par des réclamations à caractère religieux qu'ils ne savent pas, ou mal, traiter.

Reste alors la question du port de vêtements à caractère religieux et du trouble au fonctionnement de l'entreprise susceptible d'en découler, notamment dans les relations avec la clientèle.

Plus précisément, ce qui occupe aujourd'hui et depuis ces dernières années nos juges, a trait au port du voile.

Comme évoqué, notre droit a ici un vrai point de fragilité. Jusqu'à présent, le motif tiré de l'intérêt commercial de l'entreprise constituait, même si de façon aléatoire puisque livré à l'appréciation des juges en cas de litige, un motif de nature, lorsqu'il est établi, à justifier une limite à la liberté de religion.

Ainsi, la demande de l'employeur visant à obtenir de la salariée qu'elle s'abstienne de porter le voile en situation de contact avec la clientèle, est légitime et jugée comme telle, dès lors où, en dehors des relations clientèle, le port du voile est accepté le reste du temps.

On pouvait donc penser, dans un contentieux transmis à l'appréciation de la Cour de cassation, et concernant précisément le cas d'une salariée (employée en qualité d'Ingénieur d'Études) en contact avec la clientèle et refusant de quitter son voile pendant le temps de sa relation client, au mépris des remarques de ce dernier et des injonctions de son employeur, que le sort de ce litige, déjà tranché par les juges du premier et second degré, ne porterait pas à grande difficulté devant les juges suprêmes, ces derniers ayant déjà eu à connaître de la médiatique affaire de la crèche Baby Loup.

Pourtant, au mois d'avril 2015, ces derniers ont décidé de transmettre à la Cour de Justice Européenne, une question préjudicielle visant à inviter cette dernière à trancher si le souhait de la clientèle, de ne plus vouloir travailler avec une salariée voilée, pouvait constituer une « exigence essentielle et déterminante », justifiant que soit portée une limitation à la liberté fondamentale de religion dans l'entreprise.

Il s'agit ici d'un manque de courage certain de notre plus haute juridiction, qui s'abstient tout simplement de se prononcer sur un point de droit pourtant simple, et préfère passer la « patate chaude » à son voisin.

Cette question préjudicielle témoigne surtout de l'instabilité juridique criante à laquelle se retrouvent confrontées les entreprises, qui ne peuvent qu'avoir les mains qui tremblent lorsqu'il leur faut rompre le contrat de travail, afin pourtant de sauvegarder leurs intérêts premiers et légitimes, bousculés par les excès de faits religieux.

Elle apporte un démenti cinglant à tous ceux qui se refusent à ce qu'il soit légiféré sur la question, au motif que notre arsenal juridique serait parfaitement à même de répondre à toutes les situations rencontrées.

Et un malheur n'arrivant jamais seul, le 13 juillet 2016, l'Avocat Général a rendu ses conclusions au titre desquelles l'intérêt commercial de l'entreprise ne pourrait faire obstacle à la liberté de religion.

Plus précisément, et selon la « religion » de l'avocat Général, ni l'intérêt commercial de l'entreprise dans ses relations avec la clientèle, ni le préjudice financier que pourrait subir l'employeur, ne seraient susceptibles de justifier le licenciement de la salariée. Le licenciement serait donc constitutif d'une mesure discriminatoire, et devrait, par conséquent, être jugé nul.

Cette position interpelle à tout le moins. Elle s'inscrit en parfaite méconnaissance de la vie et des enjeux

de l'entreprise, jusqu'alors bien entendus au titre de notre droit national. Pareille position est foncièrement dangereuse pour l'avenir et les intérêts légitimes de l'entreprise. Si l'entreprise privée n'est pas laïque, elle n'est assurément pas religieuse. L'entreprise est commerciale !

En cela, la position de l'avocat Général est constitutive d'une véritable entrave à la liberté d'entreprendre, dont il convient de rappeler qu'elle a valeur constitutionnelle.

Reste désormais que la CJUE, qui statuera pour la première fois sur cette question, et qui n'est fort heureusement pas liée par la « religion » de l'Avocat Général, saura faire la part des choses, sans céder au dogme.

Dans l'hypothèse où la Cour Européenne devait faire sienne la vision de l'Avocat général, il est alors à craindre une recrudescence du fait religieux en entreprise, porté par des individus usant de cette liberté fondamentale, tel le *Cheval de Troie*, dans le but de mettre l'entreprise à l'épreuve et de porter durablement atteinte à la paix sociale, afin de servir des intérêts résolument étrangers à ceux commandant une bonne et loyale exécution du contrat de travail.
Sa décision est attendue pour la fin 2016.

Face à tant d'instabilité juridique, interdisant que pareille question puisse être traitée au cas par cas, l'intervention du législateur est nécessaire.

Elle est certes déjà présente au titre de la Loi Travail, qui permet à l'entreprise d'introduire un principe général de neutralité dans son règlement intérieur.

S'il s'agit là d'un pas appréciable, témoignant que le Politique semble enfin avoir pris la mesure de la situation, il n'apporte toujours pas de garantie et de sécurité juridique aux entreprises qui seraient désireuses d'y souscrire. Le principe est posé, mais son mode d'emploi est laissé à la seule responsabilité de l'entreprise qui devra veiller à ce que les restrictions apportées à la liberté religieuse soient « *justifiées par l'exercice d'autres libertés et droits fondamentaux ou par les nécessités du bon fonctionnement de l'entreprise et si elles sont proportionnées au but recherché* ». Autrement dit, et comme l'a d'ailleurs fait savoir le ministère du travail, il n'est pas question de fixer quelque cadre d'application à ce principe. L'entreprise est donc à nouveau laissée dans le vague, son sort confié, après coup, aux bons soins du juge qui dira un droit aléatoire.

En cela, le texte [Loi Travail] n'apporte pas de réelle sécurité juridique aux entreprises qui désirent une neutralité sur le lieu de travail. Cet écueil pourrait être évité si le législateur s'appliquait plus simplement à introduire un principe de neutralité mesuré, à savoir : l'interdiction de tout port de vêtement / insigne religieux dans les rapports avec la clientèle. Point qui fait aujourd'hui véritablement débat tant les décisions judiciaires y afférentes se distinguent par leur caractère aléatoire, alors que sont en jeu des impératifs liés à la paix sociale en interne, et à l'objet éminemment commercial de toute entreprise. ■

QUEL EST LE MEILLEUR ENDROIT EN FRANCE POUR RÉUSSIR LE « VIVRE-ENSEMBLE » ?

Thomas BOUVATIER
Psychanalyste, écrivain, travaille à l'association Entr'Autres à la psychologie du jihadisme et analyse de la radicalisation

À l'école, où l'autorité des professeurs est toujours plus contestée ? Dans les centres sportifs où essaiment de nombreux recruteurs islamistes ? Dans ces quartiers où la cohésion sociale est urgente mais que l'État semble ne plus pouvoir contrôler ? Enfin, dans les centres de déradicalisation, qui sont visiblement un échec ?

Des solutions sont encore à trouver et à tester dans ces lieux publics, mais il y a forcément un autre espace en France pour apprendre une meilleure manière de cohabiter. Un espace de taille suffisamment importante, proche des gens et engendrant une véritable dynamique entre eux.

Ce lieu existe depuis longtemps, c'est l'entreprise.
Qu'elle soit publique ou privée, elle est le seul endroit politiquement et religieusement neutres, où des hommes et des femmes entrent en contact toute la journée, partagent leurs expériences au fils des ans, et unissent leurs efforts dans le but d'une réussite commune. L'entreprise est une société. Elle est très bien placée pour jouer le rôle d'une matrice de la citoyenneté, en accueillant des Français riches de leur diversité, qui peuvent s'y identifier et y trouver un moyen d'affermir le sens qu'ils donnent à leur vie.

À cette vision vient s'opposer un obstacle de taille.
À l'ère de la mondialisation et de la flexibilité, le milieu du travail a parfois évolué vers une forme d'inhumanité. C'est du moins ce qui est ressenti par certains employés dans les multinationales, qui disent ne plus être reconnus, être isolés, incapables de saisir l'utilité du but qu'ils poursuivent.

Comment les individus les plus marginalisés pourraient être attirés par le monde de l'entreprise, eux qui ne sont pourtant pas dénués d'esprit d'entreprise, comme le montrent les réseaux clandestins de type mafieux ou jihadistes que certains montent avec succès ?

Prenons deux exemples d'entreprises publique et privée pouvant intégrer au mieux ses membres les plus divers : l'armée française et la haute finance.
Chez elles, l'importance attachée à la réussite des missions est telle, que leur direction recrute sans distinction de couleur de peau, de sexe ou de religion. En revanche, chacune attache un soin tout particulier à éviter celui ou celle qui est porteur d'une division potentielle, car, pour des raisons bien différentes, elle prône l'union absolue en son sein – au moins pour le temps de la mission en ce qui concerne la finance.

Cette union de type fusionnel est essentielle car c'est ce type dont il est question dans la radicalisation.

Qu'est-ce que recherche un jeune en voie de radicalisation ? Un lien sacré dans un groupe, une reconnaissance absolue, un but glorieux. Cette radicalisation n'est pas forcément religieuse, elle peut être politique comme on peut le voir dans les partis extrémistes, ou amicale comme dans les gangs. Mais la radicalisation peut être aussi professionnelle.

Ce point est important, car il nécrose à sa manière le milieu du travail.
Observons la clinique du *burn-out* par exemple. L'employé qui en est victime est celui qui a constaté sa non reconnaissance, son rejet et l'impossibilité d'atteindre le but qu'il s'était fixé, souvent disproportionné par rapport

à ses capacités. Il peut aussi s'agir d'un but qu'on lui a fixé, quand il été victime de ce que les médias appellent « un pervers narcissique ». Un patron qui commence d'abord à flatter sans cesse son employé, à qui il dit qu'il est comme son fils ou sa fille, qu'il veut associer à des projets grandioses et qui lui promet à un avenir brillant. Ou il fait pareil avec son associé, qu'il compare à un frère ou une sœur, avec qui il fait des plans sur la comète, dressant un portrait d'eux idyllique et se réjouissant de devenir millionnaires. Puis un différend survient, le patron se sent en faute, critiqué, il n'en faut pas beaucoup. Il devient alors distant avec son employé ou son associé, puis il se met à le critiquer sans cesse dans son dos, à le pousser toujours davantage au sacrifice. C'est ça ou la sortie. L'employé ou l'associé peut alors quitter son poste, faire un procès ou, à l'inverse, s'attacher à plaire toujours plus au patron pour retrouver ce moment de grâce entre eux, jusqu'à travailler comme un esclave, être toujours disponible, ne plus dormir, s'oublier. Cette radicalisation au travail utilise les mêmes techniques que dans les sectes ou les groupes terroristes :

Phase 1 : reconnaissance absolue / union sacrée de type familial / projet brillant
Phase 2 : culpabilisation
Phase 3 : demande de réparation

Dans le cas de l'entreprise, l'employé ou l'associé peut tomber en *burn-out* ou, dans les cas les plus extrêmes, se suicider.

Les personnes qui sont en difficulté affective sont plus désireuses que d'autres à l'idée d'une telle affiliation. C'est en les repérant qu'un patron pervers, ou qu'un groupe pervers déploiera tous ses talents pour le convaincre de se soumettre à lui.

Parmi ces groupes se trouvent par exemple « les jihadistes à col blanc ». On appelle ainsi les islamistes qui tentent de prendre le pouvoir non pas par la violence, mais en utilisant les valeurs occidentales afin de mieux les rejeter une fois le pouvoir conquis et la société régie par la Charia, la loi selon Allah. Ces groupes islamistes tentent de remplacer les syndicats traditionnels en offrant une protection identitaire au travailleur. La tentation est grande pour celui-ci de l'accepter. Chaque décision commise à son encontre par la direction de l'entreprise, chacune de ses revendications religieuses refusées, seront désormais susceptibles d'être considérées comme islamophobes. Dans un pays travaillé par la lutte contre les dissensions religieuses, toutes formes d'accusation de ce type menacent de salir durablement la réputation d'une entreprise. C'est une arme que les syndicalistes traditionnels ont des difficultés à fournir, d'où le soutien des ultragauchistes aux islamistes qu'ils voient remporter plus efficacement le combat contre l'ennemi capitaliste commun. Cette logique victimaire des militants islamistes est particulièrement efficace contre toute forme d'autorité non musulmane, et permet ainsi une revendication constante.

La fracture menace les *open-spaces*.
Le patron et le groupe pervers se positionnent comme les représentants d'une nouvelle famille, soudée, protectrice et ambitieuse, dans une société qui n'est plus capable de jouer ce rôle.

Il faut rappeler que le capitalisme familial de type patriarcal, tel qu'il existe souvent en Asie, a deux cent ans d'ancienneté en France et n'a pris fin qu'après les Trente Glorieuses. L'entreprise se présentait alors comme un nouveau foyer, dirigée par un patron paternaliste. Ce modèle faisait prolongement ou substitution à l'environnement familial du travailleur, cela avait son utilité quand ce dernier était défaillant. Avec la fin de ce modèle mais aussi du travail à vie, de la sécurité professionnelle, auquel il faut ajouter l'atomisation de la famille traditionnelle et la forte diminution des rites sociaux, les individus recherchent un environnement plus englobant, uni et rassurant.

Il n'est surtout pas dit qu'on doive regretter le capitalisme à papa, de type autoritaire et phallocrate. *Team building*, éthique, management, communication interne, gestion de crise, contre-radicalisation… Les chantiers ne manquent pas dans l'entreprise du futur. À la fois innovante, sûre d'elle-même et humaine, elle est à construire et l'État doit y participer.

Quant aux demandes de type fusionnel elles doivent être vite repérées lors des séances d'orientation, dès l'école, et des métiers adaptés peuvent être alors proposés. Il n'y a pas que l'armée ou la finance qui puissent fortement les impliquer et les reconnaitre, mais aussi des petites entreprises de type familial qu'on trouve notamment dans l'artisanat ou les métiers de l'art.

Certes, la lutte contre le terrorisme et l'islamisme ne passe pas que par l'intégration. Laissons à la Défense, à l'Intérieur et à d'autres ministères la reconnaissance qu'ils méritent dans ce combat.

Mais en ces temps pré-électoraux, il est important de souligner aussi que les hommes politiques qui vont gouverner la France de 2017 ne sont pas les seuls en charge de l'intérêt général et du bien commun. Les dirigeants d'entreprises, grandes et petites, publiques et privées, sont aussi des acteurs politiques, ancrés dans la réalité et contributeurs du vivre ensemble.

C'est un lien nouveau qui doit être établi entre ces acteurs clés, la population active et l'État, afin de mieux intégrer les citoyens dans les entreprises, favoriser le vivre ensemble et lutter contre la radicalisation. ■

POUR ALLER PLUS LOIN

«Petit manuel de contre-radicalisations», mars 2017, Éditions du PUF.
« Il y a obsession commune aux dépressifs et aux djihadistes
Thomas Bouvatier - Victimaire et sanguinaire - Le Point

Entretien avec
CLAUDE SOLARZ

Vice-Président du Groupe PAPREC

Au nom d'un combat qu'il mène contre les discriminations, Jean-Luc PETITHUGUENIN, PDG fondateur de PAPREC Group, a souhaité que l'ensemble de ses 4000 collaborateurs (56 nationalités différentes) se prononcent sur l'application d'une charte de laïcité qui sera inscrite au règlement intérieur de Paprec Group. Une initiative qui pourrait faire avancer le débat sur la laïcité même si elle est en avance sur la législation et la jurisprudence actuelle.

Pourquoi cette charte ? Y-a-il eu un élément déclencheur ?

Nous avons pris un pari il y a 20 ans. Celui de la diversité. Employer des hommes et des femmes de toutes origines, culturelles et sociales. Nous rassemblons dans notre entreprise aujourd'hui 56 nationalités. Dans un contexte de montée de l'intégrisme, mais sans que Paprec ait eu à vivre de crise en son sein, nous avons décidé d'anticiper et d'élaborer une charte de la laïcité et de la diversité. Objectif : coucher sur le papier nos règles communes pour redire notre vision du vivre-ensemble. C'est aussi une façon de protéger nos salariés des pressions communautaires.

Quel a été le processus pour concevoir cette démarche ?

Cette charte a été votée à l'unanimité par l'ensemble des comités d'entreprise. Comme c'était une démarche inscrite dans une continuité, elle a été acceptée par tous. Nous n'avons pas épargné nos efforts pour expliquer notre démarche. Sur chacun des 102 sites, un membre du comité exécutif a fait la pédagogie de la charte. Nous avons communiqué dans notre journal interne, Paprec News, à plusieurs reprises, en y consacrant des dossiers pour expliquer notre démarche et amener les collaborateurs à réfléchir à ce texte. Les directeurs et les directrices sur le terrain ont ensuite été les porte-voix et les pédagogues pour expliquer ce texte.

Comment a-t-elle été perçue par les salariés ? Ont-ils été favorables à sa mise en oeuvre ?

Notre démarche puise ses racines dans un travail de plus de 20 ans pour faire exister une diversité heureuse. Le respect, la tolérance, ce sont des notions auxquelles sont très sensibles nos collaborateurs. Ils souhaitent que ce « bien vivre ensemble » puisse perdurer. Ils ont choisi d'appuyer ce projet qui, selon eux, allait dans ce sens.

Quel est le cadre légal de cette charte ?

Depuis la loi Travail 2, nous sommes désormais en phase avec la loi qui vient consacrer le principe de neutralité religieuse en entreprise. Nous avons été pionniers sur le sujet. Nous allons suivre avec intérêt les prochaines jurisprudences qui amèneront sans doute le législateur à préciser ce que recouvre la notion de neutralité en entreprise. ■

CHARTE DE LA LAÏCITÉ ET DE LA DIVERSITÉ

PAPREC GROUP

1 / La laïcité en entreprise assure aux salariés un référentiel commun et partagé, favorisant la cohésion d'entreprise, le respect de toutes les diversités et le vivre ensemble.

3 / La laïcité en entreprise permet l'exercice de la liberté d'expression des collaborateurs dans la limite du bon fonctionnement de l'entreprise comme du respect des valeurs républicaines et du pluralisme des convictions.

5 / La laïcité en entreprise implique que les collaborateurs ont un devoir de neutralité : ils ne doivent pas manifester leurs convictions politiques ou religieuses dans l'exercice de leur travail.

7 / Au sein de l'entreprise et dans l'exercice de leurs fonctions, les règles de vie des différents espaces, précisées dans le réglement intérieur de chaque établissement, sont respectueuses de la laïcité. Ainsi, le port de signes ou tenues par lesquels les collaborateurs manifestent ostensiblement une appartenance religieuse n'est pas autorisé.

2 / La laïcité en entreprise offre aux collaborateurs les conditions pour forger leur personnalité, exercer leur libre arbitre et exercer leur citoyenneté. Elle protège de tout prosélytisme et de toute pression qui empêcheraient de faire ses propres choix et de réaliser son activité dans un environnement serein.

4 / La laïcité en entreprise implique le rejet de toutes les violences et de toutes les discriminations, garantit l'égalité entre les Hommes et les Femmes et repose sur une culture du respect et de la compréhension de l'autre.

6 / Conformément à la loi, nul ne peut se prévaloir de son appartenance religieuse pour refuser d'exécuter sa mission ou pour perturber le bon fonctionnement de l'entreprise.

8 / Par leurs réflexions et le respect mutuel, les collaborateurs font vivre au sein de l'entreprise la valeur fondatrice du Groupe de promotion des Diversités.

Télécharger
la charte de la laïcité et de la diversité

Interview de
FRANÇOIS PUPPONI

Député Maire de Sarcelles

À supposer qu'il y en ait une, comment se caractérise la contribution des acteurs locaux à la politique de sécurité publique ?

De façon générale, les relations partenariales entre les collectivités locales avec les pouvoirs publics déconcentrés sont trop rares. Elles sont encore, pour le moment, très informelles et dépendent de l'état des relations interpersonnelles de chacun avec le préfet ou les services de renseignement territoriaux.

En outre, les collectivités locales ne sont pas systématiquement associées aux réformes qui les concernent de façon directe ou indirecte. Il en résulte des situations très inégales entre les territoires.

Le contexte sécuritaire force nos institutions à faire évoluer leur fonctionnement. Cette adaptation contrainte met entre parenthèses leur capacité à coopérer efficacement, chacun s'efforçant d'agir dans son périmètre.

La coproduction de sécurité est-elle aujourd'hui suffisante et adaptée au contexte ? Est-elle encore valable ? Quels en sont, à votre niveau, les principaux acteurs ?

Conçue il y a 30 ou 40 ans pour mobiliser les institutions sur le problème de la délinquance, cette doctrine d'emploi n'est plus valable, en l'état, en matière de lutte contre le terrorisme. Les services de l'État, Police, Justice, Renseignement, considèrent le sujet trop grave pour être collectivement traité. Il y a, en toile de fond, une bataille sur les compétences régaliennes et les périmètres d'intervention de chacun.

Nous avons tout intérêt à formaliser/systématiser les relations avec les services, c'est évident. Sur un sujet aussi grave, nous ne sommes pas encore capables de mettre toutes les institutions républicaines autour de la table… Nous devons pourtant nous accorder sur ce principe de réalité : nous sommes en guerre, nous sommes attaqués ! De ce constat, devrait découler une logique d'action collective. Sans cela, les tentatives de certains maires pour faire passer les messages resteront inefficaces et isolées.

Je crois qu'il faut multiplier partout les structures de prévention, qui doivent être organisées par les services municipaux, départementaux et régionaux. Nous revivons le même débat que nous avons eu en matière de lutte et de prévention contre la délinquance il y a maintenant 20 ans. Il faut créer un réseau d'acteurs locaux en charge de la prévention de la radicalisation, puis mettre en place un groupe opérationnel de surveillance avec les services de l'État.

Le phénomène religieux, communautariste, a-t-il des répercussions directes sur l'économie locale ?

Le phénomène est inquiétant… Les « déstructurés » que nous avons dans nos banlieues sont plus ou moins récupérés par les réseaux avant de passer à l'acte. Ce sont des gens qui sont psychologiquement « fracassés » et qui, pour la plupart, sont des cas relevant de la psychiatrie. Nous le savons

et nous les connaissons. Nous les avons vus évoluer personnellement et déraper collectivement. Nous : les écoles, les institutions, les éducateurs spécialisés ; à défaut de pouvoir les encadrer, nous les avons oubliés, mis de côté parce que nous n'arrivions plus à les gérer. Ceux qui sont passés à l'acte ont tous un profil chaotique… Nous les connaissons ! Il s'agit de quelques dizaines d'individus qui dérapent, par tranches d'âges. Il y a encore quelques années on se disait : « *de toute façon, ils seront rattrapés par la délinquance, on les retrouvera en prison un jour* ». Aujourd'hui, ils sont rattrapés par les réseaux de radicalisation.

Les têtes de réseaux radicalisés ne passent pas elles-mêmes forcément à l'acte. Elles recrutent plutôt la chair à canon dans nos quartiers. Leurs cibles sont les plus fragiles, les plus déstructurées et malléables.

Il ne faut pas confondre la radicalisation djihadiste avec une forme d'extrémisme religieux. Nous constatons qu'un certain nombre d'habitants de ces quartiers, pour la plupart issus de la communauté musulmane, ont maintenant une pratique rigoureuse, affirmée, affichée et revendiquée de l'islam. La combinaison de ces deux phénomènes est un risque pour l'entreprise qui regroupe à la fois des jeunes radicalisés, qui sont aux mains de Daech, susceptibles de passer à l'acte, et à la fois des gens de plus en plus pratiquants, qui revendiquent une expression religieuse de l'islam. Nous devons cesser d'être naïfs. Les passerelles ne sont pas systématiques mais elles existent.

De plus en plus de salariés, de plus en plus pratiquants, revendiqueront leur appartenance à la religion musulmane. D'une manière plus officielle, ils revendiqueront des droits d'expression religieuse dans l'entreprise. Cela ne veut pas dire que ce sont des djihadistes, même si cela n'en exclut pas la présence. Comment gérer les deux phénomènes ? Les signes distinctifs ne sont pas forcément physiques et visibles : les deux individus peuvent être ou voilés ou barbus, pourtant, la différence entre un salafiste et un djihadiste est grande. La conscience populaire et les médias font l'amalgame entre les djihadistes et les salafistes alors que cela n'a rien à voir. Alors que les deux processus distincts sont en marche.

C'est incontestable, les entreprises sont et seront des cibles potentielles de la menace terroriste, surtout celles qui représentent le mode de vie occidental : les entreprises de consommation, les industries culturelles, du luxe, les grands magasins… Et, parallèlement à cela, toutes les entreprises de France sont confrontées à la montée de la revendication musulmane des musulmans de France. Les jeunes musulmans de France disent : « *Nos parents ont rasé les murs pendant 40 ans. Nous, maintenant, on va faire comme les catholiques, comme les chrétiens, comme les juifs : on est musulmans, on se revendique en tant que tels, on n'est pas des terroristes mais on va afficher notre islam et on va afficher notre manière de vivre l'islam en France* ». De plus en plus viendront travailler en djellaba, voilées etc… Et ils répondront « *non mais attendez, d'accord je mets le voile, mais pourquoi mon collègue qui vient avec la kippa depuis 20 ans on ne lui dit rien à lui ?* ». Pour le monde de l'entreprise, c'est LE sujet de demain, avec tout ce que cela entraîne de traumatismes, d'incompréhensions, d'islamophobie, etc.

Le pays en général et les entreprises en particulier, sont confrontés à l'émergence de pratiques religieuses très rigoureuses. Les principes de la République laïque interdisent, paradoxalement, tout débat ! Sarkozy l'a lancé en 2007 avec son livre sur la place des religions. Depuis, rien ! Doit-on, ou non, mettre des limites à l'exercice du fait religieux sur l'espace public ? On parle du djihadisme, du salafisme, mais pas de la place de l'islam dans la République.

Il y a une communautarisation religieuse d'un certain nombre de structures publiques ou privées et de certains secteurs d'activités, avec des gens pour la plupart issus du Maghreb ou de l'Afrique et qui sont musulmans. C'est le cas des taxis, des employés à Roissy ou à Orly et, de façon générale, de tous les métiers attenants à la logistique des sites. Les syndicats eux même sont très souvent tenus par ces communautés. La mixité commence à être en question dans ces secteurs et ces métiers.

? Avez-vous des demandes particulières émanant d'acteurs économiques locaux concernant des mesures renforcées de sécurité ? Quels sont les secteurs les plus en demande (sites commerciaux, banques, industries, transports…) ? Si oui, quels sont les moyens susceptibles d'être mis en œuvre et avez-vous la marge de manœuvre pour y répondre (patrouilles de Police-renseignement…) ?

Nous sommes tous des cibles potentielles. Tous. Tout le monde est concerné. Les messages de Daesh s'adressent à tous les « déstructurés » de notre société qu'ils récupèrent dans nos quartiers, mais pas seulement. « *Tuez toux ceux que vous pouvez, tout ce qui bouge, faut taper : les élus, les fonctionnaires, les policiers, les femmes, ceux qui font de la musique, tout le monde, les journalistes, les juifs, tout le monde* ». Ils incitent à des actions imprévisibles. Ce sont des « bombes humaines » qui peuvent exploser à n'importe quel moment, sur n'importe quelle cible. Malgré les efforts des services de l'État, il n'y a malheureusement aucune raison pour que cela n'arrive pas.

Les entreprises les plus exposées sont celles qui relèvent des secteurs de la Défense et de la sécurité, bien qu'elles disposent de dispositifs de protection spécifiques. Ensuite, ce sont celles présentes sur les plateformes aéroportuaires. Les entreprises qui ont joué le jeu de « l'embauche de proxi-

mité » se sont exposées à la radicalisation djihadiste. Les médias ont largement relayé le sujet (le lendemain du 13 novembre, une centaine de fiches S a été détectée à Roissy).

Dans nos quartiers, ce sont les petits commerces qui se sentent démunis et qui sollicitent notre aide.

À Sarcelles, l'économie locale est basée sur la communauté musulmane. Ce sont surtout les plus petits commerces traditionnels qui sont touchés, ceux de confession juive n'ont plus de clients, ils sont menacés, mettent la clé sous la porte et s'en vont.

La drogue est aussi un vrai problème parce que c'est une économie souterraine et qu'elle tue l'économie réelle. Les dealers rodent dans les magasins toute la journée.

Sarcelles souhaite mettre en place un programme de prévention de la radicalisation, qu'en est-il ? En quoi votre commune est-elle particulièrement touchée par la radicalisation violente ? En quoi consiste-t-il et prend-il en compte des besoins spécifiques des entreprises ?

Pour faire face à la radicalisation religieuse, je suis allé voir des spécialistes et nous avons essayé de créer une structure qui soit à la fois une structure de formation des élus et des agents municipaux sur le radicalisme. C'est une structure de prévention pour les jeunes qui ne sont pas encore radicalisés, mais qui sont approchés par les réseaux. On s'occupe généralement de ceux qui sont partis faire le djihad et on attend que la catastrophe arrive. Cette structure est faite pour empêcher que cela arrive. Cela suppose de faire un effort considérable de sensibilisation, d'éducation et de prise en charge avec des psychologues, des analystes comportementaux, etc…

Nous sommes livrés à nous-mêmes localement. Il y a un manque criant de soutien de la part des pouvoirs publics ! L'État a pourtant les capacités d'avoir une vision précise de ce qui se passe et de comment ces réseaux s'organisent sur le territoire : des associations qui s'implantent, des écoles salafistes qui s'ouvrent, des têtes de réseaux… Nos services de renseignement sont performants. Ce qu'il manque aujourd'hui, ce sont des structures de prise en charge qui permettent de réagir face à un phénomène constaté. Exemple, à Sarcelles, il y a deux écoles a priori très proches des réseaux salafistes. Légalement, nous ne pouvons rien faire sauf, peut-être, de la prévention auprès de ces enfants qui, a l'âge de 5-6 ans, si on ne s'interfère pas, sont pris en charge par des réseaux…

Du 3 au 7 octobre, les Sarcellois ont eu la possibilité de se prononcer par bulletin sur l'opportunité d'armer la police municipale. La consultation citoyenne sur un sujet aussi régalien est osée. Pensez-vous qu'elle pourrait-être appliquée à l'échelle nationale ?

Ce référendum vise à savoir s'il faut, ou non, armer la police municipale. Comment continuer de demander à des policiers municipaux qui n'ont pas d'armes d'aller garder une synagogue ? Aujourd'hui, ils gardent des synagogues à côté de militaires qui ont leur *Famas* avec balle engagée. La police nationale fait régulièrement appel à la police municipale, mais elle n'a pas les mêmes moyens de défense.

L'État ne pourra pas continuer à assurer seul la sécurité. Les policiers, les gendarmes, les militaires n'en peuvent plus. Il faudra les former et il faudra des doctrines d'emploi qui, bien sûr, évolueront.

L'État est-il en mesure d'assurer la sécurité sur un territoire jugé particulièrement sensible ou bien recourez-vous à la sécurité privée ? Comment s'organisent les moyens privés ou publics sur le territoire ?

L'État, seul, n'a plus forcément la capacité de couvrir tous les grands évènements qui se déroulent au quotidien en Île-de-France et en province. Un transfert de ses missions auprès de structures privées pourrait se présenter comme une solution efficace. ■

ALAIN ZABULON

Directeur de la Sûreté, du Management des Risques et de la Conformité – ADP

Percevez-vous une aggravation de la menace terroriste sur votre secteur d'activité ? Les attentats représentent-ils un risque majeur dans les espaces dédiés aux transports en commun ?

Oui incontestablement. La menace vise tous les modes de transport. N'oublions pas que, depuis 1980, une quinzaine d'attentats a visé les gares et aérogares européennes. S'agissant plus précisément du transport aérien, les groupes terroristes, et notamment les deux principaux, Daech et Al Qaida, désignent régulièrement ce mode de transport comme une cible prioritaire en visant soit l'avion soit, plus récemment, les aéroports. Les attentats meurtriers contre l'aéroport de Bruxelles, le 22 mars 2016, et celui d'Istanbul, pourtant réputé bien protégé le 28 juin dernier, confirment cette tendance.

Une évolution du cadre juridique est-elle nécessaire ? La loi Savary trouvera-t-elle une application en mars 2016 dans les espaces aéroportuaires ?

Les espaces aéroportuaires sont déjà régis par des règles spécifiques. Celles-ci sont définies par l'Organisation de l'Aviation Civile Internationale (OACI), sous forme de recommandations, et par l'Union européenne, sous forme de réglementations applicables à tous les États membres. La sûreté aéroportuaire, c'est-à-dire la protection des avions contre les actes de malveillance, n'a cessé de se renforcer depuis les attentats du 11 septembre. Chacun peut s'en rendre compte en tant que passager à l'occasion des contrôles de sûreté obligatoires pour accéder à l'avion. L'objectif de ces contrôles est de garantir le même niveau de sûreté dans tous les aéroports. Les aéroports non reconnus comme sûrs peuvent se voir imposer la mise en œuvre de contrôles supplémentaires pour se conformer aux standards requis. Les gestionnaires d'aéroports sont tenus au strict respect de ces règles qui s'imposent aux États, lesquels encourent des sanctions en cas de manquement. En revanche, la sûreté dans les aérogares, ouvertes au public, n'est pas enserrée dans des règles internationales aussi strictes, et les États ont une grande latitude pour définir et faire appliquer les dispositions réglementaires qu'ils édictent. En France, les aérogares, parkings et linéaires d'accès, sont placés sous la protection de l'État, ce qui n'empêche pas le gestionnaire de déployer des mesures de surveillance avec ses moyens propres.

Les investissements en matériels et dispositifs de sûreté qui contribuent à maintenir la confiance des consommateurs/visiteurs ne cessent de croître depuis les attentats du 13 novembre 2015. Ne faudrait-il pas définir un standard de sûreté en deçà duquel un modèle économique n'est plus jugé comme viable ? Par exemple, serait-il pertinent, selon vous, de généraliser le régime de protection des OIV aux secteurs plus particulièrement exposés à la menace ? Une transposition de l'arrêté du 11 septembre 2013, relatif aux mesures de sûreté de l'aviation civile, pourrait-elle-être envisagée aux autres secteurs d'activité ?

Les investissements et matériels dédiés à la sûreté aéroportuaire sont certifiés par l'État et financés, comme toutes les autres dépenses de sûreté, par une taxe d'aéroport prélevée sur le billet d'avion. Pour les aéroports franciliens, cette taxe est de 11,50 euros. C'est le prix à payer pour avoir la certitude d'embarquer dans un avion dont les passagers, les personnels navigants et les bagages ont été contrôlés. Le modèle français de financement de la sûreté fait reposer l'intégralité du financement de la sûreté sur le transport aérien – passagers et compagnies – et non sur le contribuable. Ce modèle économique, qui a fait ses preuves, est aujourd'hui questionné car il repose sur les acteurs économiques du transport aérien dans un environnement fortement concurrentiel. Si les dépenses de sûreté devaient continuer à augmenter sous l'effet de la menace terroriste, d'autres voies de financement devraient être alors imaginées.

Sans entrer dans le détail des dispositifs de protection et de surveillance (ostentatoire-discrète), quelles sont les tendances à privilégier ?

Outre les mesures réglementaires de sûreté aéroportuaires obligatoires évoquées plus haut, et que le groupe ADP applique avec la plus grande rigueur, nous avons déployé des mesures complémentaires en zone publique, non en substitution, mais en complément de ce que fait l'État : rondes de surveillance, déploiement d'équipes cynophiles de détection d'explosifs, contrôle aléatoire à l'entrée des terminaux, recours massif à la vidéo protection (8 000 caméras déployées dans nos aéroports), sont quelques-unes des mesures que nous avons mises en œuvre après les attentats de 2015. Nous avons également recours à des agents de détection comportementale, discrètement placés à certains endroits stratégiques des aérogares, et nous formons nos agents en poste en zone publique à cette technique.

Les directions sûreté ont-elles la marge de manœuvre suffisante pour mettre à niveau les dispositifs de sûreté ?

Si nous n'avons pas de marge de manœuvre pour modifier, de notre propre initiative, les règles de sûreté aéroportuaire qui obéissent à des standards internationaux, nous avons pu décider assez librement des mesures additionnelles en zone publique. Nous avons pris le soin, toutefois, de nous concerter très étroitement avec les services locaux de l'État, placés sous l'autorité du préfet.

Quelles sont les mesures exceptionnelles qui pourraient assurer la continuité des activités dans un contexte d'état d'urgence ? Les pouvoirs publics peuvent-ils en faciliter la mise en œuvre ?

La décision du gouvernement de décréter l'état d'urgence au soir des attaques terroristes du 13 novembre n'a pas entravé la continuité d'activité de nos aéroports. En revanche, le durcissement, au demeurant nécessaire, des contrôles aux frontières, a provoqué un allongement significatif du temps d'attente aux aubettes de la police de l'air et des frontières (PAF). Conscient de cette situation, le ministre de l'Intérieur a consenti des moyens humains supplémentaires, tandis que le groupe ADP porte et finance intégralement un programme de développement du contrôle automatisé aux frontières avec les sas Parafe. De manière plus générale, comme tous les opérateurs d'importance vitale (OIV), le groupe s'est doté d'un plan de continuité d'activité, destiné à répondre à des situations très dégradées. Il faudrait un évènement, naturel ou intentionnel, d'une ampleur exceptionnelle pour mettre nos aéroports à l'arrêt.

Les dommages causés sur la voie publique peuvent impacter considérablement l'image d'une entreprise. Jusqu'où la manœuvre sûreté est-elle à la charge de l'entreprise ? La protection périmétrique/périphérique ne nécessite-t-elle pas une présence des forces publiques quasi systématique ? Les relations avec les partenaires publics (Préfectures ; police et gendarmerie en fonction des secteurs de compétences ; services de renseignement) sont-elles renforcés ?

Comme je l'ai expliqué, la zone publique est sous le contrôle et la protection de l'État. La protection périphérique, qui ceinture l'ensemble de la zone aéroportuaire, est surveillée par la gendarmerie du transport aérien, les militaires de l'opération *Sentinelle* et les équipes du groupe ADP. Les relations avec les partenaires publics sont intenses, et se sont renforcées sous la pression de la menace terroriste. L'État a consenti des efforts significatifs en matière d'effectifs. À titre d'exemple, les effectifs des services de renseignement sur Roissy ont été plus que doublés dans la période récente. La vie quotidienne de quelque cent mille salariés sur nos plateformes, partagée avec celle des fonctionnaires de l'État, crée un écosystème public/privé original et propre au milieu aéroportuaire. Nous vivons quotidiennement avec l'État qui nous contrôle et nous protège.

Les prestataires privés de sécurité sont-ils en mesure de répondre qualitativement aux besoins du secteur ? Qu'en est-il du contrôle de la sous-traitance et de la fiabilité des agents ? L'armement d'agents privés de sécurité est-il une solution ?

Les procédures de contrôles de sûreté, appliquées aux passagers, aux personnels et aux bagages, sont mises en œuvre par des entreprises privées sélectionnées par des appels d'offres dont les cahiers des charges sont particulièrement exigeants. Les salariés de ces entreprises doivent avoir la qualification d'agent de sûreté aéroportuaire, ils sont sélectionnés sur des bases rigoureuses et doivent passer par trois enquêtes successives de police avant de pouvoir exercer dans les aéroports. Leur travail est très contrôlé par les équipes d'ADP et les services de l'État. Les manquements aux procédures constatés peuvent donner lieu à des sanctions et à l'application d'un malus financier à l'encontre de l'employeur. C'est peu de dire que ce domaine d'activité, qui fait travailler quelque 5 000 salariés sur les aéroports franciliens, est particulièrement surveillé en raison de la sensibilité des missions de sûreté.

S'agissant de l'armement des personnels, la profession aéroportuaire ne revendique pas un droit à l'armement pour les personnels privés puisque la protection des personnes et des biens incombe à l'État qui est fortement présent sur site.

Le recrutement de futurs salariés ou sous-traitants requiert aujourd'hui davantage de vigilance de la part des directions sûreté et des RH. Ces derniers sont-ils sensibilisés à la question de la « radicalisation » ? Est-ce dans leurs prérogatives que d'en déterminer les critères ? Peuvent-elles en référer aux services de l'État ? En cas de comportement d'un salarié traduisant un risque de « radicalisation » ou de basculement vers la violence, la circulation des informations (montantes/descendantes) entre les services de l'État et l'employeur est-elle en vigueur ?

Le phénomène de la radicalisation religieuse, devenue en quelques années une question sociétale des plus sensibles concerne toutes les strates de la société et n'épargne évidemment pas le monde de

l'entreprise. N'oublions pas que le principe de laïcité et son corollaire, celui de la neutralité ne s'impose que dans les services publics et non dans l'entreprise privée, sauf pour celles qui exercent une mission de service public. Il en résulte que l'expression des convictions religieuses, mais aussi politiques, philosophiques ou syndicales est protégée par le droit positif et ne peut faire l'objet d'une interdiction absolue. L'employeur peut en revanche poser des limites à cette liberté à la condition que celles-ci soient proportionnées et justifiées par des motifs liés au bon fonctionnement de l'entreprise.

Toute la difficulté pour les managers et les responsables RH est de faire la part entre l'expression autorisée des convictions religieuses et la radicalisation religieuse qui se traduit par des comportements, attitudes ou propos qui entrent en conflit avec les valeurs de la République et peuvent gêner le bon fonctionnement de l'entreprise.

Dans nos aéroports franciliens, et notamment à Roissy, le préfet délégué a retiré ou refusé plus de quatre-vingts habilitations administratives à des salariés pour des faits de radicalisation. Aucun salarié d'ADP n'a été touché par cette mesure qui traduit de la part de l'État une sévérité accrue que nous approuvons sans réserves.

S'il fallait brosser brièvement une typologie caractérisant ce qu'est la radicalisation, on pourrait mentionner parmi les motifs de retrait d'habilitations par le préfet :

- des cas de salariés refusant de travailler sous l'autorité d'une femme ;
- des comportements de prosélytisme agressif portant atteinte à la liberté de conscience des autres salariés ;
- des prises de position pouvant s'apparenter à une apologie du terrorisme, ou un appel à la discrimination et à la haine raciale, faits qui, rappelons le, constituent des délits pénalement répréhensibles.

Le groupe ADP a, pour sa part, mis en place une formation à la radicalisation religieuse au profit de ses cadres et managers de proximité pour leur donner les outils conceptuels et d'analyse leur permettant de détecter, d'analyser, et de signaler les cas de radicalisation. Ces formations rencontrent un grand succès car elles répondent à une attente forte de l'encadrement face à un phénomène qui les laissait jusqu'alors démunis.

L'enjeu est majeur pour la cohésion sociale de nos « villages aéroportuaires » dont la sociologie reflète la grande diversité des bassins d'emplois de l'agglomération parisienne dans lesquels nos entreprises puisent pour satisfaire leurs besoins de recrutement. Si nous voulons préserver ce modèle social respectueux de la diversité des origines de nos salariés, nous devons être très fermes sur la dérive que représente la radicalisation religieuse, dont les comportements sectaires qu'elle induit sont porteurs d'un risque de fracturation de notre tissu social. L'enjeu ainsi défini, n'est pas fondamentalement différent de celui qui se pose à la société française dans son ensemble.

? Les situations de post attentat ont montré des salariés en état de choc. Quelles sont les mesures pouvant être mises en place par les directions sûreté avec les RH pour gérer ce risque ?

Je voudrais d'abord souligner l'extraordinaire sang-froid de nos salariés qui, dans la nuit tragique du 13 au 14 novembre 2015, étaient sur le pont pour mettre en œuvre les premières mesures décidées par le gouvernement lors de l'exceptionnel conseil des ministres qui a suivi de quelques heures les attentats de Paris. Pour autant, nos salariés sont des hommes et des femmes qui s'inquiètent légitimement de leur sécurité, conscients que les aéroports sont des cibles de choix pour les terroristes. Les attentats de 2016 contre les aéroports de Bruxelles et d'Istanbul leur ont hélas donné raison.

Pour répondre à ce besoin de sécurité, nous avons déployé toute une série de mesures dont j'ai donné le détail plus haut (rondes de surveillance, contrôles aléatoires, video protection etc.).

Nous y avons ajouté un plan de sécurisation pour l'accès aux locaux professionnels non ouverts au public.

Nous avons également mis en place un plan de formation à la détection comportementale en faveur des quelque 1 200 agents d'ADP en poste dans la zone publique des aérogares.

D'une manière plus générale, le renforcement des moyens de l'État dans le cadre du plan d'urgence (effectifs de police, militaires du dispositif Sentinelle, renfort des services de renseignement), améliore notre niveau de protection pour les passagers mais aussi pour les salariés.

Nous sommes conscients qu'un aéroport est un lieu par définition ouvert et largement accessible et que la parade absolue contre une attaque terroriste n'existe pas. Cette réalité ne constitue pas une raison pour faire preuve de fatalisme, c'est au contraire une puissante incitation à améliorer sans relâche notre politique de sécurité dont nos salariés sont des acteurs de premier plan par la vigilance et le professionnalisme dont ils font preuve au quotidien. ■

GROUPE ADP

Le Groupe ADP est un leader mondial de la conception, de la construction et de l'exploitation d'aéroports. Il compte 3 aéroports (Paris-Charles de Gaulle, Paris-Orly, et Paris-Le Bourget), 1 héliport (Issy-les-Moulineaux) et 10 aérodromes (Chavenay-Villepreux, Chelles-le-Pin, Coulommiers-Voisins, Étampes-Mondesir, Lognes-Emerainville, Meaux-Esbly, Persan-Beaumont, Pontoise-Cormeilles-en-Vexin, Saint-Cyr-l'École, Toussus-le-Noble).

Le groupe ADP c'est aussi : 172 compagnies aériennes – 476 villes nationales et internationales desservies depuis Paris – 2 916 millions € de chiffre d'affaires – 95,4 millions de passagers – 34 aéroports dans le monde

Pour en savoir plus : http://www.parisaeroport.fr/groupe/groupe-et-strategie/essentiel

STÉPHANE GOUAUD

Directeur de la Sécurité – RATP

Les attentats représentent-ils un risque majeur dans les espaces dédiés aux transports en commun ? Quels sont le rôle et les actions de la RATP en la matière ?

La sécurisation du réseau RATP, qu'empruntent chaque jour plus de 10 millions de voyageurs, est un défi quotidien, permanent et en constante évolution, notamment pour ce qui est de la menace terroriste. Si la lutte contre le terrorisme relève des services spécialisés de l'Etat, la RATP, dont les réseaux ont été touchés à plusieurs reprises, s'est particulièrement investie dans le domaine de la prévention et du traitement des conséquences de l'acte terroriste. A cet égard, la RATP est en liaison constante avec les autorités pour relayer dans ses espaces la mise en œuvre des mesures du plan VIGIPRATE. La RATP sensibilise, en outre, ses voyageurs à la vigilance au travers de sa campagne « Attentifs ensemble », qui se décline en affiches et messages sonores. La RATP est, par ailleurs, impliquée dans l'élaboration des procédures qui seraient mises en œuvre en cas d'action terroriste. Ces procédures sont testées et sans cesse améliorées au travers d'exercices de grande ampleur organisés par les pouvoirs publics et/ou la RATP. Ces exercices préparent et entraînent les acteurs qui seraient mobilisés. Sur le plan de l'innovation, la RATP a développé un dispositif unique en son genre d'équipiers NRBCe (nucléaire, radiologique, biologique, chimique et explosifs), une centaine d'agents représentant l'ensemble des métiers opérationnels, formés par des professionnels de la sécurité civile.

Quels sont les moyens techniques, humains et financiers consacrés par la RATP à la sûreté de ses espaces ?

La RATP, qui considère la sécurité comme une composante essentielle de sa mission de service public et un élément essentiel de la continuité de service, compte parmi les seuls opérateurs de transport urbain au monde à bénéficier d'une internalisation aussi forte de la sûreté au sein de l'entreprise. Nous y consacrons des moyens humains, techniques et financiers très importants, avec un budget de fonctionnement moyen de 100 M€ environ par an. La forte présence humaine est au cœur de notre dispositif de sécurisation, avec notamment nos 1 000 agents du Groupement de Protection et de Sécurisation des Réseaux, dont les compétences sont définies par le législateur, et qui assurent, chaque jour, des missions de prévention, de dissuasion et de sécurisation. Assermentés et autorisés au port d'arme, les agents du GPSR font l'objet d'un recrutement strict et d'un long processus de formation. Cette présence humaine sur le réseau est complétée par les 6 000 agents de stations et gares qui sont, eux aussi, en position de vigilance. En complémentarité de cette présence humaine, nous déployons des moyens techniques importants, au premier rang desquels la vidéoprotection, outil indispensable dans la chaîne de sécurisation et l'aide à la décision, avec près de 40 000 caméras au total, dans nos matériels roulants, nos quais et nos couloirs. Cette articulation entre moyens humains et moyens techniques, ainsi que la coordination avec les forces de police, permettent des délais d'intervention inférieurs à 10 minutes après signalement dans 85% des cas.

Que change concrètement la loi Savary ?

La Loi Savary renforce les prérogatives de nos agents du GPSR. Depuis le 9 juin dernier, après une phase de sensibilisation des voyageurs, les agents du GPSR peuvent procéder à des inspections visuelles et à des fouilles. 25 inspections et fouilles sont réalisées en moyenne chaque jour sur nos réseaux. Aucun incident n'a été recensé à ce stade. Les agents du GPSR vont également pouvoir procéder à des palpations, selon un périmètre défini par arrêté préfectoral, et seront formés en conséquence. Enfin, ils pourront exercer leurs missions en civil, armés et assermentés, dans des conditions restrictives, définies en accord avec la Préfecture de Police. Ces agents

sont recrutés parmi les agents les plus expérimentés du GPSR et formés à cet effet. Ces missions en civil vont être réalisées en complémentarité et en coordination avec les services de Police.

Sans entrer dans le détail des dispositifs de protection et de surveillance (ostentatoire-discrète), quelles sont les tendances à privilégier ?

Nous souhaitons, en premier lieu, continuer à faire de la présence humaine le pilier fondamental de notre dispositif de sécurisation. Nous nous réjouissons à cet égard de notre nouveau contrat avec le STIF, l'autorité organisatrice des transports d'Île-de-France, qui prévoit le recrutement de 100 agents de sûreté supplémentaires. Nous sommes, par ailleurs, attentifs à toute innovation pouvant permettre d'assurer une meilleure sécurisation. Par exemple, nous allons expérimenter dès les prochaines semaines un système de caméras intelligentes à la gare de Châtelet-les-Halles. Ce système doit faciliter la détection de flux inhabituels de personnes, le stationnement de personnes devant des endroits sensibles, la détection de personnes tombant par terre au même moment ou encore la possibilité de retrouver une personne dans nos espaces. Face à la multiplication des colis suspects (*+60% sur les huit premiers mois de 2016, comparés à la même période en 2015*), la RATP souhaite également trouver des solutions alternatives à l'intervention systématique des équipes de déminage. Une expérimentation de chiens renifleurs d'explosifs va ainsi être menée prochainement sur le RER A qui concentre à lui seul 30 % des colis suspects.

Jusqu'où la manœuvre sûreté est à la charge de l'entreprise ? La protection périmétrique/périphérique ne nécessite-t-elle pas une présence des forces publiques quasi systématique ? Les relations avec les partenaires publics (Préfectures; Police et Gendarmerie en fonction des secteurs de compétences; services de renseignement) sont-ils renforcés ?

La sûreté de nos réseaux est évidemment un défi partenarial, auquel nous répondons de manière partagée et en étroite collaboration avec tous les services concernés de l'État, de la Police… dans le respect des compétences de chacun. Depuis de nombreuses années, la RATP conduit un partenariat actif avec les forces de police et notamment la Brigade des Réseaux Franciliens qui a une compétence étendue à la totalité des réseaux ferrés d'Île-de-France. De nombreuses opérations conjointes et coordonnées, visant à une présence dissuasive, une sécurisation renforcée ou une visibilité accrue, sont ainsi menées, en fonction des circonstances et de l'analyse conjointe.

Le recrutement de futurs salariés ou sous-traitants requiert aujourd'hui davantage de vigilance de la part des directions sûreté et des RH. En cas de comportement d'un salarié traduisant un risque de « radicalisation » ou de basculement vers la violence, la circulation des informations (montantes/descendantes) entre les services de l'État et l'employeur est-elle en vigueur ?

Nous faisons confiance aux autorités pour nous signaler toute information qu'ils jugeraient utiles, relatives à nos personnels. Nous pouvons ainsi être informés d'une décision administrative concernant l'un de nos salariés. Par exemple, si un salarié se voit retirer, sur décision administrative, son assermentation ou son port d'arme s'agissant d'un agent de sécurité, cette décision nous est communiquée, mais sans précision quant aux motifs. Nous prenons ensuite les mesures qui s'imposent, c'est-à-dire la révocation pure et simple.

Le Groupe **RATP** est le cinquième acteur mondial du transport public. Métro, rail, tramway, bus, la RATP est présente sur tous les modes de transport collectifs. En Île-de-France, elle exploite, entretient, modernise et développe l'un des réseaux multimodaux les plus denses au monde. Chaque jour, elle transporte plus de 14 millions de personnes en France et dans le monde. Cette expérience, la RATP et ses filiales l'exportent sur tous les continents. Unis par le sens du service public, les 57 976 hommes et femmes du Groupe partagent un même objectif : permettre aux voyageurs de se déplacer sereinement, rapidement et dans un maximum de confort.

LOI SAVARY

La loi n°2016-339 du 22 mars 2016, dite « Loi Savary », vise, comme son nom l'indique, à renforcer « la prévention et [...] la lutte contre les incivilités, contre les atteintes à la sécurité publique et contre les actes terroristes dans les transports collectifs de voyageurs » et confère, à cette fin, des pouvoirs élargis aux autorités comme aux agents des réseaux de transports publics.

Ainsi, pour mieux prévenir les actes terroristes dans les transports en commun, le titre I de la loi instaure un nouveau pouvoir d'inspection visuelle et de fouille des bagages au bénéfice des forces de l'ordre. Il simplifie également les règles de compétence territoriale des procureurs de la République en matière de délivrance de réquisitions de contrôles d'identité à bord des trains traversant plusieurs ressorts territoriaux. Enfin, il autorise les agents des services internes de sécurité de la SNCF et de la Régie autonome des transports parisiens (RATP) à procéder à des inspections visuelles et aux fouilles de bagages ainsi qu'à des palpations de sécurité (art. 1). Ainsi, ces derniers bénéficient désormais des mêmes pouvoirs que les agents de sécurité privée.

Les agents des services internes de sécurité de la SNCF et de la RATP pourront, en outre, expérimenter, à partir du 1er janvier 2017, un enregistrement audiovisuel de leurs interventions (au moyen de caméras individuelles) lorsque se produit ou est susceptible de se produire un incident.

Par ailleurs, les décisions de recrutement et d'affectation concernant en particulier les emplois en lien direct avec la sécurité des personnes dans les transports publics peuvent être précédées d'enquêtes administratives destinées à vérifier que le comportement des personnes intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées.

Pour aller plus loin :

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032282279&categorieLien=id
http://www.textes.justice.gouv.fr/art_pix/JUSD1601954C.pdf

LOI URVOAS

La loi n° 2016-731 du 3 juin 2016, dite « Loi Urvoas », renforce la lutte contre le crime organisé, le terrorisme et leur financement, et améliore l'efficacité et les garanties de la procédure pénale. Le criblage a été rendu possible par cette loi, pour contrôler l'accès aux grands évènements des personnes qui ne sont ni spectateurs, ni participants.

Pour aller plus loin :

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032627231&categorieLien=id

JEAN-LOUIS FIAMENGHI

Directeur de la sûreté – VEOLIA

Percevez-vous une aggravation de la menace terroriste sur votre secteur d'activité ? Les attentats représentent-ils un risque majeur dans votre secteur ?

Au niveau France, je ne perçois pas d'augmentation de la menace sur nos structures françaises. Cela tient au fait que, en tant qu'opérateur d'importance critique, un travail préventif a été réalisé en coopération avec l'État. Des dispositifs de protection des sites et des salariés ont donc déjà été mis en place. L'État, à travers le SGDSN, oblige les opérateurs à mettre en place des PSO (Plan de Sécurité Operateurs), déclinés au niveau des sites par des PPP (Plan Particuliers de Protection), eux-mêmes complétés par des PSE (Plans de Sécurité Extérieurs), ces derniers restant à la charge du Département. Ce sont les zones de compétences publiques et privées.

Concernant l'évaluation de la menace, elle est de plus en plus prégnante à l'étranger, notamment en Afrique, où sont engagés nos salariés. Depuis la jurisprudence Karachi, nous devons adopter des mesures de protection pour répondre à l'obligation de sécurité envers les salariés. Le code du travail oblige à garantir la sécurité et pas la sûreté.

Par voie de conséquence, le rehaussement du niveau de sécurité va contribuer à intégrer la sûreté dans le fonctionnement stratégique de l'entreprise. Quand l'entreprise vend un service, il sera forcément accompagné d'un service intégré de sûreté. C'est ce que nous faisons avec l'ANSSI dans le domaine du cyber. Grâce au rehaussement du niveau de sécurité et de sûreté, que l'État nous impose de mettre en œuvre, la direction sûreté est de plus en plus associée, en amont, à la stratégie de développement de l'entreprise.

Il y a une véritable opportunité à étendre ce fonctionnement. La notion de sûreté doit devenir un préalable au fonctionnement et au développement de toute entreprise, même de petite taille. Cette démarche tend à s'inscrire dans la continuité, notamment face à la menace terroriste à l'international et sur le territoire national. L'entreprise doit se préparer à faire face à toutes formes de radicalisme, telles que l'éco-terrorisme, le zaydisme…

Les investissements en matériels et dispositifs de sûreté, qui contribuent à maintenir la confiance des consommateurs/visiteurs, ne cessent de croître depuis les attentats du 13 novembre 2015. Ne faudrait-il pas définir un standard de sûreté en deçà duquel un modèle économique n'est plus jugé comme viable ? Par exemple, serait-il pertinent, selon vous, de généraliser le régime de protection des OIV aux secteurs plus particulièrement exposés à la menace ? Une transposition de l'arrêté du 11 septembre 2013, relatif aux mesures de sûreté de l'aviation civile, pourrait-elle être envisagée aux autres secteurs d'activité ?

Même s'ils sont coûteux pour l'entreprise, dans un contexte propice à la réduction des dépenses, il y a un intérêt à rassurer le consommateur. Intégrer la notion de sûreté dans leur offre est un motif de différentiation et de compétitivité. L'achat de certains process permet d'emporter certains marchés. L'État ne peut pas tout, mais il faut donner la possibilité à la sécurité privée d'évoluer dans son statut, la réglementation, les formations…

Sans entrer dans le détail des dispositifs de protection et de surveillance (ostentatoire-discrète), quelles sont les tendances à privilégier ?

Les technologies permettent au dispositif d'être plus efficient, elles le renforcent mais il faut savoir les combiner avec l'humain.

Les directions sûreté ont-elles la marge de manœuvre suffisante pour mettre à niveau les dispositifs de sûreté ?

La marge se fait par rapport au niveau et à la nature du risque et à l'investissement de l'entreprise, c'est une question budget et de stratégie de l'entreprise.

Quelles sont les mesures exceptionnelles qui pourraient assurer la continuité des activités dans un contexte d'état d'urgence ? Les pouvoirs publics peuvent-ils en faciliter la mise en œuvre ?

L'état d'urgence exige des mesures exceptionnelles et, en cas d'attentat, une capacité de réaction immédiate de la part des forces de l'ordre. L'État ne devrait-il pas faire évoluer le statut de la sécurité privée en terme de réglementation, de droit, mais surtout de formation afin de pouvoir se concentrer sur des actions proprement régaliennes et déléguer ainsi un certain nombre de missions ?

Les dommages causés sur la voie publique peuvent impacter considérablement l'image d'une entreprise. Jusqu'où la manœuvre sûreté est-elle à la charge de l'entreprise ? La protection périmétrique/périphérique ne nécessite-t-elle pas une présence des forces publiques quasi systématique ? Les relations avec les partenaires publics (Préfectures ; Police et Gendarmerie en fonction des secteurs de compétences ; services de renseignement) sont-ils renforcés ?

Sans parler de *Veolia*, de tout temps a existé des partenariats publics-privés pour garantir la sécurité avec les forces dans un périmètre donné. Sur une zone commerciale par exemple, il existe des co-productions de sécurité.

Les prestataires privés de sécurité sont-ils en mesure de répondre qualitativement aux besoins du secteur ? Qu'en est-il du contrôle de la sous-traitance et de la fiabilité des agents ? L'armement d'agents privés de sécurité est-il une solution ?

Aujourd'hui, la qualité n'est pas homogène en termes de prestation, car la formation généralisée n'existe pas encore.

Le recrutement de futurs salariés ou sous-traitants requiert aujourd'hui davantage de vigilance de la part des directions sûreté et des RH. Ces dernières sont-elles sensibilisées à la question de la « radicalisation » ? Est-ce dans leurs prérogatives que d'en déterminer les critères ? Peuvent-elles en référer aux services de l'État ? En cas de comportement d'un salarié traduisant un risque de « radicalisation » ou de basculement vers la violence, la circulation des informations (montantes/descendantes) entre les services de l'État et l'employeur est-elle en vigueur ?

Oui, l'État demande davantage de vigilance quant aux signaux faibles, au sujet des salariés travaillant, notamment, dans des sites protégés. En dehors de l'expression du phénomène religieux, qui ne pose pas de problème chez *Veolia* et qui est normalisé dans l'entreprise, il est dans les compétences des directions sûreté que d'être attentif au phénomène de radicalisation violente, qui n'est d'ailleurs du seul fait du Djiadisme. L'État a mis en place des procédures pour que ces signalements soient analysés par les services de renseignements. Concernant les procédures de criblage, elles entrent dans ce dispositif.

Les situations de post attentat ont montré des salariés en état de choc. Quelles sont les mesures pouvant être mises en place par les directions sûreté avec les RH pour gérer ce risque ?

Depuis les attentats, les directions sûreté proposent aux services RH des sensibilisations à la menace terroriste.

Quelles sont vos capacités de diffusion des bonnes pratiques auprès des directions générales de vos entreprises membres ?

Toutes les procédures et les études de la direction sûreté sont publiées sur le site Intranet. De plus, nous avons mis en place des *e-Learning* permettant de former le plus de salariés possible aux risques et menaces. ■

Présent sur les cinq continents avec 174 000 salariés, **Veolia** conçoit et déploie des solutions pour la gestion de l'eau, la gestion des déchets, et la gestion énergétique, participant au développement durable et à la compétitivité de ses clients. Le Groupe accompagne ainsi les industriels, les villes et leurs habitants, dans l'usage optimisé des ressources, afin d'en augmenter l'efficacité économique, environnementale et sociale. Grâce à ces trois cœurs de métiers complémentaires et synergiques, Veolia contribue à développer l'accès aux ressources, préserver les ressources disponibles et les renouveler.

PATRICK ESPAGNOL

Préfet, Directeur de la Sécurité et de l'Intelligence Économique - EDF

Nul ne doute aujourd'hui qu'il faille protéger le patrimoine des entreprises ; c'est une évidence économique, c'est aussi une obligation morale, éthique et juridique lorsqu'il s'agit du patrimoine humain.

L'état de la menace se maintient, en effet, à un niveau très élevé et ses manifestations sont de plus en plus polymorphes et complexes. Les cyber-attaques et le terrorisme, qui sont les plus redoutés, se combinent entre eux pour générer le cyber terrorisme.

Protéger le patrimoine humain implique tout d'abord de garantir la santé et la sécurité des agents ou des salariés, en particulier lors des déplacements à l'international. À cette fin, les grands Groupes et grandes entreprises ont créé des services spécialisés chargés d'analyser les menaces et les risques présents dans le pays de destination et de proposer des plans globaux de sécurité adaptés, à même d'accompagner la stratégie commerciale de l'entreprise, tout en veillant à la sécurité des collaborateurs. Une jurisprudence de plus en plus exigeante rappelle qu'en ce domaine, une obligation de résultat pèse sur l'employeur.

Chaque projet de déplacement dans les zones à forts risques fait l'objet d'une évaluation rigoureuse portant en particulier sur les conditions d'hébergement, de transport mais aussi sur le mode de vie au quotidien pour les longs séjours ou les expatriations. La protection du patrimoine informationnel doit impérativement être traitée, la captation d'informations sensibles pouvant aider les groupes terroristes à mieux cibler leurs actions. Cette mission concourt par ailleurs à protéger les savoirs faire des entreprises.

Même s'il s'agit de faits distincts, la radicalisation en milieu professionnel constitue une autre crainte des entreprises. Il importe de la dissocier de la pratique religieuse qui ne doit en aucun cas être empêchée ou contrecarrée. Face à des situations nouvelles et parfois complexes, les managers ne doivent pas rester seuls. Des guides sont souvent rédigés à leur attention afin de les aider dans l'analyse objective des faits observés ou rapportés. Dans de nombreux cas, le droit du travail ou pénal sont à même d'apporter des réponses.

Le traitement des personnes en voie de radicalisation ne peut être le fait de l'entreprise mais leur signalement aux services de l'État est cependant de leur responsabilité. Un avis des services de l'État peut être sollicité pour accéder à des installations sensibles, il reste cependant du chemin à parcourir afin d'étendre cette possibilité à des sites qui ne sont pas classés point d'importance vitale ou à des fonctions sensibles au sein des entreprises.

Face à ces nouveaux défis, acteurs publics et privés s'organisent pour concevoir et mettre en œuvre des ripostes adaptées. Elles doivent être empreintes d'une réelle volonté de co-production et de confiance partagée ; elles doivent, en outre, éviter toute surréaction sécuritaire qui ne pourrait que conduire à une inhibition de l'activité de l'entreprise voire de la nation de par la multiplicité des coups portés décrite dans la théorie des « Milles entailles ». C'est manifestement le but recherché par les agresseurs. ■

ZIAD KHOURY

Ex-directeur de la sûreté – Euro 2016 SAS

Quel a été le dispositif?

EURO 2016 SAS, la société d'organisation créée par l'UEFA et la FFF, a dû concevoir un schéma de sécurité tenant compte à la fois du contexte national et du caractère exceptionnel de l'évènement, troisième au monde.

Il s'agissait du plus grand EURO jamais organisé, comprenant 51 matches au lieu de 31 la fois précédente, 24 équipes contre 16, 5 semaines d'efforts continus (après trois ans de préparation active) et 110 sites officiels à sécuriser, dont bien sûr les 10 stades.

Son environnement était également exceptionnel, non seulement parce que l'EURO a été organisé sous le régime de l'état d'urgence, mais aussi parce qu'il a été globalement confronté à une pression de grande ampleur : mondialisation de l'évènement (spectateurs venant de plus de 200 pays, retransmission dans 170 d'entre eux avec partout des records d'audience), attractivité de celui-ci (27 millions de tweets avec la référence EURO 2016, 300 millions de visites sur le site internet) et diversité des menaces contre son bon déroulement.

Il y eut d'abord la crainte des casseurs, puis celle du terrorisme, celle des grèves avant et pendant la manifestation, des phénomènes très limités mais réels d'hooliganisme à son début, et même les inondations avant le match d'ouverture. Des menaces technologiques ont aussi été prises en compte comme les drones - avec un système innovant de surveillance et de neutralisation sur tous les stades et certains camps de base des équipes - ou la cybercriminalité (35 000 tentatives d'intrusion, toutes déjouées).

Plus généralement, il fallait à la fois maîtriser les risques endogènes, liés en premier lieu à la bonne gestion des sites et des flux, et prévenir les risques exogènes, par définition moins faciles à juguler et qu'un tel évènement attire par sa résonance.

Finalement, c'est le plus grand dispositif de sécurité publique et privé en France qui aura été déployé à cette occasion. Il l'a été dans un cadre stratégique unique, symbolisé par la signature d'un protocole sur la sécurité entre le ministère de l'Intérieur et les organisateurs en septembre 2015, et à travers un processus de préparation conjoint - aussi bien au niveau national que local (groupes de travail, réunions sur site, exercices, concertations sur les documents cadres produits) - qui aura permis de traiter tous les enjeux.

La sécurité a été considérée, dès le départ, comme une priorité élevée, avec des mesures plus strictes et plus complètes que celles habituellement mises en place pour des matches de football. Elles n'en étaient pas moins corrélées à l'analyse des risques, ce qui a d'ailleurs conduit à les renforcer après les actes terroristes de 2015, sans remettre en cause leur philosophie générale. Cette recherche de proportionnalité était à la fois dictée par les contraintes croissantes pesant sur les ressources publiques et privées de sécurité, et par la volonté d'éviter des surenchères contre-productives de moyens dans le contexte d'un évènement qui se voulait festif.

Pour les organisateurs, cela a impliqué le recours cumulé à environ 47 000 agents de sécurité privée pour le déroulement de tous les matches, et un chiffre du même ordre pour la sécurisation de l'ensemble des 110 sites. Plus de 12 000 agents ont retiré une accréditation à cette fin, après avoir fait l'objet d'un criblage par le ministère de l'Intérieur, comme l'ensemble des 100 000 personnes environ qui ont été accréditées. La moyenne d'agents de sécurité privée pour un match a été de 925, bien au-dessus des pratiques habituelles du championnat, compte tenu des besoins particuliers et du standing de l'EURO. Plus de 200 volontaires sont venus les appuyer à chaque match, afin de faciliter l'accueil et l'orientation des 2,5 millions de spectateurs, aux deux tiers étrangers.

Des moyens de contrôle spécifiques ont été également mis en place, que ce soit par la vidéo-surveillance, la détection de métaux, d'explosifs et de fumigènes ou encore les équipes cynophiles, de même qu'une sécurité passive renforcée (clôtures). Une attention particulière a été portée au contrôle des véhicules comme à la palpation des spectateurs.

Un périmètre supplémentaire de protection et de contrôle de l'accès au stade a été déployé, créant autour de celui-ci un large espace sécurisé, correspondant également aux besoins particuliers d'espace d'une telle organisation. C'est en général à ce périmètre extérieur qu'étaient effectuées les palpations, à la suite d'un premier contrôle visuel et chimique des billets. En amont, la police était susceptible d'organiser des pré-filtrages. Au total, avant d'accéder à son siège, le spectateur était donc contrôlé au moins trois fois par les organisateurs (périmètre extérieur, tripodes, vomitoires), muni de son billet très sécurisé et difficile à contrefaire.

Autour des équipes nationales, trois cercles de sécurité étaient mis en œuvre : la protection rapprochée par les services spécialisés de l'État, la protection des sites par l'organisateur, la protection périphérique par les services locaux de police et de gendarmerie. Les déplacements étaient toujours sous escorte et les lieux fréquentés par ces délégations officielles systématiquement déminés. Cet exemple illustre les interactions constantes entre organisateurs et État en vue d'une sécurité de l'événement nécessairement coproduite.

Le dispositif de sécurité de l'EURO aura donc suivi un principe de cohérence, à travers un projet unique de sécurité s'appliquant partout avec la même ambition, un principe d'anticipation, incluant un volet de coopération internationale et le choix des prestataires les plus qualifiés un an avant afin de leur laisser un temps suffisant de préparation, et enfin un principe de proportionnalité, fondé sur l'analyse conjointe des risques entre État et organisateurs.

Quel a été le partenariat public-privé ?

Le partenariat entre le secteur public et privé a d'abord été celui entre les autorités publiques, d'une part, et les institutions sportives (l'UEFA, la FFF), d'autre part, qui ont créé une société chargée d'exécuter les opérations liées à la préparation et au déroulement du championnat, EURO 2016 SAS. Ce modèle d'organisation était innovant comparé aux précédents événements du même ordre : s'il simplifiait l'organisation du côté sportif, avec une approche intégrée dans laquelle l'UEFA était motrice et assumait le risque financier, il rendait plus nécessaire encore la bonne coordination avec les pouvoirs publics, moins associés à l'organisation du tournoi.

Ce partenariat était aussi celui entre la sécurité publique et la sécurité privée, via les organisateurs. Jamais cette dernière n'avait été aussi impliquée dans la réussite d'un grand évènement, qui marquera une étape majeure dans son évolution. Dès le début, un groupe de liaison avec les représentants de la profession a été créé sur la suggestion des organisateurs et sous l'égide de l'État. Il s'est réuni une dizaine de fois et s'est métamorphosé en un groupe de contact opérationnel pendant le tournoi, permettant de répondre de façon rapide et coordonnée à des besoins imprévus.

Finalement, tous les services de sécurité, publics ou privés, ont été globalement au rendez-vous, dans une complémentarité fructueuse au sein de laquelle chacun avait une mission.

Cette même approche s'est retrouvée en matière de secours et de santé, dans la liaison entre services publics et prestataires associatifs ou privés. Aux organisateurs, une responsabilité de premier échelon dans les sites officiels ; à l'État, une responsabilité dans l'espace public ou dans ces sites, en cas de mise en œuvre d'une compétence spécialisée (NRBC par exemple) ou de gestion de crise.

Naturellement, la multiplicité des acteurs, la répartition des responsabilités et la complexité croissante de ces évènements ont nécessité un effort majeur de coordination tout au long du processus, créateur par ailleurs de confiance réciproque. La présence, au sein d'EURO 2016 SAS, d'un membre du corps préfectoral, a constitué un facteur important à cet égard.

Enfin, pendant le tournoi, il existait une présence croisée des organisateurs et de l'État au centre interministériel de crise du ministère de l'Intérieur et au centre de gestion du tournoi des organisateurs. Localement, le pilotage coordonné depuis le PC du stade a aussi été exemplaire.

Le dispositif a-t-il été efficace ?

Face à un évènement sans précédent, à un niveau de menace particulièrement élevé et à l'équation d'un pays organisateur ouvert et exposé, le dispositif a très bien fonctionné et le résultat a été un grand succès : non seulement il a su donner confiance au public, prévenir toute difficulté majeure, répondre rapidement aux quelques incidents, mais aussi laisser s'exprimer un climat particulièrement festif.

Les stades étaient remplis, malgré le contexte, et n'ont pas connu d'intrusion frauduleuse ou par la force, ni de violence grave en leur sein ou d'expression répréhensible. Le principal incident a concerné la rencontre entre la Russie et l'Angleterre, dès le deuxième jour, mais essentiellement en centre-ville de Marseille et du fait, notamment, d'une coopération insuffisante de la Russie.

La sécurité des publics cibles, comme les équipes nationales, les personnalités ou les médias, n'a jamais été mise en cause. Les dispositifs de sécurité publique et privée étaient en place, malgré, dans ce dernier cas, quelques défaillances ponctuelles vite résorbées grâce aux efforts des organisateurs et à la mobilisation de la profession. Les menaces technologiques comme la cybercriminalité,

les drones ou le risque NRBCe ont été éludées, avec la mise en place de systèmes de surveillance et de contrôle dédiés.

La gestion des flux s'est passée dans de bonnes conditions d'ensemble, avec un équilibre entre fluidité et contrôle, notamment au périmètre extérieur des stades, nonobstant quelques situations tendues liées à une arrivée des spectateurs plus tardive que prévue.

Enfin, aucun attentat n'a eu lieu, ce qui n'est pas le fruit du hasard mais d'un travail préparatoire minutieux et exhaustif conjugué à un niveau de mobilisation très élevé.

Pour autant, des pistes d'amélioration doivent être envisagées pour l'avenir : l'usage accru de nouvelles technologies de contrôle et de communication une fois arrivées à maturité ; une meilleure traçabilité des billets par la mise en place d'un billet nominatif électronique ; une priorité plus grande accordée à la sécurité au sein des différents secteurs de l'organisation et dans les arbitrages, et ce dès les grands choix de départ ; un meilleur partage du renseignement, que ce soit avec les organisateurs ou au plan international afin de prévenir les actions de fauteurs de trouble.

? Le dispositif pourrait-il constituer un modèle ?

La dimension particulière de l'EURO, sa gouvernance originale et l'évolution rapide des technologies, rendent unique son modèle d'organisation. Cependant, celui-ci constitue désormais une référence majeure. Ses principes, à commencer par la volonté d'éviter les surenchères, comme ses grandes orientations, dont la coopération exemplaire avec l'État, représentent une bonne pratique pour les grands évènements sportifs (de football ou non) des prochaines années en France comme à l'étranger.

Ce dispositif aura en tout cas démontré, à un moment critique, le savoir-faire de la France dans l'organisation d'événements planétaires et sa capacité à en accueillir d'autres. ■

L'UEFA et la Fédération française de football (FFF) créèrent, en 2011, une entreprise commune, EURO 2016 SAS, présidée par Jacques Lambert, ancien directeur exécutif du comité d'organisation de la Coupe du Monde de la FIFA 1998. EURO 2016 SAS a été responsable de tous les aspects de l'organisation de la phase finale. Ce nouveau modèle d'organisation réunissait toutes les activités relatives à l'UEFA EURO 2016, qui auraient autrefois été divisées entre l'UEFA et le(s) comité(s) d'organisation local (locaux). Tout ce qui concernait la compétition et les droits commerciaux, tels que les droits marketing ou médias, restant sous le contrôle de l'UEFA. Un comité de pilotage s'est réuni, plusieurs fois par an, pour rassembler les parties prenantes - UEFA, FFF, gouvernement français et villes hôtes - afin d'aborder les questions stratégiques et sensibles liées à la préparation de l'événement.

JEAN-CLAUDE CATHALAN

Président - Comité Montaigne

Percevez-vous une aggravation de la menace terroriste sur votre secteur d'activité ? Les attentats représentent-ils un risque majeur dans les espaces commerciaux et d'expositions de l'avenue Montaigne qu'il convient de gérer ?

Il y a une inquiétude générale sur ce qu'il pourrait arriver. Cela explique que la plupart des entreprises aient pris les mesures concernant le risque d'attentat, à travers le renforcement de la surveillance humaine et technique. Les maisons concernées sont celles les plus exposées, relativement à leur notoriété.

Les investissements en matériels et dispositifs de sûreté, qui contribuent à maintenir la confiance des consommateurs/visiteurs, ne cessent de croître depuis les attentats du 13 novembre 2015. Ne faudrait-il pas définir un standard de sûreté en deçà duquel un modèle économique n'est plus jugé comme viable ? Par exemple, serait-il pertinent selon vous de généraliser le régime de protection des OIV aux secteurs plus particulièrement exposés à la menace ? Une transposition de l'arrêté du 11 septembre 2013, relatif aux mesures de sûreté de l'aviation civile aux autres secteurs d'activité, pourrait-elle être envisagée ?

L'investissement dans les mesures de sûreté des points de vente est difficile à chiffrer. Il est essentiellement humain (des agents de surveillances) et éventuellement matériel (caméras vidéos surveillance).

La protection de l'avenue Montaigne est placée sous la vigilance de la préfecture et plus spécifiquement du commissariat du VIII^e^ arrondissement. Comment percevez-vous la coopération entre vos membres et les services de police et de la Préfecture ?

Jusqu'à présent, les moyens techniques étaient nettement insuffisants, mais nous avons eu une nette amélioration à la fin de l'année avec l'installation de nouveaux matériels de vidéo surveillance, en concertation avec les services de la préfecture. Notre coopération est excellente mais il y a un problème d'effectif sur le terrain.

Les entreprises expriment un besoin supplémentaire d'agents que le commissariat n'est pas toujours en mesure de fournir. Malgré ce manque, nous préférons que ce soient les services régaliens qui assurent la protection. En revanche, s'il reste difficile de mobiliser en permanence les agents, on pourrait renforcer les patrouilles et s'assurer d'une capacité d'intervention immédiate en cas d'urgence.

Sans entrer dans le détail des dispositifs de protection et de surveillance (ostentatoire-discrète), quelles sont les tendances à privilégier ?

Ce dont nous avons besoin, c'est d'une surveillance vidéo à la fois efficace en cas de problème et rassurante pour la clientèle. La vidéo surveillance est à la charge de la préfecture concernant les abords extérieurs. Or, si nos membres sont autorisés à avoir un dispositif de vidéo surveillance aux abords de leurs points de vente, la réglementation de la CNIL reste beaucoup trop restrictive. Elle en restreint l'exploitation, d'abord de la couverture géographique (limitée à 1 m de la vitrine), ensuite des images, notamment concernant l'identification en cas de vol, d'attaque à main armée… Ces limitations sont aberrantes au regard des besoins de surveillance mais aussi de décryptage de la criminalité. Cela pose un vrai problème dans le suivi et l'identification des réseaux.

Les directions sûreté ont-elles la marge de manœuvre suffisante pour mettre à niveau les dispositifs de sûreté ?

Oui, au sein de l'entreprise, mais elles sont encore trop limitées par les règlementations administratives. Or, nous devons adapter les dispositifs de sûreté au comportement de la clientèle, notamment haut de gamme: il faut surveiller sans inquiéter!

Les dommages causés sur la voie publique peuvent impacter considérablement l'image d'une entreprise. Jusqu'où la manœuvre sûreté est-elle à la charge de l'entreprise? La protection périmétrique/périphérique ne nécessite-t-elle pas une présence des forces publiques quasi systématique? Les relations avec les partenaires publics (Préfectures ; Police et Gendarmerie en fonction des secteurs de compétences; services de renseignement) sont-ils renforcés?

La menace terroriste et sa médiatisation excessive a surtout entraîné une dégradation de l'image de la France. Les touristes étrangers ne viennent plus en France. Dans certains pays d'Asie, les tours Operators ont rayé la France et certaines compagnies refusent d'assurer des voyages en France. Concernant notre clientèle haut de gamme, plutôt individuelle, les compagnies refusent d'assurer. Les conséquences se mesurent en termes de baisse de fréquentation de la clientèle étrangère. Il y a un problème de terminologie: «état d'urgence», fait peur, parlons plutôt de «sécurité renforcée» qui rassure!

Les prestataires privés de sécurité sont-ils en mesure de répondre qualitativement aux besoins du secteur? Qu'en est-il du contrôle de la sous-traitance et de la fiabilité des agents? L'armement d'agents privés de sécurité est-il une solution?

Une sélection sévère est réalisée. Il y a, auprès de nos membres, une notion de service irréprochable. Certains prestataires de sécurité sont préparés à intervenir en cas d'attaques terroristes.

Le recrutement de futurs salariés ou sous-traitants requiert aujourd'hui davantage de vigilance de la part des directions sûreté et des RH. Ces derniers sont-ils sensibilisés à la question de la «radicalisation»? Est-ce dans leurs prérogatives que d'en déterminer les critères? Peuvent-elles en référer aux services de l'État? En cas de comportement d'un salarié traduisant un risque de «radicalisation» ou de basculement vers la violence, la circulation des informations (montantes/descendantes) entre les services de l'État et l'employeur est-elle en vigueur?

Nos maisons sont très attentives au sujet.

Les situations de post attentat ont montré des salariés en état de choc. Quelles sont les mesures pouvant être mises en place par les directions sûreté avec les RH pour gérer ce risque?

Oui, il y a eu des cas, mais cela reste exceptionnel.

En tant que fédération, quelle écoute avez-vous auprès des pouvoirs publics sur l'expression des besoins en sûreté?

Nous avons, aussi bien avec le commissariat qu'avec la préfecture, une excellente coopération et une très bonne écoute. Mais nous sommes heurtés à un manque de moyens de leur part. Je dois dire qu'ils sont sensibles au fait que notre avenue soit un vecteur d'image important pour la France et une source majeure de revenus touristiques qu'il convient de préserver. Le tourisme haut de gamme vient chez nous et dépense beaucoup. Cette année, les attentats ont entraîné une baisse de fréquentation sur l'avenue Montaigne entre 20 et 30%, et donc, par voie de conséquence, sur le chiffre d'affaire global des maisons de luxe et la fréquentation des hôtels. Il y a une nécessité à rétablir la réputation de la France au niveau international. La sécurité doit être un sujet de diplomatie, tant sur les questions d'attentats que sur la délinquance, les deux pouvant être liés dans un contexte de post attentat où la délinquance a d'autant plus d'échos. Disons que le sentiment d'insécurité peut alimenter la délinquance. La France est perçue comme un pays dangereux à visiter.

Quelles sont vos capacités de diffusion des bonnes pratiques auprès des directions générales de vos entreprises membres?

En tant qu'association, nous réunissons nos membres deux fois par an pour faire le point sur les mesures prises et les bonnes pratiques. Nous faisons cela en présence du Commissaire de police et de ses adjoints directs.
NOS PRÉCONNISATIONS: parler de sécurité renforcée et non d'état d'urgence, aboutir à un cadre législatif permettant une plus large exploitation de la vidéo surveillance, bénéficier de plus de présence policière. ■

COMITE MONTAIGNE

Le Comité Montaigne s'attache à faire rayonner l'image de l'Avenue Montaigne et de la rue François 1er, à Paris, en France et dans le monde entier. Présidé par Monsieur Jean-Claude Cathalan, le Comité Montaigne réunit la plupart des maisons de couture et de luxe qui sont installées Avenue Montaigne et de la rue François 1er et organise des événements qui marquent l'agenda parisien, tels que les Vendanges Montaigne, la Promenade pour un Objet d'Exception, les Catherinettes, le Christmas Montaigne, les Illuminations, et les Sapins des Créateurs.

FRANCK CHARTON

Délégué général - PERIFEM

Percevez-vous une aggravation de la menace terroriste sur votre secteur d'activité ? Les attentats représentent-ils un risque majeur dans les espaces commerciaux qu'il convient de gérer ?

Les attentats ont été vécus comme un électrochoc. Nous étions déjà en alerte et le restons depuis cette période.. Ce risque fait l'objet d'une évaluation de la part des responsables sûreté des enseignes qui bénéficient notamment d'un échange régulier avec les services de l'État. Afin de diffuser les bonnes pratiques auprès de nos adhérents, nous avons édité avec le support du SGDSN trois guides destinés à la protection des espaces commerciaux ; téléchargeables sur economie.gouv.fr : « Vigilance attentat : les bons comportements ».

L'impact se mesure-t-il en termes de fréquentation des sites commerciaux ?

La baisse de fréquentation dans notre secteur a été visible dès le lendemain de l'attentat du Bataclan, mais ne s'est pas maintenue. Les comportements ont été les mêmes après les attaques de *Charlie Hebdo* et de l'*Hyper casher* début 2015. La fréquentation actuelle des sites reste globalement fragile mais la nécessité des achats fait que les citoyens reviennent dans les magasins qui sont d'ailleurs de plus en plus des lieux de vie. Il n'y a pas de sites plus sensibles que d'autres.

Qu'en est-il des conséquences sur l'image et la réputation des entreprises du secteur, et de la France ?

Certains commerces plus directement concernés par le tourisme international voient leur chiffre d'affaires impacté par la baisse de fréquentation. Le risque serait que certaines compagnies d'assurance n'assurent plus leurs salariés en mobilité en France. Et nous savons que certains tours opérateurs ne référencent plus la France dans la liste des destinations.

L'état d'urgence n'a-t-il pas paradoxalement un effet dissuasif en matière de fréquentation ?

Il y a probablement un lien mais dans notre secteur l'amplitude de l'impact reste difficile à mesurer. Les secteurs du bricolage ou de l'alimentation sont moins touchés que d'autres, plus spécifiques, les gens continuent à se nourrir et à bricoler. Notre ministère de tutelle, au travers d'Emmanuel Macron avait perçu la gravité du sujet au plan économique. Il nous a conviés dès le lundi 16 novembre 2015 à participer à la cellule de continuité d'activité économique qui a rassemblé les services de l'État et les administrations connexes avec les secteurs d'activités. L'objectif était, sur la base des propres capacités de chacun à maintenir les activités, d'aboutir à des points d'accords sur des mesures concrètes à mettre en oeuvre :

- Suite à notre demande, le contrôle aléatoire visuel des sacs a été instauré. La forte affluence aux entrées des centres commerciaux ne permettait pas le contrôle systématique des sacs.

- Concernant des mesures généralisables aux autres secteurs, certaines concernent la présence d'agents de surveillance ou l'installation de systèmes de vidéosurveillance aux abords des lieux publics commerciaux.

Certaines demandes demeurent concernant des mesures spécifiques et techniques mais la cellule de continuité d'activité économique assurée par les services de Bercy constitue une véritable avancée dans le partenariat public/privé, essentiel

dans ce contexte. Aujourd'hui, dans nos centres, la présence des forces de l'ordre rassure la clientèle alors qu'elle était vue comme anxiogène autrefois. Nous plébiscitons au maximum la présence des forces de l'ordre. Les mentalités ont changé et l'opinion accepte un niveau de risque.

Les investissements en matériels et dispositifs de sûreté qui contribuent à maintenir la confiance des consommateurs/visiteurs ne cessent de croître depuis les attentats du 13 novembre 2015. Ne faudrait-il pas définir un standard de sûreté en deçà duquel un modèle économique n'est plus jugé comme viable ? Par exemple, serait-il pertinent de généraliser le régime de protection des OIV aux secteurs plus particulièrement exposés à la menace ? Une transposition de l'arrêté du 11 septembre 2013, relatif aux mesures de sûreté de l'aviation civile, pourrait-elle-être envisagée aux autres secteurs d'activité ?

Deux axes dimensionnent les budgets alloués à la sûreté :

- La mise en place d'un gardiennage supplémentaire depuis le Bataclan a été calibrée très précisément par les membres et apporteurs de solutions de sécurité, qui sont eux-mêmes limités en capacité. Cela représente un coût substantiel que les centres commerciaux doivent intégrer dans leur modèle économique. Par voie de conséquence, l'impact sur les locataires n'est pas non plus négligeable. Pour certains espaces, les charges ont augmenté de 10 à 30 pour-cents.

Les dispositifs ostentatoires de sûreté ont une efficacité relative. Certains aspects tels que la surveillance de la sous-traitance et des livraisons mériteraient la mise en place de mesures renforcées. Les centres commerciaux ne peuvent pas prétendre à une hermeticité totale comme l'aéroportuaire. La transposition des mesures n'est pas encore envisageable.

La formation des agents de gardiennage aux comportements sensibles améliore considérablement le niveau de vigilance.

- La circulaire du ministre de l'Intérieur d'août 2015, concernant la polyvalence (sécurité et sûreté) des agents dans les centres commerciaux, était attendue et nécessaire pour fluidifier le travail des agents. La sécurité est devenue globale et cette circulaire en atteste, elle est le fruit d'un travail commun et constant avec le Ministre de l'Intérieur.

La protection de certaines zones commerciales, telles que la Défense, les Halles, boulevard Haussmann, rue de Rivoli, Champs Elysées, etc. est placée sous la vigilance de la préfecture et plus spécifiquement des commissariats d'arrondissement. Comment percevez-vous la coopération entre vos membres et les services de police et de la Préfecture ? (Réunions – exercices sur sites – technologies innovantes).

Excellente ! De manière globale sur l'ensemble du territoire, n'importe quelle ville a un bon niveau de connaissance des acteurs chargés de la sécurité sur le terrain et des commissariats locaux. Les instances nationales et locales fonctionnent en concertation et complémentarité, elles coproduisent le niveau de sécurité. Des réunions de sûreté destinées à échanger sur les problématiques opérationnelles ont lieu tous les trois mois chez Perifem et se tiennent en présence d'un membre du cabinet du ministre de l'Intérieur.

Sans entrer dans le détail des dispositifs de protection et de surveillance (ostentatoire-discrète), quelles sont les tendances à privilégier ? (Vidéosurveillance et protection ; caméras intelligentes…)

Il y a un point qui pourrait être développé : les réseaux sociaux et l'utilisation de nos portables pour participer à la surveillance et l'information des personnes. On peut aujourd'hui comptabiliser les personnes présentes dans les espaces grâce à leurs Smartphones. Mais on pourrait aller plus loin en étant capable d'envoyer un message sur le numéro de ces mêmes personnes.

L'application SAIP (Système d'alerte et d'information des populations) va dans ce sens. Nous pourrions développer une application de ce type servant directement à la protection des personnes avec l'accord de la CNIL et en partenariat avec les autorités publiques. Cela nous permettrait de localiser les événements, les attaques, de prévenir le public mais aussi d'échanger avec lui.

Le PC du centre commercial avec la préfecture centraliserait les informations. Cela nous permettrait de systématiser les remontées et les descentes d'informations utiles à la gestion de l'événement, à la fois pour informer le public et de permettre à celui-ci d'informer les autorités pour améliorer la conduite des opérations. Il serait intéressant de rassembler les acteurs autour d'un projet de système d'alerte. Ce procédé existe pour les informations commerciales, il suffirait de l'utiliser à des fins de sécurité.

Concernant le matériel et les équipements, nos surfaces sont entièrement couvertes par les systèmes de vidéosurveillance depuis des années maintenant. La culture des clients a changé concernant les dispositifs ostentatoires. Aujourd'hui, les clients plébiscitent la présence des agents de surveillance et du matériel ce vidéosurveillance.

Les développements actuels vont vers une vidéo intelligente, avec une meilleure précision des captures. Nous aurions aujourd'hui techniquement la capacité de faire de la reconnaissance faciale. La CNIL impose encore des

limites à ce sujet que nous aurions tout intérêt à rediscuter pour voir comment exploiter ces évolutions technologiques dans le respect des règles que la communauté se sera données. Il y a des installations qui ne sont pas transposables dans les centres commerciaux comme les espaces de confinement et l'utilisation des portiques qui restent incompatibles avec des flux aussi importants. Par contre, en compensation, nous pourrions transposer des méthodes telles que l'identification d'intentions malveillantes et de comportements suspects au milieu de la foule.

Les directions sûreté ont-elles la marge de manoeuvre suffisante pour mettre à niveau les dispositifs de sûreté ?

L'équation sécuritaire des centres commerciaux depuis les événements récents fait que la prise de conscience est présente chez les dirigeants. La question budgétaire est moins évidente. L'étude que nous avons conduite avec l'INHESJ sur « La sécurité des espaces commerciaux; éléments de problématiques et d'actions en profondeur » permet de promouvoir les besoins des centres commerciaux en la matière.

Par ailleurs, la convention « Sécurité dans les commerces » tripartite entre le procureur, la direction des centres commerciaux et les autorités publiques a servi de fondement à de nombreux autres travaux.

Les dommages causés sur la voie publique peuvent impacter considérablement l'image d'une entreprise. Jusqu'où la manoeuvre sûreté est à la charge de l'entreprise ? La protection périmétrique/périphérique ne nécessite-t-elle pas une présence des forces publiques quasi systématique ? Les relations avec les partenaires publics (Préfecture ; police et gendarmerie en fonction des secteurs de compétences ; services de renseignement) sont-ils renforcés ?

Les agents de sécurité privés n'ont pas accès à la voie publique. Nous avons demandé à ce que notre sécurité puisse accéder aux abords. Pour le moment, il n'y a pas de calage réglementaire. Il reste une réflexion à conduire. On ne peut exiger une présence des forces de l'ordre en patrouille permanente, ce n'est pas compatible avec l'état budgétaire de la France, il y a une mutualisation des capacités à envisager.

Lors des Assises de la Sécurité privée du 5 décembre le Ministre de l'Intérieur a d'ailleurs indiqué qu'ils souhaitait porter ce sujet devant la représentation Nationale pour un débat public puisqu'il concerne tous nos citoyens.

Les prestataires privés de sécurité sont-ils en mesure de répondre qualitativement aux besoins du secteur ? Qu'en est-il du contrôle de la sous-traitance et de la fiabilité des agents ? L'armement d'agents privés de sécurité est-il une solution ?

Les terroristes ne discutent pas, nous devons nous donner les moyens de les arrêter dans leur action. Soit les forces publiques sont en capacité d'intervenir dans l'immédiat, soit pourquoi ne pas armer les agents ! Certains membres de notre secteur s'interrogent sur la nécessité d'armer des agents.

Le sujet n'est pas mâture mais demande à être considéré de près. Il y a des discussions avec le CNAPS à ce sujet concernant différents secteurs.

Le recrutement de futurs salariés ou sous-traitants requiert aujourd'hui davantage de vigilance de la part des directions sûreté et des RH. Ces derniers sont-ils sensibilisés à la question de la « radicalisation » ? Est-ce dans leurs prérogatives que d'en déterminer les critères ? Peuvent-elles en référer aux services de l'état ? En cas de comportement d'un salarié traduisant un risque de « radicalisation » ou de basculement vers la violence, la circulation des informations (montantes/descendantes) entre les services de l'état et l'employeur est-elle en vigueur ?

Le Service central du renseignement territorial (SCRT) a assuré une conférence de sensibilisation le 6 décembre 2016, lors de notre dernière réunion sûreté. De façon générale, la radicalisation est un sujet de préoccupation pour les directions impliquées.

Les situations de post attentat ont montré des salariés en état de choc. Quelles sont les mesures pouvant être mises en place par les directions sûreté avec les RH pour gérer ce risque ?

Les enseignes ont mis en place depuis des années des cellules psychologiques prêtes à répondre. Nous avons eu à faire face à des attaques à main armée, des braquages… Notre secteur est déjà sensibilisé depuis des années à cela.

En tant que fédération, quelle écoute avez-vous auprès des pouvoirs publics sur l'expression des besoins en sûreté ?

Nous avons de très bonnes relations avec eux, en témoigne la présence systématique d'un membre du cabinet dans nos réunions sûreté et la convention de partenariat signée avec le ministère de l'Intérieur. Et nous avons une relation privilégiée avec le ministère de l'Économie.

Quelles sont vos capacités de diffusion des bonnes pratiques auprès des directions générales de vos entreprises membres ?

C'est le rôle de Perifem. L'existence de notre association est financée par les distributeurs et leurs apporteurs de solutions.

Nous avons aussi un contact privilégié avec le Haut fonctionnaire de Défense de Bercy sur les pos-

tures *Vigipirate*. Aussi, notre réseau, très proche du terrain, nous offre une forte capacité de diffusion. Pour exemple, les guides que nous réalisons sont diffusés auprès de tous les directeurs sécurité et sûreté du secteur. Il y a une bonne circulation de l'information en interne dans les organisations qui s'est encore améliorée dans ce contexte. ■

Perifem a été créée en 1980 afin d'améliorer la construction et l'exploitation des surfaces commerciales avec 3 expertises (Energie-Environnement ; Technologie ; Sécurité). Interlocuteur reconnu des pouvoirs publics et des leaders d'opinion depuis plus de 30 ans, la mission de Perifem est de représenter les enseignes de la grande distribution, du commerce spécialisé et des centres commerciaux ; de connecter ces enseignes avec les fournisseurs de solutions, les institutionnels et les parties prenantes ; de contribuer au partage d'informations, au déchiffrage d'innovations et à l'élaboration des règlementations.

POUR ALLER PLUS LOIN

GUIDE PRATIQUE POUR LES ÉQUIPES DE DIRECTION DES CENTRES COMMERCIAUX :

http://www.economie.gouv.fr/files/files/directions_services/hfds/OKSGDSN-BROCH-DIR-CENTRES_HD.pdf

GUIDE PRATIQUE POUR LES ÉQUIPES DE DIRECTION DES ESPACES COMMERCIAUX (GRANDS MAGASINS, HYPERMARCHÉS, MAGASINS DES CENTRES COMMERCIAUX) :

http://www.economie.gouv.fr/files/files/directions_services/hfds/OKSGDSN-BROCH-DIRECTIONS_Espaces_HD.pdf

GUIDE PRATIQUE POUR LE PERSONNEL DES ESPACES COMMERCIAUX :

http://www.economie.gouv.fr/files/files/directions_services/hfds/OKSGDSN-BROCH-PERSONNEL_HD.pdf

ETUDE MENÉE PAR L'INHESJ SUR *« LA SÉCURITÉ DES ESPACES COMMERCIAUX : ELÉMENTS DE PROBLÉMATIQUE ET D'ACTION EN PROFONDEUR »*

SOPHIE HUBERSON

Déléguée générale - SNELAC

Percevez-vous une aggravation de la menace terroriste sur votre secteur d'activité ? Les attentats représentent-ils un risque majeur dans les espaces commerciaux qu'il convient de gérer ?

La multiplication des attentats sur le sol français, tant sur l'espace public (la promenade des Anglais à Nice) que sur l'espace privé (le Bataclan à Paris) a fait prendre conscience aux Français que la menace était aveugle et que les terroristes pouvaient frapper partout et n'importe quand.

La résonance donnée aux attentats fait courir deux autres menaces, un risque d'image et un risque économique à tel ou tel pan de l'activité touristique en stigmatisant un secteur plutôt qu'un autre, ce qui a pour conséquence de semer le doute dans l'esprit des Français et *in fine* de faire le jeu des terroristes.

Les investissements en matériels et dispositifs de sûreté qui contribuent à maintenir la confiance des visiteurs ne cessent de croître depuis les attentats du 13 novembre 2015. Ne faudrait-il pas un standard de sûreté en deçà duquel un modèle économique n'est plus jugé comme viable ? Par exemple, serait-il pertinent selon de vous de généraliser le régime de protection des OIV aux secteurs plus particulièrement exposés à la menace ? Une transposition de l'arrêté du 11 septembre 2013 relatif aux mesures de sûreté de l'aviation civile pourrait-elle être envisagée aux autres secteurs d'activité ?

Le SNELAC, syndicat national des espaces de loisirs, d'attractions et culturels rassemble un réseau de 500 entreprises qui ont accueilli 52 millions de visiteurs et réalisé 2,2 milliards d'euros de chiffre d'affaires en 2015.

Les exploitants des parcs d'attractions, aquatiques ou animaliers, musées privés et châteaux ont une priorité commune : la sécurité de leurs visiteurs et de leurs collaborateurs afin de faire vivre une expérience unique de divertissement en les détournant de leur quotidien.

L'investissement humain et financier nécessaire s'élève déjà à plusieurs dizaines de millions d'euros dans notre secteur. C'est la contribution nécessaire pour que les sites de loisirs et culturels demeurent le loisir le plus sûr hors de chez soi.

A l'instar de tous les établissements recevant du public, les grands sites de loisirs et de culture présentent aujourd'hui en France un élément caractéristique pour des mouvances terroristes qui peuvent être amenées à les prendre pour cible à cause du cumul d'un symbole fort, d'une forte résonance médiatique liée à la fréquentation élevée et permanente sur un même site et d'une relative facilité d'accès du fait du nombre de personnes accueillies et travaillant dans un univers voué au divertissement.

La sécurité est bien l'affaire de tous, et tout un chacun doit hausser son niveau de vigilance et, pour les entreprises, il s'agit de se préparer à la gestion d'une crise terroriste.

Sans entrer dans le détail des dispositifs de protection et de surveillance (ostentatoire-discrète), quelles sont les tendances à privilégier ? Les directions sûreté ont-elles la marge de manœuvre suffisante pour mettre à niveau les dispositifs de sûreté ?

Les leçons tirées des pratiques actuelles dans le domaine de la sécurité des sites de loisirs et culturels démontrent qu'une importance toute particulière doit être accordée à trois modes de sécurisation :

- le maintien d'une présence humaine dans et autour des espaces de loisirs, qu'il convient de mieux encadrer,
- une meilleure collaboration aux frontières de ces sites entre les institutions et les exploitants et l'organisation d'un domaine de compétence en périphérie des sites,
- le développement de la supervision, dans et autour des sites comme support de la collaboration renforcée entre les services de sécurité intérieure et les exploitants.

Ces trois éléments apportent un gain d'efficience tant au plan de la prévention qu'à celui de l'enquête judiciaire et de l'identification des coupables.

Ces éléments de spécificité du secteur des sites de loisirs et culturels déterminent le contenu des exigences de sécurité préventive.

Celles-ci peuvent être regroupées sous l'égide de la triple préoccupation de :
- la planification et de l'organisation,
- la sensibilisation et de la formation,
- la capacité de réaction et de l'entraînement.

Avant tout, l'analyse de risque et la définition de la politique générale de sécurité de l'opérateur permettent d'élaborer le plan de sécurité du site. L'exercice permet à l'opérateur de mettre en confrontation les vulnérabilités de ses installations et de définir une réponse adaptée.

Puis nous incitons les exploitants à identifier et à justifier l'identification de leurs points d'importance vitale.

Enfin, nous recommandons la désignation des correspondants zonaux et délégués de site et la mise en place de la chaîne d'alerte et de sécurité. La chaîne de sûreté est ici entendue comme, d'une part, l'ensemble des moyens tant humains que matériels et, d'autre part, les modes d'organisation et procédures visant à garantir la bonne application des prescriptions de sécurité tant au plan de la prévention qu'au stade de la gestion de crise avec l'objectif permanent de maintenir la vulnérabilité à son niveau minimal, d'assurer la sécurité des personnes ainsi que la continuité des activités.

Le premier objectif est de décourager les auteurs potentiels par l'augmentation du risque d'échec de la tentative d'attentat, augmentation générée par l'élévation du niveau de sécurité. La destruction d'un lieu de visite emblématique est différente dans sa nature et ses conséquences d'une attaque dans une attraction au milieu d'une foule. Les deux appellent donc des réactions sensiblement différentes des services d'alerte et de gestion de crise.

Le deuxième objectif est d'élaborer des scénarii concrets afin d'évaluer des conséquences diverses d'une frappe terroriste et un plan de continuité d'activité.

Le troisième objectif est de définir les exigences de sécurité à faire partager aux différents collaborateurs.

Cela passe par la description des différentes mesures de protection et de renforcement du dispositif de sécurité (active et passive) envisagées, leurs coûts (au regard des effets attendus), le calendrier de leur mise en œuvre ... (mise en place ou renforcement des contrôles d'accès, renforcement des clôtures, rondes télésurveillance, vidéosurveillance, PC de Sûreté, etc.).

Le plan de l'opérateur contient également tous les éléments d'une gestion de crise, c'est-à-dire l'ensemble des mesures, différenciées en fonction de la nature de l'attaque et de l'ampleur des conséquences, susceptibles d'être mises en œuvre au cas de survenance de l'attentat.

Il s'agit des mécanismes de détermination de la nature de l'attaque : différentes hypothèses doivent être envisagées avec description précise des symptômes ou caractéristiques résultant de l'utilisation de tel ou tel moyen d'attaque et l'identification des compétences ou services spécialisés à mobiliser ou à alerter. Les fiches réflexes, l'articulation des différents plans de sécurité sont testés lors d'exercices. Ils sont destinés à tester le maintien de la fiabilité : - des conclusions de l'analyse de risques, - de ses vulnérabilités, - de la pertinence et de l'efficacité de ses procédures (audit), - de la réactivité des agents de sécurité, - de la prise en considération par l'ensemble des collaborateurs de l'impératif de sécurité.

Sous l'impulsion du service de sécurité, l'ensemble du personnel est associé aux exercices, notamment en ce qui concerne les procédures d'évacuation et la répétition des gestes de base en matière de sécurité.

? Quelles sont les mesures exceptionnelles qui pourraient assurer la continuité des activités dans un contexte d'état d'urgence ? Les pouvoirs publics peuvent-ils en faciliter la mise en œuvre ? En tant que fédération, quelle écoute avez-vous auprès des pouvoirs publics sur l'expression des besoins en sûreté ?

Le *Snelac* travaille depuis 2009 à l'élaboration d'un plan qui vise à associer et à responsabiliser les opérateurs - publics et privés- à la gestion de ce risque et à déterminer les mesures générales d'organisation de la prévention.

La mise en place par le ministre de l'Économie de la Cellule de Continuité d'Activité Economique à la suite des attentats du 13 novembre 2015 a permis au *Snelac* de sensibiliser l'État et de présenter les objectifs et les politiques de sécurité du secteur touristique et culturel, particulièrement concerné par des rassemblements massifs de population dans des espaces récurrents pouvant constituer des cibles faciles et d'ampleur médiatique et économique.

? Les dommages causés sur la voie publique peuvent impacter considérablement l'image d'une entreprise. Jusqu'où la manœuvre sûreté est à la charge de l'entreprise? La protection périmétrique/périphérique ne nécessite-t-elle pas une présence des forces publiques quasi systématique? Les relations avec les partenaires publics sont-ils renforcés?

L'exploitant élabore un plan de communication et de sensibilisation. Ce plan comporte les éléments relatifs au comportement des populations et à leur participation, pour ce qui les concerne, à la gestion de la crise.

Ces éléments contribuent à la bonne articulation avec le plan de protection externe élaboré par les services préfectoraux. Ce plan de protection externe représente l'engagement des parties prenantes, État et exploitant dans la sécurisation du site.

? Le recrutement de futurs salariés ou sous-traitants requiert aujourd'hui davantage de vigilance de la part des directions sûreté et des RH. Ces dernières sont-elles sensibilisées à la question de la « radicalisation » ? Est-ce dans leurs prérogatives que d'en déterminer les critères ? Peuvent-elles en référer aux services de l'État ? En cas de comportement d'un salarié traduisant un risque de « radicalisation » ou de basculement vers la violence, la circulation des informations (montantes/ descendantes) entre les services de l'État et l'employeur est-elle en vigueur ?

La formation et la sensibilisation constituent un élément clef de la crédibilité globale du plan de l'exploitant, surtout dans la mesure où la qualité des personnels et leur implication dans la sécurisation du site sont in fine les seuls garants du divertissement des visiteurs.

Le plan de formation détermine des actions visant les collaborateurs du site. Son contenu vise à :
- faire prendre conscience de la réalité du risque ;
- faire partager les objectifs de sécurité ;
- favoriser l'appropriation individuelle du plan de sécurité par les agents ainsi que leur aptitude au respect des postures graduées.

S'agissant des agents plus spécifiquement en charge de la sécurité, le plan de formation délivre les éléments visant à la mise à niveau de leur capacité à analyser la nature d'une attaque et ses conséquences, leur aptitude au déclenchement et à la gestion des différentes composantes du plan de gestion de crise, la mise en œuvre, en contact avec les responsables concernés, des solutions alternatives de maintien partiel ou total de l'activité.

Il contient également des éléments visant les intervenants extérieurs : brochures d'information, clauses contractuelles de bonne connaissance des éléments du plan de sécurité applicables à tel ou tel intervenant.

Il doit être intégré dès la démarche de recrutement, notamment au travers de deux mesures phares :

1- Un meilleur contrôle des personnels à l'embauche de façon à ne pas intégrer dans les dispositifs de sécurisation de ces sites des éléments à risques. Ce contrôle relève des services de sécurité intérieure et le *Snelac* travaille à l'élaboration d'une passerelle systématique entre une personne dûment habilitée dans l'entreprise et les services de renseignement intérieur.
2- Un parcours de formation à l'embauche qui responsabilise les personnels nouvellement emb auchés autour des problématiques de sûreté et contribue à leur donner des réflexes de sécurité et de sûreté dès le départ de leur collaboration.

Une procédure raccourcie de ces deux mesures clefs devrait, par ailleurs, être définie pour les personnels occasionnels ou saisonniers qui constituent un effectif important du personnel des sites de loisirs et culturels. ■

Le SNELAC est un syndicat professionnel et patronal ouvert à tous les sites de loisirs recevant un public familial dans un espace clos et aménagé. Parcs d'attractions, parcs aquatiques ou animaliers, parcs à thème ou à vocation scientifique, sites culturels et sites naturels ont ainsi adhéré au SNELAC afin de promouvoir leurs activités.

LA PROTECTION DES DONNÉES PERSONNELLES, UN ATOUT POUR LES ENTREPRISES

Edouard GEFFRAY
Secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL)

Alors que se sont égrénées, au fil des derniers mois, de spectaculaires failles de sécurité, ces attaques, qui portent parfois sur des dizaines de millions de comptes clients, montrent que la protection des données personnelles est aujourd'hui, non seulement une obligation légale, mais un enjeu stratégique pour les entreprises. Enjeu stratégique pour les droits des personnes concernées; enjeu stratégique pour le capital informationnel potentiellement « pillé »; enjeu stratégique en termes d'image de marque. Dans le même temps, ces mêmes entreprises sont parfois tentées de rechercher des informations sur leurs salariés, ou d'accroître leur surveillance, collectant ainsi des données potentiellement excessives. Or, le cadre juridique s'appliquant au traitement de données par les entreprises est le même, même si les déclinaisons sont différentes selon la nature et la finalité des traitements. Quelle que soit l'hypothèse, la protection des données est devenue un enjeu majeur, encore renforcé par l'entrée en vigueur du règlement européen, adopté en avril 2016 et qui sera applicable à compter du 25 mai 2018. C'est cette transition numérique et juridique qu'accompagne la CNIL.

Un cadre général en évolution

Rappelons tout d'abord, à titre liminaire, que le paysage normatif en matière de protection des données évolue substantiellement. La loi « informatique et libertés » sera en effet remplacée pour l'essentiel par un règlement européen à compter du 25 mai 2016. Celui-ci reste fidèle aux principes fondateurs de la protection des données: obligation de traiter des données à des fins explicites et légitimes, proportionnalité des données traitées, durée de conservation. Il reprend également l'obligation d'assurer la sécurité des données. En revanche, il renforce la responsabilisation des entreprises et de leurs sous-traitants, en supprimant les déclarations auprès de la CNIL et autorisations préalables, et en promouvant une approche de mise en conformité dynamique, accompagnée par le régulateur qu'est la CNIL. Le règlement renforce aussi, de ce fait, les sanctions en la matière, puisqu'elles pourront atteindre 4% du chiffre d'affaires mondial. C'est donc à l'aune de ce nouveau cadre que devront être examinées à l'avenir les questions posées par le traitement de données en entreprise.

La collecte des données sur les salariés, une pratique encadrée

Les moyens potentiels pour surveiller les salariés sont nombreux, et les moyens techniques repoussent parfois les frontières de l'imagination. À titre d'exemple, la CNIL a ainsi pu recevoir des plaintes sur l'installation par des employeurs indélicats de « *keyloggers* », des logiciels qui enregistrent toute la frappe clavier avec ou sans copie d'écran, sur les ordinateurs de leurs salariés. Pratique interdite et répréhensible pénalement…

Quelques règles simples peuvent donc utilement être rappelées. Si l'on devait résumer les choses de manière un peu caricaturale, on pourrait dire que l'entreprise a le

droit d'utiliser certains dispositifs pour assurer la sécurité de ses biens et des personnes, mais qu'elle n'est pas, en revanche, un auxiliaire des forces de sécurité dans la détection d'infractions qui ne relèvent pas de son propre fonctionnement.

L'article 9 de la loi du 6 janvier 1978, dite « informatique et libertés », limite en effet les cas dans lesquels une entreprise privée peut traiter des données relatives aux infractions. Elle ne peut en effet le faire que dans la perspective ou l'exercice d'un contentieux la concernant. Le Conseil d'État a ainsi confirmé récemment une décision par laquelle la CNIL avait refusé d'autoriser une société à surveiller systématiquement et automatiquement les ordinateurs de ses salariés pour détecter d'éventuels contenus pédopornographiques et pouvoir ensuite prendre des mesures contre les auteurs de ces infractions. Il ne fait aucun doute que la société entendait ainsi lutter contre une forme de criminalité particulièrement grave, mais ce faisant, elle traitait des données qui n'avaient pas de lien avec son activité précontentieuse, et n'était donc pas autorisée à le faire par la loi.

L'autre limite posée aux entreprises est bien sûr la vie privée des salariés. Le principal champ dans lequel la CNIL est saisie de plaintes relatives à d'éventuelles atteintes à la vie privée est celui de la vidéosurveillance. En général, ces dispositifs sont autorisés pour la sécurité des biens et des personnes, à condition, d'une part, que la collecte soit loyale et licite (d'où l'importance de mentions d'informations telles que des panonceaux, et l'information des IRP et du personnel) et, d'autre part, qu'elle n'est pas pour effet, sauf circonstances exceptionnelles, de placer le salarié sous surveillance permanente et constante. La durée de conservation des données est également limitée, généralement à 30 jours, à l'instar de ce qui existe en matière de vidéoprotection (les dispositifs situés sur la voie publique ou dans les lieux ouverts au public). Cette durée laisse ainsi la possibilité à l'entreprise, en cas de précontentieux ou de plainte, de remettre à la justice tout ou partie des enregistrements.

La même question a pu être posée au sujet de salariés susceptibles de constituer une menace pour l'entreprise. En la matière, on rappellera que les professions « à risque », souvent estimées à plus d'un million d'emplois en France, sont soumises à une enquête administrative préalable (ex: les personnels de sécurité, les personnels des plates-formes aéroportuaires). En revanche, une entreprise a l'interdiction de se voir communiquer, par exemple, des éléments issus des fichiers de police au stade du recrutement d'un candidat comme ultérieurement. Elle peut évidemment signaler des comportements suspects, mais la recherche, la prévention et la répression d'infractions relèvent des seules forces de sécurité.

Enfin, on rappellera que la vie privée ne peut pas, à l'inverse, être actionnée par un salarié indélicat comme une barrière absolument étanche au travail. Ainsi, par exemple, la jurisprudence a été amenée à préciser les conditions dans lesquelles l'employeur peut accéder aux e-mails de ses employés, y compris, en leur présence et sur la base de soupçons précis, à des e-mails intitulés « privés ».

Mais le traitement des données des salariés n'est qu'une petite partie des traitements effectués par les entreprises. De manière plus générale, l'entreprise est en effet soumise aux mêmes risques et aux mêmes menaces sur l'ensemble de son patrimoine informationnel, ce qui justifie une vigilance renforcée, notamment de la part de la CNIL.

La sécurité des données, une exigence fondamentale

La cybersécurité est devenue, en quelques années, un enjeu majeur pour les sociétés à l'ère numérique. Enjeu d'image et de protection de la vie privée, alors que les individus stockent de plus en plus de données personnelles sous forme dématérialisée; enjeu économique, dans un univers où le capital informationnel est un actif financier.

La CNIL joue désormais un rôle clé en la matière: en tant que régulateur de la protection des données personnelles, elle exerce en effet une mission de contrôle qui intègre la dimension « sécurité informatique », et dispose d'une expertise de haut niveau dans ces domaines. À titre d'illustration, plus de 80% de ses contrôles se soldent par des conseils, recommandations, mises en demeure ou sanctions relatifs à des questions de sécurité informatique. Or, la cybersécurité est une chaîne: à partir du moment où la plupart des internautes utilisent les mêmes mots de passe pour plusieurs services, il suffit qu'un seul d'entre eux soit piraté pour mettre en danger l'ensemble de la chaîne. En étant dotée de pouvoirs de contrôle et de sanctions sur l'ensemble des entités qui traitent des données personnelles, la CNIL contribue donc fortement à la diffusion d'une culture commune de la cybersécurité, profitable à la fois aux personnes et aux entreprises.

La question de la protection des données n'est bien sûr pas épuisée par celles du traitement des données relatives aux salariés ou de la cybersécurité. Les transferts internationaux de données, et leurs risques en termes d'intelligence économique, les questions de territorialité des droits applicables, ou encore les alertes professionnelles, sont autant de champs dans lesquels, sur la base de la législation existante, la CNIL développe une régulation soucieuse de l'équilibre entre les droits fondamentaux, l'innovation et la sécurité collective.. ■

PROTECTION DES DONNÉES DES SALARIÉS

Alexandre LINDEN
Personnalité qualifiée désignée par la CNIL

Certaines entreprises sont concernées par la propagande terroriste sur l'Internet :
- les fournisseurs d'accès à l'Internet (FAI), bénéficiant d'une irresponsabilité de principe du fait du contenu;
- les hébergeurs, non responsables, par principe, des contenus mis en ligne;
- les éditeurs de service, responsables des contenus mis en ligne.

En vertu de l'article 12 de la loi du 13 novembre 2014, les hébergeurs et les FAI concourent à la lutte contre la provocation à la commission d'actes de terrorisme et leur apologie. Il a été instauré un dispositif de blocage administratif de sites Internet.

Les textes permettent à l'autorité administrative (l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication - OCLCTIC):
- de demander aux éditeurs et hébergeurs de retirer les contenus qu'elle estime constituer une provocation à des actes de terrorisme ou une apologie de tels actes;
- en l'absence de retrait de ces contenus dans un délai de vingt-quatre heures ou directement, sans demande préalable de retrait auprès des éditeurs, lorsque ces derniers n'ont pas mis à disposition du public les informations permettant de les contacter, de notifier aux FAI la liste des adresses électroniques des services de communication au public diffusant ces contenus, qui doivent alors «empêcher sans délai l'accès à ces adresses»;
- de notifier cette même liste aux moteurs de recherche ou aux annuaires, lesquels prennent «toute mesure utile destinée à faire cesser le référencement du service de communication au public en ligne».

Une personnalité qualifiée, désignée en son sein par la Commission nationale de l'informatique et des libertés, a pour mission de contrôler le bien-fondé des demandes de retrait, de blocage et de déréférencement. En cas d'irrégularité, cette personnalité peut recommander à l'autorité administrative d'y mettre fin et, à défaut de suivi de cette recommandation, saisir la juridiction administrative.

Au cours de la première année de contrôle, une seule recommandation a été faite, concernant une photographie de personnes décédées gisant au sol, prise à l'intérieur du Bataclan après l'attentat du 13 novembre 2015, publiée sur des réseaux sociaux, des blogs et par un organe de presse.

L'OCLCTIC a voulu faire retirer cette photographie, massivement diffusée, en considérant qu'elle constituait une atteinte à la dignité humaine, ainsi qu'une provocation à des actes de terrorisme ou l'apologie de tels actes.

Or, la possibilité de demander le retrait ou le blocage d'un contenu diffusé au public en ligne suppose que ce contenu soit en tant que tel constitutif du délit de provocation à des actes de terrorisme ou d'apologie de tels actes.

En conséquence, seul le contexte de diffusion de cette photographie était de nature à caractériser ces infractions. Il a été estimé que tel n'était pas le cas pour 96 des URL dont le retrait était demandé par l'Office, la photographie en cause faisant l'objet soit d'un traitement neutre, soit d'une dénonciation explicite des actes de terrorisme commis.

Cette recommandation a été suivie par l'OCLCTIC, qui a renoncé à prendre des mesures administratives et demandé aux éditeurs de moteurs de recherche de référencer à nouveau les adresses ayant fait l'objet d'une mesure de déréférencement. ■

SÉCURITÉ PUBLIQUE ET PROTECTION DES DONNÉES

Béatrice ŒUVRARD
Juriste Senior chez Microsoft France, responsable des affaires BtoC

Cloud Computing, Big Data, Machine learning… **Ces nouvelles générations d'innovations technologiques transforment nos modes de vie et reflètent le début de cette nouvelle ère passionnante qui s'offre à nous. Certains l'appellent déjà la Quatrième Révolution Industrielle !**

Nous observons des avancées rapides dans les domaines de l'intelligence artificielle, de la robotique, de l'impression 3D, et bien d'autres encore. De toute évidence, ces nouvelles technologies sont aussi un vrai challenge juridique pour une société comme *Microsoft* et pour les autorités en charge de la sécurité publique. Nous sommes confrontés à de nouvelles questions dès lors que la technologie progresse mais, aujourd'hui, concentrons-nous sur une problématique qui nous est chère: comment respecter le strict équilibre entre préserver les relations avec les autorités en vue de la sécurité publique et protéger les données de nos clients?

Ceci soulève des questions fondamentales sur les arbitrages à effectuer entre intérêts antagonistes tels que la sécurité publique et le respect de la vie privée.

Pour autant, l'avènement du *Cloud Computing* constitue une opportunité pour nos clients, nous en sommes persuadés. Il est essentiel de leur fournir suffisamment de garanties, un *Cloud* fiable, responsable et inclusif, pour ne pas entraver ce développement.

Le meilleur moyen d'instaurer cette confiance est de mettre en place un cadre légal qui affirme la nécessité d'assurer la sécurité tout en tenant compte de l'importance capitale que revêt la protection de la vie privée. Ce juste équilibre relève de la règle de droit.

Cette confiance doit également être trouvée entre acteurs privés et publics. Nous savons qu'elle peut être entachée lorsque les gouvernements agissent en dehors du cadre légal afin de collecter des informations personnelles au nom de la sécurité nationale. Lorsque la vie privée est mise à mal par une surveillance intrusive ou par une collecte non contrôlée d'informations personnelles, il est certain que ce type de dispositif menace la sécurité publique et ne la sert pas. L'affaire révélée par Edward SNOWDEN en est la propre illustration.

Aussi sombre soit elle, l'année 2015 a eu la vertu de forcer la communication entre autorités officielles et entreprises. Dès janvier 2015, à l'initiative du Ministre de l'Intérieur, Monsieur Bernard CAZENEUVE, et du Préfet en charge des Cybermenaces, Monsieur Jean-Yves LATOURNERIE, un groupe de contact permanent [aujourd'hui repris par Monsieur Thierry DELVILLE – Délégué aux industries de sécurité] a été créé pour dialoguer, échanger, confronter les points de vue entre entreprises de nouvelles technologies et autorités judiciaires et administratives.

Ce travail, essentiel à la compréhension de chacune des parties en présence, permet également le rappel du cadre législatif et réglementaire applicable. Nous sommes convaincus que cette confiance sera acquise par la mise en œuvre d'une harmonisation des textes tant au niveau européen qu'au niveau international.

Après de bons et loyaux services pendant presque 40 ans, notre très chère loi de 1978 «informatique et libertés» vit ses derniers mois, puisqu'elle sera remplacée, dès mai 2018, au profit du règlement européen en matière de protection des données personnelles. Nous ne pouvons que nous féliciter d'une telle harmonisation.
En matière de respect de la vie privée, il est essentiel de pouvoir donner un véritable contrôle aux usagers, qu'ils puissent disposer d'une capacité de décision raisonnable s'agissant de la façon dont leurs données sont collectées et utilisées.

En tant qu'acteur privé, nous sommes trop souvent confrontés à des gouvernements qui prennent de plus en plus de mesures unilatérales en vue de saisir des informations conservées en dehors de leurs frontières. Cela peut créer une certaine insécurité juridique et occasionner des conflits de lois obligeant les entreprises privées à ignorer sciemment une loi nationale pour se conformer à celle d'un autre État.

Pour exemple récent, le 14 juillet dernier, la Cour d'appel du Second Circuit de New York («*New York Warrant Case*») a donné raison à *Microsoft* dans un contentieux qui l'opposait au Gouvernement américain. En l'espèce, le FBI avait mis en demeure *Microsoft* de fournir des données de contenus d'un utilisateur hébergées en Irlande. *Microsoft* avait contesté l'accès à cette demande au motif que cette requête ne respectait pas les principes de coopération judicaire internationale («*Mutual Legal Assistance Treaty* – MLAT») et devait, en l'espèce, être validée par le juge local irlandais.

Le respect de la procédure doit être d'autant plus strict au regard de la typologie des informations stockées. Globalement, nous pouvons identifier trois typologies de données: (1) données de contenu type e-mails, fichiers électroniques, (2) les données hors contenus qui incluent les données de connexion, adresse IP par exemple et (3) les données relatives aux informations d'abonnement, comprenant notamment ce qui est rempli à titre déclaratif par les usagers lors de leur inscription pour ouvrir un compte ou une messagerie par exemple.

On comprend aisément que les informations relatives au contenu sont les données les plus sensibles, car elles constituent la substance même de l'échange de l'individu. Il nous semble, en conséquence, nécessaire d'appliquer des règles de procédure plus strictes comprenant un renforcement du contrôle judiciaire lorsqu'une autorité cherche à accéder à ce type de contenu.

Si nous reprenons le cas décrit ci-dessus du New York *Warrant Case*, on comprend qu'un mandat américain portant sur une donnée de contenu hébergée en Europe sans respect des règles procédurales internationales ne peut être accepté. *A contrario*, ceci reviendrait à lui donner une portée extraterritoriale.

Les entreprises et les individus s'attendent légitimement à ce que les informations qu'ils créent et stockent au format numérique bénéficient des mêmes mesures de protection de la vie privée que les informations qu'ils confient en version papier.

Toutefois, afin de lutter efficacement contre le terrorisme auquel nous sommes confrontés, nous comprenons que les États aient un besoin manifeste d'accéder aux données numériques.

Lorsque des situations d'urgence s'imposent à nous, notamment lorsqu'il y a une atteinte imminente à la vie d'autrui, il est important, voire vital, de pouvoir déroger aux procédures de droit commun. Ainsi, lors des attaques sanglantes au Bataclan le 13 Novembre 2016, *Microsoft* a mis en place des exceptions au traitement des données, ceci en toute transparence.

Lorsque les forces de l'ordre doivent faire face à l'exceptionnel, il est important que les entreprises privées aient la latitude d'adapter leurs procédures en fonction de situations exceptionnelles. Toutefois, la transparence doit être la garante de ces dérogations. Ainsi nous publions, chaque semestre, un rapport annuel de transparence permettant au public de comprendre la manière dont les États exercent leur pouvoir d'investigation.

Nous considérons que les innovations actuelles doivent être accompagnées par des lois modernes en mesure de fournir aux autorités compétentes et forces de l'ordre nationales des mécanismes d'accès aux informations numériques garantissant un traitement conforme à la loi, protégeant les droits fondamentaux des citoyens et respectant la souveraineté des nations. Toutefois, nous souhaiterions une meilleure harmonisation et rationalisation des accords internationaux, afin de faciliter le traitement des requêtes et éviter parfois de graves répercussions sur les investigations en cours.

Pour *Microsoft*, construire un *Cloud* universel passe par la mise en place d'un cadre juridique qui respecte certains droits et valeurs intemporels et assure la sécurité publique. Ce cadre doit être élaboré par les États et soumis à la règle de droit. Même si les approches internationales ou européennes sont importantes, le régime législatif de chaque pays sera différent, car il est bien naturel que les législateurs tiennent compte de leur culture locale et nationale, des usages, des normes, des réalités politiques et économiques du moment.

Toutefois, une harmonisation du cadre législatif et réglementaire est nécessaire et vitale. Pour faciliter ce dialogue, nous avons édicté une feuille de route pour un *Cloud* fiable, responsable et inclusif: «*A Cloud For Global Good*». Avec des experts juridiques, des organisations professionnelles, les leaders de notre écosystème et de simples citoyens, nous avons regroupé un ensemble de propositions et de recommandations destinées à offrir un cadre moderne et adapté à la mise en œuvre d'une nouvelle génération de lois et faire face à ces nouveaux enjeux sociétaux. ■

LES ENTREPRISES : VICTIMES DE LA CONSUMÉRISATION DES CYBERATTAQUES

Nicolas ARPAGIAN
Directeur scientifique, Cycle « Sécurité des Usages Numériques », INHESJ

L'informatisation des entreprises et des administrations a débuté il y a plusieurs décennies. Depuis lors, les organisations se sont développées en empilant les technologies du moment. Avec un seul mot d'ordre : que l'ensemble continue à fonctionner, sans faire exploser les coûts et en intégrant les épisodes classiques de la vie des affaires (fusion, absorption, délocalisation, externalisation…). Dans ce contexte, la vaste majorité des systèmes d'information en place dans le tissu économique et administratif des pays industrialisés est composée d'ensembles disparates combinant des équipements de plusieurs générations. Ce contexte est une première explication de la vulnérabilité desdits systèmes d'information. Les entreprises sont des corps sociaux qui ont un impact qui va bien au-delà de leur stricte activité économique. Leur fragilisation atteint ces producteurs de richesses mais également leurs collaborateurs et, par extension, toute une chaîne économique : les familles, les fournisseurs, les clients… Avec des conséquences tangibles en ce qui concerne la prospérité collective et l'état d'esprit d'une nation. C'est la raison pour laquelle les cyberattaques visant les entreprises ou les administrations peuvent avoir des finalités crapuleuses classiques, mais également des visées politiques afin de marquer les opinions publiques. Et ainsi influer sur le climat politique. Cette façon de faire peut s'inscrire dans une démarche terroriste, dont le but est précisément de diffuser un sentiment de peur auprès du grand public.

Utiliser la cyberattaque comme arme de communication

En janvier 2015, plusieurs centaines de sites Internet de collectivités locales, de syndicats d'initiative et autres musées à travers la France ont été victimes de « défaçage », consistant en la prise de contrôle du système de publication d'un site vitrine pour en modifier la page d'accueil. Ici, ce sont des appels au Jihad, de soutien à l'islam et des encouragements à conduire des opérations violentes qui se sont multipliés, prenant la place des informations habituellement présentées sur ces sites. Très impressionnantes, car étant très visuelles, ces campagnes sont en fait d'un faible niveau technique. Les attaquants ayant utilisé un logiciel qui leur désigne simplement les sites Internet dont les gestionnaires n'ont pas effectué les mises à jour basiques de sécurité.

Leurs structures éditrices sont souvent des associations ou des services communication qui ne disposent généralement pas des personnels à même d'assurer le suivi en termes de sécurité. De plus, comme il s'agit souvent de sites sans enjeux commerciaux immédiats, leur maintenance est rarement considérée avec attention. Il n'empêche que cela marque les esprits, notamment du grand public, qui peut se sentir affecté dans un cadre très local, qui fut longtemps à l'abri des attaques terroristes qui se concentraient essentiellement dans les grandes villes. Relayant ces séquences, les médias conventionnels participent également à en amplifier les effets. Dans le même esprit, l'attaque survenue contre les antennes de *TV5 Monde* en avril 2015 est un exemple d'un assaut numérique destiné à conduire ce qui est avant tout une opération de propagande. Idem en janvier 2015 avec la prise de contrôle à distance des comptes *Twitter* et *YouTube* du Commandement militaire étatsunien au Moyen-Orient (*Centcom*) par des partisans de l'État Islamique qui, pendant quelques minutes, ont diffusé des messages en faveur du «CyberCalifat». Une performance qui permet à l'assaillant numérique de ridiculiser l'entité ainsi piégée, de tirer parti de son aura médiatique et de valoriser son expertise technique au détriment de sa victime.

Intercepter les communications

Les outils d'interception des communications existent depuis que lesdites communications existent. Dès 1917, les échanges télégraphiques étaient abondamment écoutés par les autorités militaires. Aujourd'hui, cette capacité à capter les communications n'est plus l'apanage des services étatiques. Une simple recherche sur l'Internet permet d'accéder à des logiciels très abordables financièrement et techniquement qui permettent de sonoriser les smartphones: collecte des métadonnées (heure et durée des appels), détail de la navigation Internet, intégralité des SMS, accès au répertoire des contacts, suivi des déplacements, possible déclenchement à distance du micro de l'appareil… Des équipements relevant autrefois de la panoplie des services de renseignement mais qui sont désormais facilement accessibles. De quoi initier des opérations de repérage pour suivre une personnalité, connaître son emploi du temps et la localiser afin, le cas échéant, de lui porter préjudice.

Économie numérique et financement du terrorisme

Les organisations criminelles et terroristes se sont rapidement appropriées les réseaux sociaux et les systèmes de transferts de fonds pour faire circuler leurs avoirs. Un rapport[1] du Comité permanent des finances de la Chambre des Communes du Canada s'alarmait en 2015 que « l'État islamique utilise *Twitter*, *JustPaste.it*, *Asf.fm* et *PayPal* pour collecter et transférer des fonds ». La mondialisation des échanges rendue possible par la numérisation des communications accentue l'imbrication entre les structures illicites. Ainsi, Interpol[2] constate officiellement que l'extension de l'accès à l'Internet «*offre aux réseaux de criminalité organisée des possibilités de cybercriminalité croissantes, visant souvent à financer d'autres activités illégales*». Comme ce fut le cas longtemps avec la petite délinquance (vols de voiture, trafic de cannabis…) qui pouvait servir à des cellules locales d'organisations terroristes à financer leurs activités au quotidien, la cybercriminalité et la contrefaçon leur permettent de générer leurs propres ressources.

L'arme numérique pour frapper les infrastructures économiques

L'exposition au risque numérique des entreprises va croissant. Outre les possibles atteintes à l'image et à la réputation qui affectent leur capital confiance, la non-disponibilité de leurs services en ligne constitue des préjudices qui se traduisent en pertes financières très conséquentes. C'est par exemple le cas des «rançongiciels», ces outils malveillants qui chiffrent les fichiers des victimes. Celles-ci doivent payer une somme d'argent pour retrouver la maîtrise de leurs documents ou ne pas risquer de les voir diffusés sur la Toile. Même si l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) déconseille formellement[3] de verser la rançon réclamée, l'expérience montre que les entreprises victimes de «rançongiciels» sont plutôt prêtes à payer. Leur principal obstacle, pour régler la facture, étant souvent le bon ou mauvais maniement de la monnaie virtuelle, comme le *Bitcoin*. Les indispensables opérations de sauvegarde n'ayant pas été effectuées régulièrement, elles sont prêtes à être assez généreuses pour recouvrer leur actif numérique. C'est donc une activité très lucrative pour les escrocs, qui n'ont pas besoin d'être des experts en informatique, puisque des packs de ces *ransomwares* clés en main se

(1) «Financement du terrorisme au Canada et à l'étranger: mesures fédérales requises» - Rapport du Comité permanent des finances - Chambre des Communes - Canada - Juin 2015. http://www.parl.gc.ca/content/hoc/Committee/412/FINA/Reports/RP8048561/finarp13/finarp13-f.pdf

(2) «Interpol et le FBI resserrent leurs liens dans la lutte contre le terrorisme et la cybercriminalité», Communiqué d'Interpol - 23 septembre 2015. http://www.interpol.int/fr/Centre-des-m%C3%A9dias/Nouvelles/2015/N2015-142/

(3) Communiqué de l'ANSSI – *Alerte Campagne de Rançongiciel* – Site de l'ANSSI : http://www.ssi.gouv.fr/actualite/alerte-campagne-de-rancongiciel/

négocient facilement sur le Net. Les sociétés, rechignant ensuite à porter plainte, créent de fait une impunité pour ces racketteurs 2.0. On trouve la même efficacité avec les outils permettant la réalisation de campagnes de Déni de Service (DDoS). Quand la sollicitation simultanée de très grandes quantités d'ordinateurs infectés à l'insu de leurs légitimes propriétaires conduit à saturer des sites Internet, au point de les rendre complètement inopérants. Ces attaques par vagues peuvent causer des pertes très importantes à des sites de e-commerce, pour lesquels chaque minute de non-disponibilité se traduit par un manque à gagner qu'ils ne pourront pas compenser. Là encore, la menace de telles actions conduit des fleurons du commerce électronique à subir cette forme d'extorsion numérique, le plus souvent, sans aucun dépôt de plainte. L'automatisation de ces opérations rend possible leur déploiement sur un grand nombre de cibles réparties sur plusieurs pays. Seul le détournement du flux de connections malveillantes par un opérateur télécoms permet de neutraliser ces actions de déstabilisation.

Les Opérateurs d'Importance Vitale (OIV) : des cibles qu'il faut protéger à tout prix

La Loi française de Programmation Militaire de 2013 et ses arrêtés sectoriels, qui ont été publiés depuis le mois de juin 2016, et la Directive NIS (*Network & Information Security*) , qui a été adoptée par le Parlement européen en juillet 2016, établissent la désignation des Opérateurs d'Importance Vitale (OIV), dont le dysfonctionnement pourrait s'avérer fatal à la continuité de l'activité de la collectivité France. Ces entités doivent bénéficier d'un niveau de cybersécurité sans équivalent dans le reste de l'industrie et faire appel à des prestataires dûment répertoriés et qualifiés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pour conduire leurs opérations d'audit technique et de sécurisation de leurs systèmes d'information. Ce corpus juridique confirme l'importance stratégique des organisations informatiques, qui pourraient faire l'objet d'attaques de grande ampleur. Avec des conséquences sur la population et l'économie comparables à des actions terroristes. Cette dimension numérique est donc désormais une composante majeure de la stratégie globale de sécurité nationale. ■

(4) Dont le texte est disponible sur le site de la Commission européenne : https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

#TERRORISME

L'ENTREPRISE FACE AU TERRORISME À L'HEURE DE TWITTER

Emma VILLARD
Emma VILLARD Regional Security Manager, Autriche

Internet - et tout particulièrement le web contributif 2.0, peuplé de réseaux sociaux tels que *Twitter*, *Instagram* ou *Facebook* - ainsi que les nouveaux appareils de communication – notamment les smartphones (téléphones ayant une connexion à l'Internet) – sont en passe de profondément modifier la gestion de crise telle que les entreprises la pratiquent. S'il est vrai que les réseaux sociaux constituent une plateforme rêvée de propagande [1] et mettent à disposition des outils de communication cryptée (notamment *via WhatsApp* et *Telegram*) pour les groupes terroristes, ils sont également une aubaine inouïe pour ceux qui savent y traquer ces mêmes groupes.

Dans un premier temps : qui sont et que sont ces fameux social media ? Ces sites (et leur pendant sur téléphone : les applications) transmettent des flux d'information en réseau (*many to many*). Ils sont dits « sociaux » car l'internaute y est actif et participatif, il y crée et y partage du contenu à l'opposé de la logique contemplative dans laquelle le public est placé face aux *mass media* (*one to many*). *Twitter*, le plus connu des sites de *microblogging*, permet aux utilisateurs de poster à la fois des photos, des vidéos et des messages publics d'environ 140 caractères (la règle a récemment été assouplie [2]). En moyenne, 500 millions de *tweets* y sont publiés quotidiennement. *Facebook*, quant à lui, est un site de mise en relation privé (*social networking*), mais qui permet également de publier des messages publics ou d'organiser des événements visibles par tous. Il compte aujourd'hui une moyenne de 890 millions d'utilisateurs actifs par our, parmi lesquels 745 millions se connectent *via* un téléphone mobile. Par mois, nous sommes ainsi 1,39 milliard (dont 1,19 milliard sur mobile) à nous connecter sur *Facebook*.

Ces deux réseaux sociaux sont les plus célèbres et les plus populaires à l'échelle mondiale ; néanmoins, plutôt que *Facebook*, nous utiliserons plus volontiers *VKontakte* en Russie ou *Weibo* en Chine.

Les réseaux sociaux changent profondément la production et la circulation de l'information. Ils participent à son

(1) Voir : http://www.lemonde.fr/pixels/article/2016/08/18/twitter-affirme-avoir-supprime-235-000-comptes-de-propagande-terroriste-en-six-mois_4984673_4408996.html

(2) Pour plus de détails : http://www.lemonde.fr/pixels/article/2016/05/24/twitter-assouplit-la-regle-des-140-caracteres_4925575_4408996.html

décloisonnement, à sa «dé-hiérarchisation»: l'écriture publique est désormais démocratisée, *Twitter* ou *Facebook* permettant en effet à n'importe qui ayant un compte de publier des *posts*. La communication est horizontale et non plus uniquement pyramidale comme traditionnellement. Ainsi, des journalistes, chercheurs et autres passionnés sont devenus de véritables références en matière de djihadisme sur la twittosphère. Nous pensons ici, entre autres, à David THOMSON ou Romain CAILLET. Revers de la médaille: il est désormais possible de diffuser des contenus haineux ou faisant l'apologie du terrorisme (avant que ces derniers ne soient supprimés sous 24 heures[3]).

Par ailleurs, les réseaux sociaux peuvent garantir à ceux qui le souhaitent un degré d'anonymat – et par là une certaine impunité - puisque tout un chacun peut créer un compte sous un faux nom et ainsi (essayer de) se protéger d'éventuelles représailles ou de poursuites judiciaires.

Enfin, à l'immédiateté apportée par l'Internet, les *social media* ont ajouté la *mobiquité* permise par les smartphones: aucune contrainte de lieu ou de temps ne tient. L'utilisateur lambda est à même de publier des commentaires, des photographies ou des vidéos dans la minute qui suit un événement majeur ou pendant son déroulement-même. Les exemples ne manquent pas: *tweets* depuis l'intérieur du *Pulp* à Orlando, vidéos postées par des personnes habitant en face du Carillon à Paris, etc.

Puisque les entreprises ne disposent pas de moyens étatiques[4] pour suivre des milliers de comptes de militants radicalisés, et que l'acte terroriste n'est pas prévisible, que peuvent-elles tirer des réseaux sociaux afin de faire face à la menace terroriste? Pourquoi et comment peut-il être pertinent, pour le responsable sûreté d'une entreprise, d'utiliser les réseaux sociaux pour mieux se préparer à l'éventualité terroriste?

L'avant...

Tout d'abord, les réseaux sociaux sont une option supplémentaire dans la palette de solutions dont dispose le *security manager* pour mieux comprendre l'environnement dans lequel ses collaborateurs voyagent ou sont expatriés, et ensuite décider des mesures de sécurité à faire appliquer. En utilisant *Twitter* ou *Facebook* de façon méthodique, le responsable sûreté doit être capable de mieux cerner la menace indirecte à laquelle les employés de son entreprise sont exposés. Les «seuils de reportabilité» appliqués par les médias traditionnels afin d'éviter une surreprésentation de certaines problématiques, n'ont pas de place sur *Twitter* ou *Facebook*: si les attaques du groupe Boko Haram, dans le Nord-Est du Nigeria, ne sont mentionnées dans les journaux ou radios suivant l'actualité nigériane qu'au dessus d'un certain nombre de victimes, ou en fonction de leur localisation, il en va tout autrement sur *Twitter* où aucun filtre ou ligne éditoriale n'est appliqué (pour le meilleur et pour le pire).

Ensuite, le *security manager* peut mettre en place une veille spécifiquement liée au nom de son entreprise, d'un projet en particulier ou de personnes potentiellement exposées, afin d'être mis au courant de menaces directes.

Quand bien même la date et l'heure de la prochaine attaque ne seront évidemment pas communiquées sur les réseaux sociaux, il se peut que, au préalable, des commentaires négatifs soient publiés ou des menaces soient proférées à l'égard de telle personne ou tel projet. Si c'est le cas, ils se retrouveront presque immanquablement sur *Twitter*. Il revient alors au *security manager* de les intercepter. Mais comment?

Ces sites sont une mine d'informations pour le responsable sûreté qui peut faire des recherches ponctuelles à sa guise, en utilisant les mêmes opérateurs booléens[5] que sur *Google*. Sur plusieurs plateformes telles que *Twitter*, *Facebook* ou *Instagram*, les *hashtags* (mots-dièse) rassemblent toutes les publications sur un même sujet. Ainsi les *tweets* et photographies liés à l'«intifada des couteaux» à l'automne 2015 étaient regroupés sous des *hashtags* tels que *#troisièmeintifada* ou *#intifadadescouteaux* (en arabe).

Cela permet des recherches d'autant plus faciles: il suffit de taper le mot-dièse en question dans la barre de recherche d'un réseau social donné, et toutes les publications le mentionnant viendront automatiquement peupler la page visionnée.

Plutôt que de se limiter à des recherches ponctuelles, avoir un compte *Twitter* permet également de suivre de façon continue des utilisateurs sélectionnés. Si l'on s'intéresse à la situation socio-politique et sécuritaire dans une ville en particulier, il est – entre autres – pertinent de suivre les envoyés permanents de différents journaux et/ou radios qui y sont en poste: ils sont a priori une source fiable.

Notons que sur *Twitter* les comptes officiels sont identifiables à l'icône bleue représentée à côté du nom

(3) Pour lire le communiqué de la Commission européenne: http://europa.eu/rapid/press-release_IP-16-1937_fr.htm
(4) L'exemple d'Israël pendant l'«intifada des couteaux»: http://www.atlantico.fr/decryptage/comment-israel-reussi-lutter-contre-terrorisme-grace-aux-reseaux-sociaux-eric-denece-facebook-twitter-dark-net-web-internet-2672382.html
(5) Pour plus de détails sur les opérateurs booléens : http://www.ebsi.umontreal.ca/jetrouve/internet/booleens.htm

de l'utilisateur. Des étudiants, ou encore des personnes lambda passionnées par l'analyse du fait terroriste, seront potentiellement autant de sources intéressantes à suivre et dont on testera la crédibilité au fil du temps: voilà pourquoi il est nécessaire de conduire ces recherches avant l'irruption de la crise.

Attention toutefois à l'*infobésité* : l'information doit demeurer accessible. Suivre trop de comptes pourrait en effet noyer des informations importantes dans la masse. Afin d'améliorer la lisibilité d'une sélection soigneuse d'utilisateurs et rendre possible une réaction d'autant plus rapide en cas d'incident, il est recommandé de créer des listes de comptes *Twitter* et de les organiser géographiquement ou thématiquement.

Tweetdeck, par exemple, est un outil gratuit et facile à manier qui permet de visualiser ces listes dans des colonnes qui viennent occuper l'équivalent d'un large tableau de bord. Le logiciel les met automatiquement à jour à chaque nouveau *tweet* publié par un compte suivi.

Enfin, le *security manager* peut également mettre en place une veille géolocalisée à travers des solutions payantes telles que *Geofeedia* ou *Echosec*. Le principe est simple: l'utilisateur définit une zone sur une carte, le logiciel se charge ensuite d'aspirer toutes les publications géo-référencées dans la zone en question.

En effet, il faut savoir qu'un grand nombre de publications sur *Twitter*, *Instagram* ou d'autres réseaux sociaux tels que *Picasa*, *Flickr* ou *YouTube* sont géo-taggés, c'est-à-dire que les coordonnées GPS du lieu de leur publication leur sont associées.

...et l'après

Si les réseaux sociaux aident au suivi minutieux d'un événement annoncé au préalable, ils alertent aussi lors d'événements imprévisibles, tels que des attentats. Être rôdé à une utilisation efficace de ceux-ci s'avère donc bénéfique au *security manager* au moment où la crise se déclenche. S'il est connecté aux réseaux sociaux, il sera au courant d'un incident de façon quasi immédiate: les premiers *tweets* sont publiés dans les secondes qui suivent les explosions au Stade de France en Novembre 2015, fournissant ainsi de l'information bien avant les principaux médias traditionnels.

Du fait de ce temps de réaction très court, les réseaux sociaux s'avèrent être un élément clef pour toute cellule de crise, en fournissant rapidement de l'information et ce, en continu. Puisqu'ils sont aussi bien utilisés par des journalistes que par des personnes qui communiquent avec leurs proches, les réseaux sociaux mettent à disposition des informations extrêmement précises.

Grâce aux commentaires, vidéos et photos qui sont publiés, le responsable sûreté peut, en deux ou trois clics, avoir une idée de la violence d'une déflagration ou reconnaître la zone visée. Avant même qu'un journal ne publie une dépêche, on sait quel terminal de l'aéroport de Bruxelles Zaventem a été touché ou quelle partie de la Promenade des Anglais a été affectée à Nice. Enfin, la résilience des réseaux sociaux - encore constatée lors des attentats de Bruxelles en Mars 2016 - leur permet de continuer à fonctionner quand les réseaux téléphoniques sont saturés et donc de continuer à fournir des informations à ceux qui les surveillent.

En cas d'événement majeur, il se peut que les comptes de journalistes spécialisés, ou des quidams que l'on suit, ne relaient aucune information dans les 15 ou 30 premières minutes, voilà pourquoi il est important que les directions sûreté s'équipent avec des solutions – payantes celles-ci – telles que *Dataminr* ou *Visibrain* qui recensent (et traduisent, pour certaines d'entre elles) en permanence tous les *tweets* publiés de par le monde et envoient de façon proactive un e-mail au client en cas de *tweet* employant certains mots-clefs ayant été définis au préalable.

* * *

En tout état de cause, les réseaux sociaux ne sont pas la panacée et doivent être utilisés avec parcimonie. Lors des attentats de Boston en Avril 2013, parmi les 7,8 millions de *tweets* les plus populaires, 29% contenaient de fausses informations; 50% n'étaient que du bruit (c'est-à-dire des opinions et commentaires); et seuls 20% étaient des informations factuelles et vérifiées[6].

Ces *social media* doivent être perçus comme un canal d'information supplémentaire qu'il faut savoir maîtriser afin d'en tirer le maximum, en évitant à tout prix de se reposer sur une source unique. De la même façon, il est fondamental de pouvoir évaluer la crédibilité des comptes que l'on suit et, dans la mesure du possible, de recouper l'information avec des contacts sur place afin d'éviter les rumeurs.

Enfin, certains sites tels que *Google Images* ou *Tineye* permettent de savoir si une photo a déjà été publiée sur l'Internet ou s'il s'agit d'un photomontage; ce sont là des techniques redoutables pour vérifier la véracité

(6) Chiffres avancés par http://www.slate.fr/life/79342/attentats-boston-twitter-informations-fausses
(7) Voir : http://observers.france24.com/fr/20151106-comment-verifier-images-reseaux-sociaux

et/ou l'origine de photographies partagées et republiées des centaines de fois. Sur ce sujet, quelques «manuels» - tels que celui des Observateurs[7] - proposent un travail salutaire.

En somme, les réseaux sociaux sont un adjoint précieux au responsable sûreté qui se doit d'identifier des menaces «raisonnablement prévisibles» (*reasonably foreseeable*) en accord avec le «*Duty of Care*» auquel est légalement tenue son entreprise[8]. ■

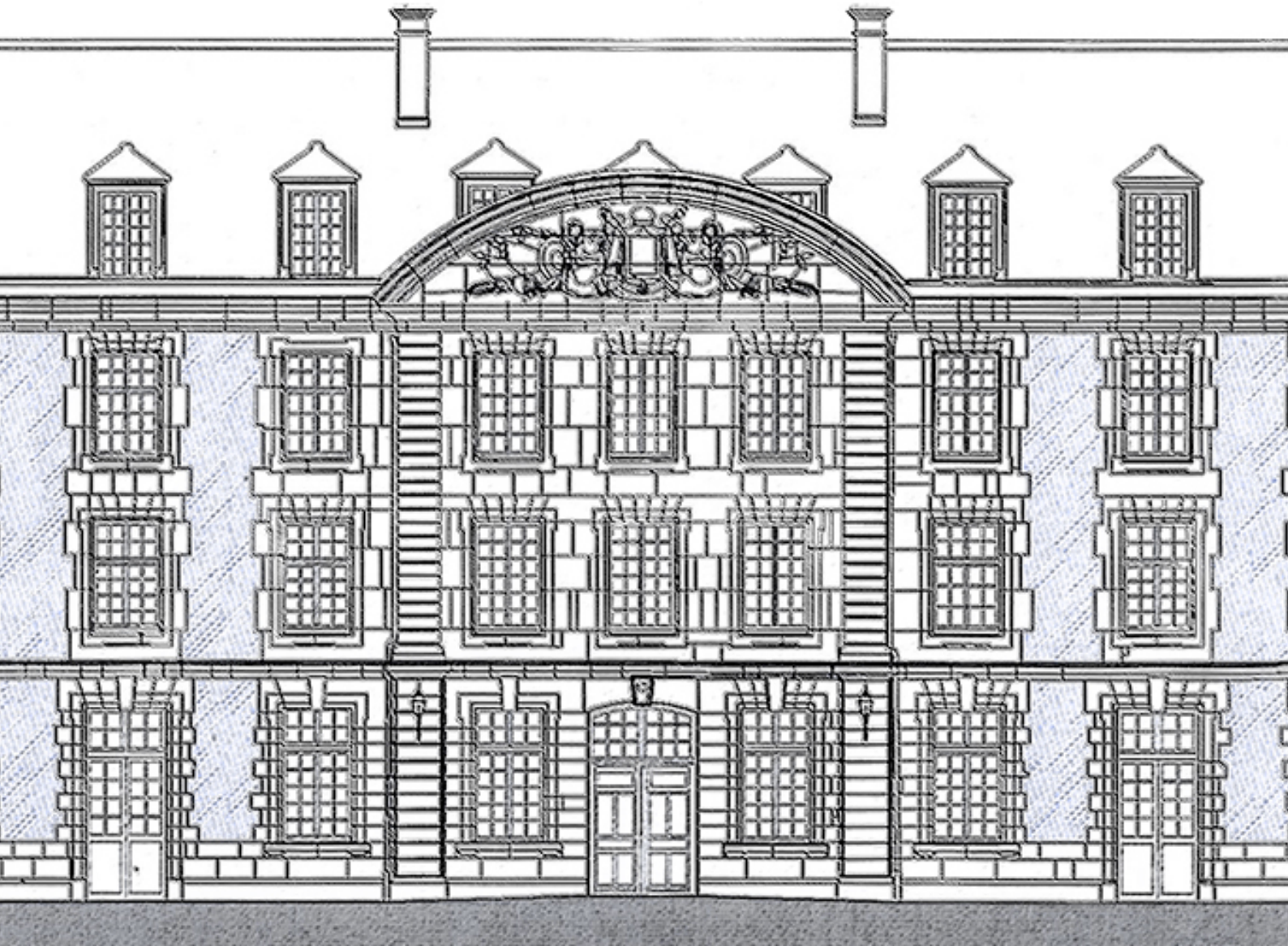
POUR ALLER PLUS LOIN

Apport des applications intelligentes et des réseaux sociaux dans la protection des citoyens :

Dernières nouvelles concernant les efforts de Twitter *dans la lutte contre l'extrémisme violent,* https://blog.twitter.com/fr/2016/lutte-contre-extremisme

(8) Pour davantage d'informations sur ce sujet, consulter : https://www.internationalsos.com/duty-of-care

PORTRAIT



HÉLÈNE CAZAUX-CHARLES

Directrice de l'INHESJ

Madame Hélène Cazaux-Charles, Magistrate, a été nommée Directrice de l'INHESJ le 28 octobre 2016. Nous la remercions vivement de bien vouloir nous consacrer un entxretien dans ce nouveau numéro de *Défis*.

Suite à son cursus à l'École nationale de la magistrature, Hélène Cazaux-Charles a été successivement nommée juge des enfants à Angoulême (1986), la Roche-sur-Yon (1990) puis Orléans (1997). En 1999, elle devient procureure adjointe à Évry. L'année suivante elle est nommée chargée de mission à la délégation interministérielle à la famille, avant de devenir conseillère technique au cabinet de la ministre déléguée à la Famille, à l'Enfance et aux Personnes handicapées en 2001. En 2004, elle est nommée vice-procureure, secrétaire générale du procureur de la République du tribunal de grande instance de Créteil, puis vice-présidente du tribunal de grande instance de Nantes en 2006. En 2008, elle devient ensuite inspectrice à l'inspection générale des services judiciaires, avant d'être nommée conseillère justice de Manuel Valls au ministère de l'Intérieur en 2012 puis à Matignon en 2014.

? Au regard de l'ensemble de votre parcours professionnel, pourquoi votre choix s'est-il aujourd'hui tourné vers la Direction de l'INHESJ ?

J'ai été nommée dans mes premières fonctions de magistrat en janvier 1986, il y a donc trente ans cette année. Mon parcours professionnel est marqué du sceau du métissage.

Métissage géographique d'abord : la moitié de ma carrière s'est déroulée en province, au sein de petites et moyennes juridictions, avant de rejoindre pour l'autre moitié de mon parcours professionnel, la région parisienne et exercer mes fonctions au sein de grandes juridictions.

Métissage fonctionnel ensuite, puisque, j'ai exercé ce métier, autant en qualité de magistrat du siège que de magistrat du parquet ; en outre, ces dix dernières années, d'un exercice direct et quotidien de mes fonctions auprès des justiciables comme des divers acteurs de la sécurité, je me suis tournée vers les fonctions de plus en plus stratégiques de gestion et d'organisation judiciaire.

Métissage institutionnel enfin, grâce à mes fonctions de conseillère en cabinet ministériel ; en effet, magistrate indéfectiblement liée à un ministère choisi par vocation, celui de la justice, j'ai pu vivre deux années très riches au sein du mi-

nistère de l'intérieur, avant de rejoindre le cabinet du premier ministre.

Juste un mot sur le ministère de l'intérieur: on ne sort pas de ce ministère comme on y est entré ! C'est un ministère attachant, passionnant, où l'on rencontre de belles personnes, habitées par un grand sens de l'intérêt général. Parler de droit pénal et de procédure pénale avec ceux qui, chaque jour, mettent en oeuvre les textes, dans des situations d'une complexité qu'il n'est plus besoin de décrire, assurément, transforme votre vision du métier de magistrat comme celle des métiers de policiers, de gendarmes, de préfets, pour ne citer que ceux-là.

Toutefois, pendant toutes ces années, absorbée par des fonctions très prenantes, j'ai toujours eu le regret de ne pouvoir bénéficier d'une dimension pourtant essentielle du métier de magistrat : celle de la recherche. J'ai dû construire seule, en dehors de l'institution, cet espace indispensable à l'exercice du métier de juge : l'espace de la pensée. Or, la responsabilité professionnelle, ce n'est pas seulement exercer correctement son métier, en reproduisant, même à la perfection, ce qu'on nous a enseigné ; c'est aussi revisiter nos pratiques professionnelles et faire évoluer le métier de magistrat, pour les générations qui viennent.

C'est donc naturellement que je me suis tournée vers l'INHESJ, lieu par excellence de métissage professionnel (en terme plus policés, lieu de l'inter-ministérialité , où se retrouvent le ministère de la justice, celui de l'intérieur, mais aussi le ministère de la défense, de l'éducation nationale et d'autres encore), lieu encore où se trace un chemin indispensable entre la recherche et les pratiques professionnelles.

? Comment abordez-vous cette nouvelle mission ? Avez-vous d'ores et déjà identifié des priorités à suivre ? Quelles sont vos ambitions pour l'Institut ?

J'aborde ces nouvelles fonctions avec enthousiasme puisque j'ai souhaité les exercer et que le premier ministre m'a fait l'honneur de me les confier.

Je rends tout d'abord hommage à l'action de mon prédécesseur, Cyrille Schott, qui a su donner à cet institut un élan et un dynamisme certain. Je dois désormais proposer un nouveau projet directeur au printemps 2017, pour les trois années qui viennent.

Mes priorités s'inscrivent logiquement dans le propos qui précède. Bien entendu, il faut conforter l'action des départements fondateurs de cet institut en veillant à répondre avec rigueur et précision aux enjeux de formation des hauts cadres de la sécurité, d'intelligence économique ou de gestion des crises.

Mais la France traverse depuis 2015 des épreuves redoutables qui ont provoqué une brutale prise de conscience : nous sommes entrés pour de très longues années dans un monde d'incertitude, voire de confusion. Nous devons non seulement contribuer à l'élaboration de réponses efficaces à ces risques et dangers connus, mais nous devons de surcroît anticiper les évolutions possibles de la menace, comprendre et déceler ses nouvelles formes, autrement dit aller au-delà de la prévision pour entrer dans le champ de la prospective. Il ne s'agit pas encore une fois de prédiction car il n'est pas sérieux de laisser croire qu'il puisse exister une science exacte nous affranchissant de l'incertitude et des épreuves qui s'annoncent. En revanche, il s'agit de mettre à jour des tendances lourdes et souterraines, à partir de l'observation de signes apparemment anodins, en apparence étrangers les uns aux autres et qui, éclairés par des savoirs rigoureux et diversifiés, légitiment la mise en oeuvre de stratégies anticipatrices pour aider les institutions à construire des politiques publiques préventives, à affronter avec sang-froid les crises quand elles surviennent, comme à en maitriser les conséquences. Ce sera une priorité pour moi.

En même temps, nous devons penser l'articulation du temps long et du temps court. Il faut absolument qu'un institut comme l'INHESJ, devienne un passeur, passeur entre d'une part la recherche fondamentale, nécessairement inscrite dans la durée et la complexité, d'autre part l'action, nécessairement inscrite dans le temps court des exigences opérationnelles et de l'actualité sociale et politique. C'est un second objectif, sans doute le plus difficile à mettre en oeuvre.

Le département « Etudes et recherches » est donc appelé à évoluer et à jouer un rôle majeur, en étroite concertation avec l'observatoire national de la délinquance et des

réponses pénales, en charge de conduire des études statistiques. La statistique est essentielle pour poser les bases d'un diagnostic sérieux comme pour piloter finement les politiques publiques. Essentielle mais pas suffisante. La statistique c'est l'art et la science du questionnement, une science qui exige des connaissances solides, diversifiées alliées à beaucoup de rigueur dans la construction des questions et l'interprétation des réponses.

Dès votre arrivée, le Premier ministre a décidé de confier à l'INHESJ une mission de réflexion concernant la législation relative à l'usage des armes par les forces de sécurité. Que pouvez-vous nous en dire ?

Par lettre de mission du 28 octobre le premier ministre a confié une triple mission à l'INHESJ : d'abord offrir un espace de dialogue apaisé avec les organisations représentatives de la police et de la gendarmerie, ensuite construire un espace de réflexion interministérielle entre le ministère de l'intérieur et le ministère de la justice, enfin proposer, dans des conditions de délai très contraintes, trois semaines, des pistes d'évolution de la législation sur l'usage des armes par les forces de sécurité pour répondre à l'évolution d'une menace préalablement caractérisée.

A l'issue de ces travaux, denses et constructifs, un rapport a été remis au premier ministre le 21 novembre. Il a servi de base à la réflexion du gouvernement dans le cadre du projet de loi dont l'examen est soumis au conseil d'Etat.

C'est une illustration parfaite de ce rôle stratégique de passeur qui peut et doit être celui de l'INHESJ.

Le droit est de plus en plus perçu comme une arme potentielle dans les différents affrontements économiques, qu'il soit au service d'une stratégie de puissance d'un Etat et/ou qu'il soit instrumentalisé par des acteurs privés, notamment devant les juridictions. En qualité de magistrate, quel regard portez-vous sur ces enjeux ? Pensez-vous que le niveau de prise de conscience générale sur ces problématiques soit suffisant aujourd'hui ?

Que le droit soit une arme très efficace pour qui en maîtrise l'histoire et la technicité n'est pas nouveau. On pourrait même presque dire que c'est l'essence du droit : se défendre, et dissuader pour conserver la paix !

La question se pose sans doute plutôt du côté des acteurs de l'institution judiciaire, de la formation des magistrats, des méthodes et de l'organisation du travail, de la maitrise complète des enjeux de ces contentieux, dont notamment celui de l'exécution des mesures probatoires, qui exposent parfois nos entreprises. Je connais les compétences de mes collègues actuellement en charge de ces diverses formes du contentieux du droit économique et financier. Il faut les soutenir car c'est effectivement là que se rencontrent tous les risques et menaces : fraudes fiscales, financement du terrorisme et du crime organisé, corruption, trafic d'influence, atteinte au secret des affaires comme à la compétitivité de nos entreprises etc.

La question se pose aussi aux Etats, bien sûr, car la justice, à la fois mission et vertu régaliennes, est garante d'une résolution impartiale des conflits. Le risque est ici celui d'un contournement de l'autorité judiciaire, qui n'occuperait plus qu'une fonction subsidiaire à celles d'instances de régulation privées, parfois affranchies des exigences d'impartialité et de transparence qui participent de l'équilibre démocratique. Ce risque renvoie certes à la question des moyens de la Justice dont la paupérisation a été soulignée à de nombreuses reprises et sur tous les bancs de l'assemblée. Mais bien au-delà, ce risque renvoie à l'évolution du rôle de l'autorité judiciaire au sein de nos démocraties.

Je pense que la prise de conscience est au rendez-vous. Encore une fois, le questionnement doit plutôt porter sur l'organisation judiciaire, sur la définition de véritables stratégies étatiques en la matière, enfin sur la diffusion et l'appropriation de connaissances pointues et pluridisciplinaires pour appréhender des enjeux complexes, à dimension souvent internationale, et requérant bien d'autres connaissances que celle du droit.

Tel est aussi le sens de la formation dispensée à l'INHESJ. ■

ENJEU

VERS UNE NORME DE MANAGEMENT DE LA SÛRETÉ ?

Pierre NOVARO
Président chez SALIX - Security Governance

Un comité technique de l'ISO, le TC 292 « Protective Security » pour être précis, a demandé à un groupe d'experts français de présenter une étude sur un projet de norme relative au management de la sûreté.

De quoi s'agit-il ?

Rappelons en premier lieu qu'en matière de sûreté, trois questions doivent être posées : Que doit-on protéger, contre quoi, et comment ?

Pour les deux premiers points, les questions sont bien cernées, si ce n'est les réponses.

Que doit-on protéger ? Le périmètre des actifs de l'entreprise, que la fonction sûreté est appelée à protéger, couvre :

- ***Les personnes***. Ce sont les salariés, quels que soient leur nationalité, leur contrat de travail ou leur lieu d'emploi, mais également les collaborateurs sous contrat de prestation. Et il ne faut pas oublier les clients. Les attaques terroristes contre des hôtels, des centres commerciaux, des restaurants, des musées, imposent cette protection.

- ***Les emprises immobilières***. Les sites de production ne sont pas seuls concernés. Ce sont tous les sites d'activité, qu'elle soit administrative, commerciale, logistique, de recherche… En fait, ce n'est pas tant la valeur immobilière du site qu'il faut considérer, mais sa capacité à concourir à la continuité d'activité.

- ***Les flux***. Pour les produits, il s'agit de sauvegarder la qualité et l'exactitude des produits fournis contre le risque de détérioration, de pollution, de destruction, ou de contrefaçon.
  Ensuite, on constate que la fraude s'exerce généralement sur les flux : flux de produits, mais aussi flux financiers, flux numériques. La lutte contre la fraude n'est pas traitée par la fonction sûreté dans toutes les entreprises. La question reste ouverte et la réponse dépend de la structure, du métier, et de la culture de chaque entreprise.

- ***Le patrimoine informationnel***. Il s'agit du savoir-faire, de la capacité à gagner des parts de marché, des projets…

Ce patrimoine informationnel n'est pas uniquement détenu et échangé sur des supports numériques. Il l'est par le biais de prototypes, de tests, de réunions et séminaires. La protection du patrimoine informationnel a trop souvent été confondue avec la sécurité informatique. La sûreté doit se positionner en maîtrise d'ouvrage par rapport à la sécurité des systèmes d'information, qui demeure un métier technique.

- ***La réputation***. Si la construction de l'image de l'entreprise et sa réparation, lorsqu'elle est dégradée, demeurent du ressort de la fonction communication, la sûreté n'est pas à l'écart de cette thématique. Par une sensibilisation appropriée, elle évitera aux collaborateurs de mettre en cause cette réputation par inadvertance ou négligence. Par une veille adaptée, elle détectera les risques de dégradation de l'image pour en aviser les responsables de la communication.

· ***Enfin, l'intelligence économique***. Étant, finalement, chargé de protéger l'activité et la profitabilité de son entreprise, le responsable de la sûreté contribue à l'analyse des risques, c'est-à-dire des enjeux, des vulnérabilités, de l'attractivité, de la probabilité, mais aussi des opportunités. Dès lors, la séparation de l'intelligence économique ou son intégration dans la sûreté dépend, là encore, de l'ADN de chaque entreprise.

Quant à l'identification de la menace, c'est-à-dire contre quoi doit-on se protéger ? Elle découle des précédentes réflexions : terrorisme, grande criminalité et petite délinquance, espionnage industriel, fraude sous toutes ses formes, dénigrement malveillant, activisme politique et social. On pourra, là encore selon les circonstances, intégrer ou pas les risques de conflits armés, de basse ou haute intensité, les troubles sociaux, voire les catastrophes naturelles.

Nous voyons que, sur ces aspects, un consensus existe généralement entre professionnels de la sûreté. Si le découpage des attributions peut varier d'une entreprise à l'autre, c'est pour mieux s'adapter à sa structure.

Il reste la question du Comment se protéger ?

Parfois, les réponses ne sont pas apportées, ou, surtout, le sont mal. Tout simplement parce que les questions n'ont pas été posées. Par exemple, qui est redevable de l'intelligence économique ? Ou qui est responsable de la gestion de crise ? Ou qui pilote la lutte contre la fraude ? Ce n'est pas le lieu ici de traiter des réponses à ces questions, mais relevons qu'il est important de bien définir les domaines à traiter et de bien préciser les dévolutions de responsabilités.

D'autres fois, la sûreté est considérée comme un simple empilement d'outils. Une collection de caméras de vidéosurveillance, de grillages, de vigiles, et même d'antivirus FOCUS et de moyens de chiffrement. Dans ces cas, l'approche logique ou l'édiction de règles font défaut. Et même quand des règles sont édictées, il arrive qu'elles se surajoutent les unes aux autres sans approche systémique. On réglemente alors le contrôle d'accès comme l'utilisation des broyeurs de documents, le suivi des voyageurs comme l'utilisation de la clef USB, la protection de l'information comme la spécification du grillage. La granularité de ces documents de référence n'a alors aucune cohérence et on peut en comparer la liste à un empilement de vaisselle où l'on aurait entassé une tasse à café, une soupière, un plat à poisson, une assiette à dessert…

D'autres fois encore, aucune de ces critiques ne peut être encourue. La fonction sûreté, sans doute conseillée par un expert spécialisé, répond à l'exigence de cohérence et à une réelle approche systémique. L'organisation est bien décrite, les responsabilités bien distribuées, les moyens bien affectés, les directives bien publiées.
Mais rien ne se passe.
Quelques feuilles, voire quelques classeurs au fond d'un placard, quelques octets, voire mégaoctets au fond d'un intranet, ne font pas la sûreté.

S'il n'y a pas un véritable planning de déploiement, d'accompagnement, de conseil, de formation des acteurs, tout effort aura été vain.

Enfin, dernières difficultés constatées, il arrive que les solutions adoptées reposent sur le tropisme du manager chargé de la sûreté. Sans chercher vainement à établir des catégories liées aux filières d'ingénieurs ou aux couleurs d'uniforme, il est incontestable que l'expérience acquise modèle les options d'organisation. Les organisations et solutions choisies le sont trop souvent en fonction de la personnalité du ou des acteurs chargés de la sûreté. Or, cette dernière n'est pas dans le cœur de métier de l'entreprise et les solutions adoptées sont donc trop souvent disparates et partielles.

La réponse repose donc non seulement sur un organigramme, des outils, des services et opérations, mais surtout et avant tout sur un pilotage de la fonction, selon un processus intégré et pérenne adapté à l'ADN de l'entreprise. Le projet de norme de management de la sûreté vise à garantir efficacité et l'éthique dans la réalisation de ces prestations.

Pour toutes ces raisons, il apparaît nécessaire d'établir une référence commune à toutes les structures chargées de la sûreté afin de s'assurer de leur efficience.

Une autre raison milite pour une telle référence commune : la coproduction de sûreté.

Il s'agit, d'une part, de la coproduction de sûreté tout au long de la chaîne de valeur. La fonction sûreté est généralement amenée à externaliser un certain nombre d'activités, et donc à s'assurer qu'un même niveau d'exigence est pris en compte par ses prestataires.

Mais c'est aussi toute l'activité de l'entreprise qui s'appuie sur des prestations externes. Par exemple, en matière de logistique. Confiant, comme on l'a dit, ses produits, c'est-à-dire ce qui conditionne sa survie et sa profitabilité, à un prestataire externe pour livraison à ses clients, l'entreprise a tout intérêt à ce que ce prestataire ait implémenté une organisation de la sûreté répondant aux mêmes exigences qu'elle.

Il s'agit aussi d'une coproduction de sûreté entre la sphère privée et la

sphère publique. Lorsqu'une attaque terroriste vise une école, un lieu de culte, un stade ou un rassemblement public, on voit s'imposer la coproduction de sûreté public-privé. Si la répression demeure du domaine étatique, la protection se met en place de façon identique et conjointe.

Ces circonstances soulignent le besoin de références communes partagées par tous les acteurs.

La norme constitue le meilleur vecteur pour porter ces références.

Le ministère de l'Intérieur a parfaitement saisi les enjeux puisqu'il co-anime le groupe de travail qui a présenté un rapport en ce sens à l'ISO.

Elle devrait décrire les fondamentaux d'une véritable organisation de la sûreté, non pas dans la vision statique d'un organigramme ou d'une accumulation d'outils et de procédures, mais dans une approche dynamique permettant souplesse et efficacité.

Il s'agit de rappeler les fondamentaux tels qu'ils sont décrits dans un système de management : définition des rôles et responsabilités, allocation des ressources, accompagnement et contrôle, communication, formation, sensibilisation, amélioration continue…

À l'origine de la démarche, un groupe de travail a été constitué au sein d'Afnor – Normalisation.

Animé par *SALIX-Security Governance*, il a réuni plusieurs catégories d'acteurs :

- De grandes entreprises, telles qu'EDF, Air France, AXA, GRTGAZ, l'Imprimerie Nationale, la RATP, le Musée du Louvre.
- Des organisations professionnelles telles que le GICAT.
- Des prestataires de sûreté tels que SURYS, IREMOS, ADENIUM, OFAPS.
- Des établissements de formation tels que l'INHESJ ou l'Université de Technologie de Compiègne.
- Des structures gouvernementales telles que le ministère de l'Intérieur, de l'Énergie et de la Mer, la DGITM (direction générale des infrastructures, des transports et de la mer) du ministère de l'Environnement, , le CNAPS.

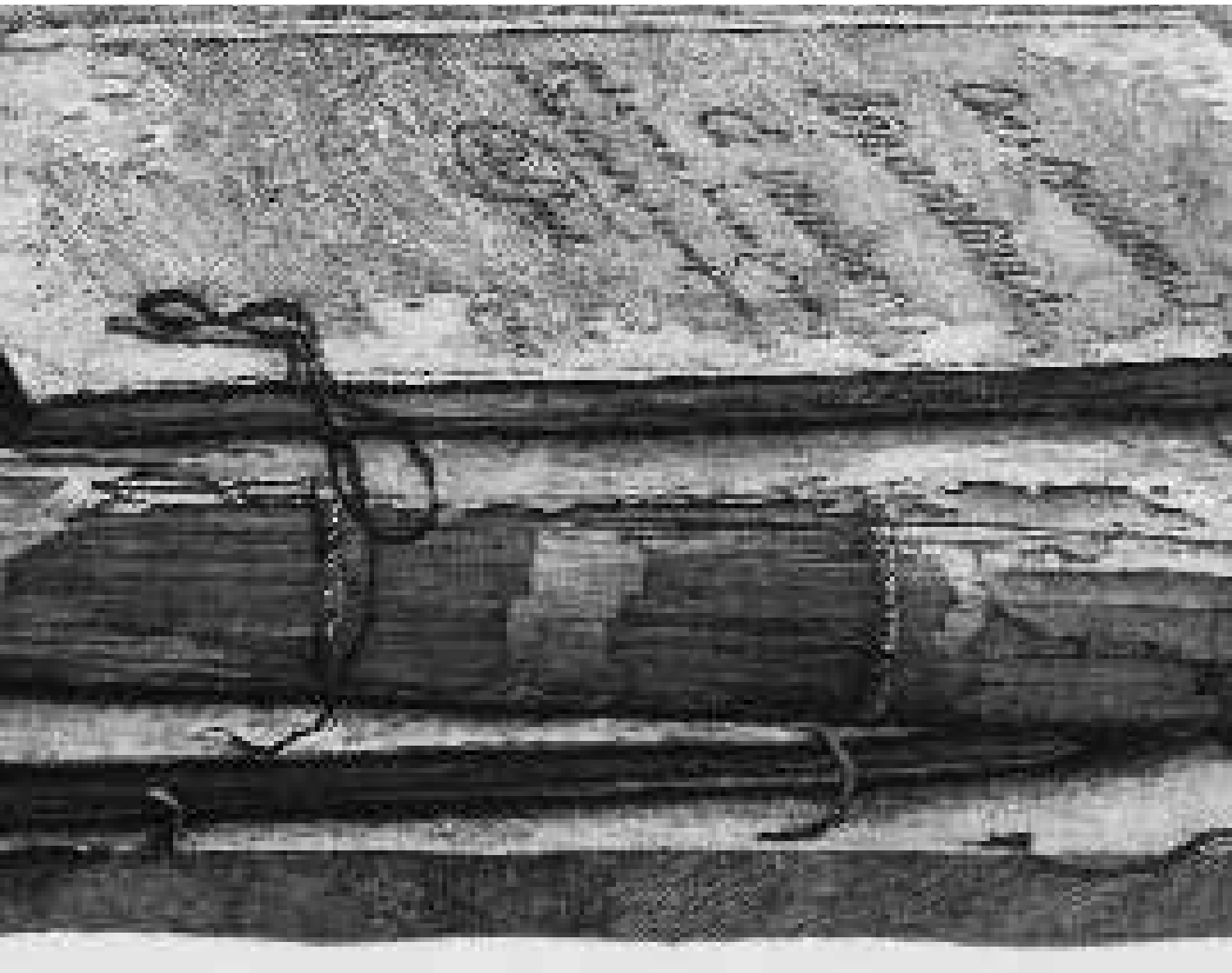
Cette variété d'acteurs montre tout l'intérêt que peut présenter une telle norme.

Pour les entreprises, il s'agit de répondre à l'exigence de sûreté de la façon, la meilleure et la moins contestable.
Pour les prestataires de services, c'est un avantage commercial.
Pour les prestataires de conseils, c'est une référence non subjective.
Pour les structures gouvernementales, c'est une garantie d'efficacité des différents acteurs et de bonne coordination.
C'est la raison pour laquelle les travaux au sein de l'ISO sont conduits dans le cadre d'un groupe de travail présidé par un représentant du ministère de l'Intérieur.

Le contexte actuel a constitué un moteur pour les experts français et le leadership de la France représente un avantage certain.
Des experts de plusieurs pays ont déjà manifesté leur intérêt pour une telle norme : Australie, UK, Suède, Italie, Allemagne…

Suite à la présentation du rapport d'étude au comité technique TC 292 de l'ISO en septembre 2016, l'élaboration de cette norme sous la conduite de la délégation française a été accueillie favorablement. ■

ACTUALITÉS ÉDITORIALES



FOCUS

CRIMES DU FUTUR

Jérôme BLANCHART (Dir.)
Premiers parallèles, 2016

Paru en avril 2016 aux Éditions Premier Parallèle, l'ouvrage de Jérôme Blanchart projette un futur dans lequel le crime, ou plutôt les crimes, semblent tout droit sortis de nos imaginations ou d'un bon roman policier. Pourtant, il ne s'agit pas là de fiction, et ces crimes, si futuristes qu'ils paraissent, ne sont finalement pas si éloignés de la réalité d'aujourd'hui, comme le montre l'auteur.

Crimes du futur pourrait être le titre racoleur d'un roman policier, qui mêlerait futurisme et science-fiction. Mais il s'agit bien du titre qu'a choisi Jérôme BLANCHARD, journaliste scientifique et rédacteur en chef du magazine *Sciences & vie Junior*, pour nous parler de crimes bien plus ancrés dans la réalité qu'on ne le pense. Car ce n'est pas d'un futur lointain, encore flou, dont il est question, mais d'un avenir bien plus proche; il s'agit déjà des Crimes de demain et même, si l'on en croit l'introduction, des Crimes d'aujourd'hui, puisque «les criminels de demain hantent déjà le présent».

En effet, la société que nous sommes, aujourd'hui, en train de bâtir, avec l'hyper connectivité et toutes les technologies de l'information et de la communication, fournit aux criminels un large panel d'armes possibles: Google car, imprimantes 3D, drones, objets connectés... Ces objets *a priori* inoffensifs, déjà bien implantés dans le monde actuel, seront ou sont déjà détournés à des fins malveillantes. Jérôme Blanchart consacre un chapitre par «arme» nouvelle, tout en montrant bien le mauvais usage qui en est déjà fait ou qui pourrait l'être facilement.

Mais les Hommes ne se soucient pas ou trop peu de ces risques futurs qui pèsent au-dessus de leur tête comme une épée de Damoclès. Ces crimes concernent en effet le monde virtuel, se passent derrière les écrans d'ordinateurs, de smartphones, de GPS. Or pour ce qui a trait aux Technologies de l'Information et de la Communication, la sécurité est le cadet des soucis. L'Homme a assez naturellement le réflexe de ne prendre garde qu'au monde réel, dans lequel il a toujours évolué, et ne s'est pas encore assez familiarisé avec le monde virtuel. Avec l'arrivée prévue de dizaines de millions d'objets connectés, l'évolution perpétuelle des moyens d'information et de communication et l'augmentation grandissante de personnes connectées, ne serait-ce pas le moment d'accorder une attention plus grande à ces nouveaux enjeux de sûreté?

Manon CHINI

SÉLECTION D'OUVRAGES

Histoire mondiale de la guerre économique

Ali LAIDI

Editions Perrin, 2016

La guerre économique est une vieille histoire. Elle est à l'économie ce que la science de la guerre est à la politique : un affrontement pour capter les ressources. Dès la préhistoire, les hommes s'affrontent pour conquérir les meilleurs territoires de chasse et de cueillette, tandis que Phéniciens, Egyptiens, Romains et Chinois de l'Antiquité sécurisent leurs routes commerciales pour éliminer la concurrence. Au Moyen Age, les marchands allemands regroupés au sein de la Hanse mènent des guerres, déclenchent des blocus économiques, le tout au nom de la défense de leurs intérêts commerciaux. Avec les grandes découvertes, les Etats prennent les rênes : Portugais, Espagnols, Hollandais, Anglais et Français se livrent de terribles batailles pour s'emparer des épices des nouveaux mondes. Lors du premier conflit mondial, détruire le potentiel commercial de l'adversaire est un des buts de guerre affichés, tandis qu'aujourd'hui les multinationales affrontent l'hyperconcurrence avec leurs propres armes, lesquelles n'ont souvent rien à envier à celles des services de renseignements et de sécurité des Etats.Cette première synthèse sur la guerre économique démontre l'enracinement des conflits de ce type dans l'histoire. On comprend, à sa lecture, pourquoi le mythe libéral du « doux commerce » a toujours nié cette évidence : la politique n'a pas le monopole de la violence. Elle le partage avec l'économie.

Intelligence économique et pôles de compétitivité

Damien BRUTE DE REMUR

VA Press, 2016

Cet ouvrage part du constat que les Pôles de Compétitivité sont par nature des leviers de la politique nationale d'Intelligence Économique. Il cherche avant tout à présenter des outils pratiques, expérimentés et évalués sur le terrain à partir d'un cas vécu. Pour cela il propose, après une synthèse simple et concrète des principaux concepts, un renversement culturel en passant du management DE l'information au management PAR l'information. Cette démarche donne tout son sens à l'IE. Les quatre personnalités interviewées tracent des axes extrêmement éclairants pour une pratique performante de l'IE. L'ensemble s'adresse aux praticiens publics et privés aussi bien qu'aux étudiants et enseignants désireux d'aborder la discipline de manière vivante et concrète. Les points forts de l'ouvrage:

- Un guide pratique pour la mise en place d'une démarche d'intelligence économique par l'exemple. Il est destiné à un public de chefs d'entreprises, de fonctionnaires territoriaux, d'enseignants-chercheurs et d'étudiants.
- Un ouvrage illustré par de nombreux schémas pour expliciter le propos de l'auteur et des entretiens avec quatre personnalités incontournables de l'intelligence économique en France.
- Un auteur incontournable de la discipline en France, pour avoir consacré l'essentiel de sa carrière à la recherche en intelligence économique.

Le droit du renseignement pour discerner les limites juridiques du droit du renseignement en France

Olivier DE MAISON ROUGE

Lexis-Nexis, 2016

Le monde actuel connaît de nouvelles menaces et nécessite de nouvelles réponses, parfois attentatoires, provisoirement ou durablement, aux libertés individuelles. Les événements tragiques de l'année 2015 ont mis en perspective les réalités, tout autant que les difficultés et les carences de l'État face à ces menaces.
Afin de comprendre les grands enjeux contemporains, qu'ils soient militaires, géopolitiques, stratégiques ou encore économiques, l'activité du renseignement est un souci majeur autant qu'un besoin prégnant, malgré les suspicions parfois légitimes entourant la matière.
Le renseignement d'État a été profondément remanié depuis 2008, pour aboutir à l'adoption de la loi du 24 juillet 2015, régissant les moyens et méthodes de renseignement et définissant les modes de contrôles institutionnels et juridictionnels.
Le droit du renseignement d'État, est un droit d'exception, de police administrative, faisant bénéficier de pouvoirs exorbitants les services compétents mais strictement encadré quant à l'usage des moyens prévus par la loi.
Le renseignement économique est quant à lui essentiellement une activité privée, dont la pratique et les méthodes sont sanctionnées a posteriori par le juge judiciaire, en regard des règles de droit commun, bien que l'information économique intéresse désormais davantage la sphère publique.
Il paraît donc essentiel d'examiner en parallèle ces deux activités concourant au même objectif : connaître l'environnement, anticiper les mouvements systémiques et plus généralement réduire les risques et l'incertitude.

Sécurite d'entreprise : le défi des menaces asymétriques

Etienne JACOB

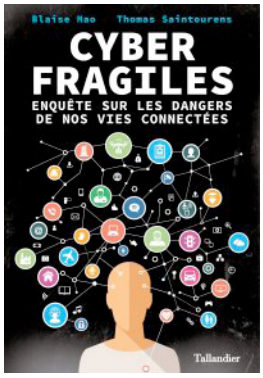
L'Harmattan, 2016

Le Pentagone engage de nombreuses sociétés de sécurité privée pour des missions de soutien à l'arrière. Paradoxalement, les conflits ont mis en évidence autant les archaïsmes que les imperfections du secteur privé de la sécurité. Les entreprises, celles qui évoluent à l'international dans des zones à risque élevé, sont contraintes de réajuster leur politique de sécurité (renforcement des technologies de la sécurité et recours à des agents de surveillance privée). Sur le continent africain émergent des risques variés, autant pour les forces de sécurité étatique que pour les entreprises.

Cyber fragiles - Enquête sur les dangers de nos vies connectées

Blaise MAO et Thomas SAINTOURENS

Tallandier, 2016



Des centaines de milliers de cyberattaques quotidiennes dans le monde. Plus un jour sans qu'une affaire de vol de données, de site piraté ou d'arnaque en ligne ne défraye la chronique. Cette enquête inédite et captivante révèle à quel point notre hyperconnexion nous rend vulnérables.

Le risque de piratage nous concerne tous. Ces menaces se nichent sur les réseaux sociaux ou dans nos boîtes mail, elles ciblent nos informations bancaires, les données stratégiques de nos entreprises comme nos données médicales et s'infiltrent dans notre ordinateur de bureau, notre tablette tactile, notre smartphone ou notre voiture. Avec le développement des « villes intelligentes » et le succès des objets connectés – déjà 25 milliards en circulation sur la planète –, elles atteignent désormais notre intimité.

Pour comprendre ces menaces et analyser leur portée, Blaise Mao et Thomas Saintourens ont enquêté auprès de professionnels de la cybersécurité, de hackers, de militants des libertés sur Internet et de responsables politiques. Des failles dans les programmes informatiques les plus usuels jusqu'au potentiel de surveillance des États, ce livre nous entraîne dans un récit vertigineux dont nous sommes les protagonistes et démontre à quel point il est nécessaire de reprendre la main sur nos vies numériques.

Menaces mortelles sur l'entreprise française

Olivier HASSID

Nouveau Monde, 2016

Affaires d'espionnage, amendes records, fusions… Le sort semble s'acharner sur les entreprises françaises. En apparence, rien ne relie les condamnations de BNP Paribas et Alstom, le piratage des données d'Areva, le rachat d'Alcatel et Lafarge. En coulisses, certains États peu scrupuleux ont déclaré la guerre aux fleurons tricolores.

Leur objectif : déstabiliser, piller et racheter pour régner. Car nos pépites font un carton à l'international. Réacteurs nucléaires, produits de luxe et high-tech sont devenus la proie des investisseurs étrangers, adeptes des profits à court terme et des économies de R&D. Au côté des grands groupes, ETI et PME ne sont pas épargnées.

Soutenu par des professionnels de la sécurité et de l'intelligence économique, cet ouvrage dresse un bilan accablant pour notre économie. Privées de débouchés, dépouillées des technologies qu'elles ont mis des années à développer, nos entreprises sont en plein décrochage. Or ce désastre n'est pas l'effet du libre jeu des marchés : il traduit une mondialisation à géométrie variable, régie par des dispositifs juridiques et sécuritaires étrangers visant à éliminer toute concurrence.

Seul un traitement de choc pourra éviter la mort programmée de l'entreprise française : droit de regard de l'État dans les domaines stratégiques, mobilisation d'investisseurs nationaux, déploiement d'un arsenal juridique en matière de secret des affaires, renforcement et synergie des services de sécurité. Loin de prôner un retour au protectionnisme, ce livre réaffirme la nécessité d'un patriotisme économique au-delà des clivages, avant qu'il ne soit trop tard.

Le secret des affaires
Comment le droit protège-t-il le secret des affaires ?

Thibault DU MANOIR DE JUAYE et Sabine MARCELLIN

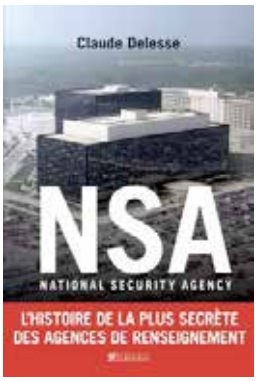
Lexis-Nexis, 2016

La protection du secret des affaires est au XXIe siècle, ce que le brevet a été pour l'entreprise aux deux siècles précédents.
À l'ère du big data, l'entreprise est centrée sur la donnée, et les enjeux économiques de l'information deviennent considérables. Par conséquent, connaître le régime juridique de la protection du secret des affaires est essentiel pour les professionnels.
Proposition de directive du 28 novembre 2013 devant être soumise au Parlement européen en avril 2016, proposition de loi du 16 juillet 2014, amendements dans le cadre de la loi Macron, évolutions jurisprudentielles sur le vol de données de mai 2015, nouvelles réformes de l'article 323-3 du code pénal… Les évolutions et débats récents sur le secret des affaires vont de pair avec l'émergence des intérêts fondamentaux de la Nation, à tel point qu'il est impossible de les examiner séparément.
Cet ouvrage est indispensable pour permettre à toutes les professions juridiques, aux publics concernés tels que les opérateurs d'importance vitale (OIV) et aux étudiants, d'appréhender les enjeux de la protection du secret des affaires, d'autant que cette protection, aujourd'hui simple faculté, est en passe de devenir une véritable obligation de protection de l'information.

NSA. National Security Agency

Claude DELESSE

Tallandier, 2016

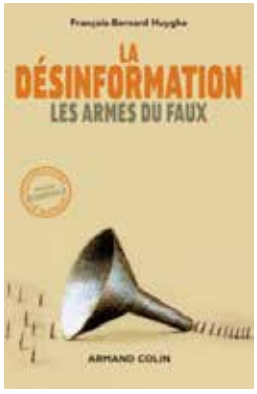


Plus grande agence de renseignement électronique au monde, la NSA espionne tout le monde : du terroriste au hacker, du grand industriel à l'employé de base, du chef d'État au simple citoyen. Comment fonctionne-t-elle? Quelles sont ses missions? Quelles sont ses cibles? Quels scandales a-t-elle traversés? Quelles conséquences aura l'affaire Snowden sur son avenir?
Depuis sa création en 1952 jusqu'à la lutte contre Al-Qaïda et Daech, en passant par les guerres de Corée, du Vietnam, d'Afghanistan et d'Irak, la NSA apporte depuis plus de soixante ans un soutien aux décisions politiques et militaires des États-Unis. Il est fascinant, voire inquiétant, de découvrir son univers interne et ses programmes, de percevoir l'envergure et l'outrance de la collecte d'informations au nom de la lutte contre le terrorisme et la criminalité. Instrument au service de la puissance américaine, la NSA s'est livrée à de tels excès que, en 2013, Edward Snowden, jeune agent d'à peine 30 ans, en a révélé les abus, provoquant la plus grande crise de son existence. Hors de toute polémique et en s'appuyant sur de multiples sources, Claude Delesse retrace pour la première fois l'histoire de la NSA. Elle décrit ses rouages et ses alliances, révèle ses dérives et ses menaces, éclairant ainsi l'incroyable épopée d'une agence obsédée par le secret.

La désinformation - les Armes du faux

François-Bernard HUYGHE

Armand Colin, 2016



Info, intox ? Complot, rumeur ? La désinformation serait partout, et la vérité nulle part. Ces questions obsèdent nos sociétés où il semble qu'en ligne tous puissent s'exprimer et que rien ne doive rester caché. Pourtant, la désinformation a une histoire. Elle s'exprime pendant la guerre froide et accompagne la mondialisation, avant que le web et les réseaux sociaux ne lui ouvrent de nouveaux horizons.
En explorant les mécanismes de ce qui nous abuse et que nous refusons parfois de croire, des systèmes de pouvoir apparaissent et de nouvelles formes d'idéologies se manifestent. Quand la vérité des faits devient l'objet central de nos luttes, la désinformation n'est plus qu'une question morale : elle est un enjeu stratégique.

Le continent des imprévus - Journal de bord des temps chaotiques

Patrick LAGADEC

Manitoba Les Belles Lettres, 2015

Depuis le tournant du siècle, citoyens et responsables sont confrontés à la multiplication des défis majeurs sur toutes les lignes de front : des dislocations géopolitiques ont bouleversé nos cartes de référence, un état de dérèglement économique et de mutation culturelle s'est durablement installé, des épidémies au potentiel gravissime ont déferlé à l'échelle intercontinentale, le désordre climatique commence à présenter la note… Le risque est de voir l'émotion anxiogène bloquer toute réflexion, conduire au découragement et à l'abandon, exacerber la nostalgie d'un ordre ancien qui n'est plus.
L'auteur du présent ouvrage ne fuit pas la réalité de ces formidables méga chocs et il sait que l'on ne résout pas des problèmes inédits avec d'anciens remèdes. En un mot, une prise de distance sereine, rationnelle mais nourrie d'expérience personnelle et cosmopolite, est nécessaire. C'est ce que propose ce journal de bord qui, au fil des pages, appelle à ce que l'auteur nomme un dépassement : un dépassement de nos craintes pour forger, en profondeur, de nouvelles visions, aptitudes et grammaires d'action.

Alstom, scandale d'état

Jean-Michel QUATREPOINT

Fayard, 2015

Le 19 décembre 2014, presqu'à la sauvette, les actionnaires d'Alstom décident de vendre à l'américain General Electric les activités énergie du groupe, un des leaders mondiaux pour l'équipement des centrales électriques. Une bonne affaire pour GE. Une mauvaise pour la France. Après Pechiney, Arcelor, Alcatel, c'est le dernier acte du grand démantèlement de l'industrie française. La France perd le contrôle d'un secteur stratégique : l'électricité, l'un des piliers de la croissance économique du XXIe siècle. D'Alstom, il ne reste que la branche Transport.

De la fabrication des turbines Arabelle indispensables à la nouvelle génération des EPR à la maintenance du parc existant de centrales nucléaires, c'est toute la filière nucléaire française qui est ainsi déstabilisée. Au moment même où Areva est en grande difficulté. Il n'y aura pas d'« Airbus européen » de l'énergie non plus.

Comment une telle chose a-t-elle pu se produire ? Pourquoi n'a-t-on pas négocié un accord équilibré ? Pourquoi l'État n'a-t-il rien vu venir ? Quel rôle ont joué les deux ministres, Montebourg, puis Macron ? Oui, il y a bien une affaire Alstom.

Jean-Michel Quatrepoint mène une enquête serrée autour de ce dossier. Il raconte la nouvelle stratégie des États-Unis pour faire main basse sur les fleurons industriels européens, et français en particulier. Notre classe dirigeante se révèle impuissante à faire prévaloir les intérêts du pays.

Quand le digital défie l'état de droit

Olivier ITEANU

Eyrolles, 2016

Avez-vous déjà lu les fameuses CGU (Conditions générales d'utilisation) avant de créer un compte sur Facebook, Google ou Twitter ? Ces dernières prévoient qu'en cas de litige le juge californien sera compétent. La cour d'appel de Pau a jugé en 2012 ce type de clause abusive, car contraire au droit français de la consommation. Or, quatre ans plus tard, ces plateformes continuent de maintenir cette clause abusive dans leurs CGU au mépris du droit et en toute impunité. Car qui a les moyens d'affronter la puissance financière et juridique des géants américains du numérique ? Les Etats européens eux-mêmes abdiquent ou, au mieux, cherchent à négocier plutôt qu'à faire appliquer la loi.

Vie privée, liberté d'expression, droits d'auteur, rôle de l'Etat dans les mécanismes de régulation… Alliés de circonstance des libertariens de la côte ouest des Etats-Unis, les grands acteurs du numérique imposent leurs règles et leurs valeurs. Le digital est-il en passe de rendre inopérants les droits français et européen, après avoir chamboulé la technologie, nos modes de vie et les modèles économiques existants ? Dans cet essai accessible à tous, Olivier Iteanu lance un cri d'alerte : s'il ne reste plus au peuple européen le choix de sa loi, que lui reste-t-il de sa souveraineté ?

Le modèle Californien
Comment l'esprit collaboratif change le monde

Monique DAGNAUD

Odile Jacob, 2016

La Californie, où sont nés Internet et les technologies qui ont bouleversé notre monde, est au coeur de l'économie mondiale. Elle est aussi le lieu où s'inventent un nouveau modèle de société et un autre imaginaire politique.
Fondée sur la collaboration et le partage, valorisant l'innovation, l'entrepreneuriat et l'association, cette société nouvelle offre au reste de la planète l'image d'un avenir possible. Monique Dagnaud invite dans ce livre à examiner de plus près ce défi lancé par la Californie, et à mesurer aussi ce que cet esprit collaboratif peut apporter de neuf à notre pays.
Une analyse du phénomène californien, jamais encore menée en France.

L'âge de la multitude
Entreprendre et gouverner après la révolution numérique

Henri VERDIER et Nicolas COLIN

Armand Colin, 2015

Et si nous étions devenus, sans le savoir, les principaux acteurs de l'économie numérique ? Si nos vies, nos inter-actions, nos créations étaient la source déterminante de la valeur et de la croissance ? Un monde nouveau, né de la révolution numérique, consacre le règne de milliards d'individus désormais instruits, équipés et connectés. Ensemble, ils forment une puissante multitude qui bouleverse l'ancien ordre économique et social. Loin d'être l'affaire des seules entreprises technologiques, l'économie numérique est au contraire dominée par ceux — entreprises, administrations, associations — qui ont su s'allier à cette multitude. Après la révolution numérique, l'enjeu stratégique est de susciter, de recueillir et de valoriser la créativité des individus. Tel est le sens de cet essai, souvent radical et décapant, qui invite entrepreneurs et politiques à comprendre et à utiliser la valeur considérable créée par chacun d'entre nous. Cette deuxième édition révisée est précédée d'une nouvelle préface.

L'année stratégique 2017 - Analyse des enjeux internationaux

Pascal BONIFACE (dir.)

Armand Colin, 2016

Marqués par le terrorisme, le chaos économique, mais aussi par des avancées diplomatiques historiques, ces derniers mois auront encore mis à l'épreuve le concept de « communauté internationale ». Des transitions – passées ou à venir – en Amérique du Nord à l'horizon d'un quatrième mandat pour Vladimir Poutine, de la recomposition de la puissance en Asie et des rapports de forces au Moyen-Orient aux doutes européens, des divergences africaines au retour de l'instabilité en Amérique latine, sans oublier la COP21 : L'Année stratégique 2017 analyse les événements marquants de l'année écoulée et livre des éléments prospectifs permettant d'appréhender leurs développements futurs.
Un outil de compréhension des relations internationales - 197 fiches-pays (indicateurs politiques, sociaux, démographiques, économiques, énergétiques, environnementaux et militaires)
- 7 fiches régionales
- cartes régionales et thématiques
- rappel chronologique des événements qui ont marqué l'année
- annuaire statistique mondial des données essentielles

L'état des entreprises 2016

DAUPHINE RECHERCHES EN MANAGEMENT

La Découverte, 2016

Pour la huitième année consécutive, DRM propose dans ce « Repères » un regard pluriel sur le monde des entreprises en mettant l'accent sur les enjeux et tendances actuels.
Parmi les sujets traités cette année, le thème du développement durable est à l'honneur avec des contributions sur les multiples nuances entre publicité verte et greenwashing, les facteurs explicatifs de la demande de produits socialement responsables, les enjeux pour les entreprises de l'évolution de nos relations avec les objets-déchets ou encore la perception du climat éthique des organisations par leurs salariés. L'ouvrage aborde également des questions centrales comme celles de l'engagement des salariés ou du rôle des médias sur les marchés financiers. Enfin, un bilan sur l'adoption des normes IFRS en France est proposé ainsi qu'une analyse de la compétitivité des entreprises françaises selon une approche institutionnelle. Des références bibliographiques sont fournies à la fin de chaque contribution et l'ouvrage s'achève par une chronologie des événements récents. L'ensemble fournit une synthèse actualisée, un véritable état annuel des entreprises.
Cet ouvrage a été réalisé par une équipe de chercheurs de DRM dirigée par Gwénaëlle Nogatchewsky et Véronique Perret.

Les leçons de stratégie et de tactique pour l'entreprise

Carl VON CLAUSEWITZ

Maxima, 2016

Aborder chaque situation professionnelle à la manière d'une opération militaire est passionnant et extrêmement efficace. Ce livre montre comment appliquer à votre entreprise et à votre carrière les conseils de l'un des plus grands auteurs en stratégie militaire. «De la guerre», le célèbre ouvrage de Carl von Clausewitz dont les principes sont étudiés par tous les stratèges depuis plus de 150 ans, va faire de vous un meilleur chef et un plus fin tacticien. Avec ce livre, découvrez les idées de Clausewitz appliquées à l'univers professionnel et à la société contemporaine. Ses théories vous donneront des arguments pour comprendre :
- pourquoi le commerce, comme la guerre, n'est ni un art ni une science;
- comment faire de votre entreprise une forteresse imprenable;
- l'importance d'un commandement fort;
- les mérites et les limites d'une attitude sans merci;
- et toutes les raisons pour délaisser votre smartphone… et ouvrir de véritables «lignes de communication».

L'État en mode start-up - le nouvel âge de l'action publique

Yann ALGAN et Thomas CAZENAVE

Eyrolle, 2016

L'action publique semble aujourd'hui faire face à une équation impossible, entre réduction des moyens et multiplication des mécontentements. Les approches traditionnelles de la réforme sont mises en échec. A cette approche décliniste, L'Etat en mode start-up oppose une autre vision, celle d'une action publique réinventée, plus agile et collaborative, «augmentée» par l'innovation technologique et sociale.
Transformation numérique, association des citoyens, remise en cause d'un modèle uniforme de service public au profit d'une approche personnalisée, confiance et responsabilisation de ceux qui ont la charge au quotidien de l'action publique : un nouvel âge de l'action publique se dessine. Il faut pour le porter une nouvelle génération d'acteurs publics. En donnant la parole à certains d'entre eux, cet ouvrage montre que la réforme est possible, qu'elle est bien souvent en cours, et qu'elle est porteuse de réponses aux inquiétudes de notre société.
Un ouvrage sous la direction de Yann Algan, doyen de l'Ecole d'affaires publiques de Sciences Po et professeur d'économie, spécialiste de l'économie numérique et collaborative, et Thomas Cazenave, inspecteur des finances, directeur de cabinet adjoint du ministre en charge de l'Économie, de l'Industrie et du Numérique, enseignant à Sciences Po et à l'ENA.

Le monde au défi

Hubert VEDRINE

Fayard, 2016

Pour Hubert Védrine, la « communauté internationale » est un objectif, pas encore une réalité. Ni les idéaux de l'ONU, ni le marché global n'ont suffi à la fonder. Le monde est éclaté, le pouvoir est émietté, les mentalités s'opposent, chaque peuple est mu par ses propres passions et ses intérêts immédiats. Et si la cohésion de l'humanité se créait autour de la vie sur la planète ?
Dans ce nouvel opus Hubert Védrine trace un portrait lucide de notre monde et tente de jeter un pont entre la géopolitique et l'écologie.
Un éclairage clair et puissant sans langue de bois sur la réalité du monde d'aujourd'hui par l'ancien ministre des Affaires étrangères.

Le Mur de l'Ouest n'est pas tombé

Hervé JUVIN

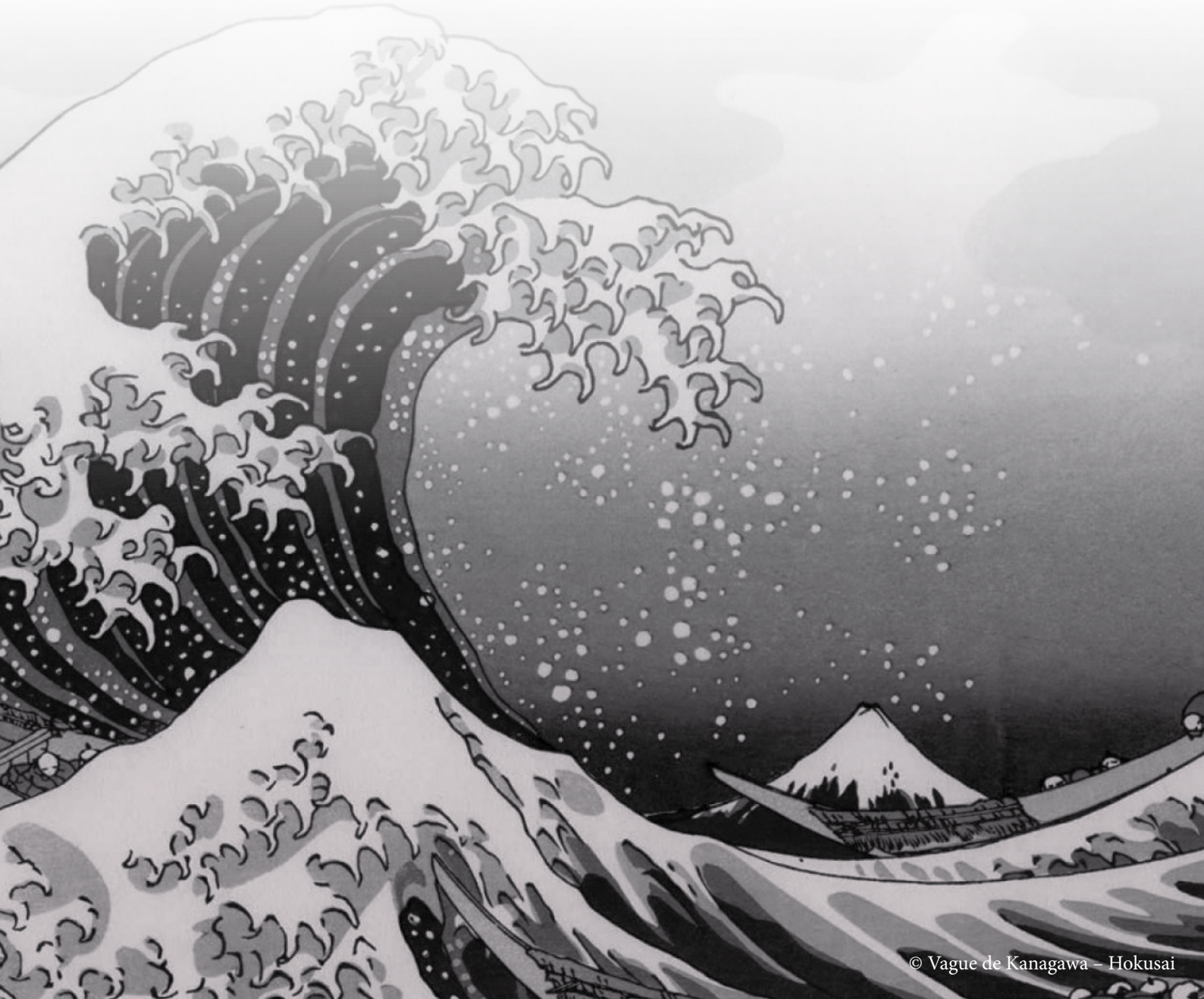
Editions Pierre Guillaume De Roux, 2015

«Qu'est-ce que l'Europe aujourd'hui ? Sinon le moyen de l'intérêt national américain. Gouvernance, création de valeur actionnariale, compétitivité et attractivité des territoires... Quatre expressions d'une idéologie, celle de la primauté de l'économie comme moyen de la puissance. Sans oublier le copié-collé d'une « culture » d'importation américaine : toute puissance de la com', adoption du mariage pour tous, bientôt peut-être de la procréation médicalement assistée, dogme de l'indifférenciation des sexes, tiré de la théorie du genre qui fit fureur aux Etats-Unis voici vingt ans ; dévaluation de l'appartenance nationale, et déchéance d'un projet national fédérateur et identifiant, etc. Faire Europe oui mais à condition de rompre avec l'erreur de l'occidentalisme qui la dresse contre ses voisins et alliés naturels, de la Russie aux pays du sud, ceux sans qui elle ne se fera pas l'Europe ne participera à une renaissance de la civilisation qu'en affirmant la séparation nécessaire entre les cultures et les Nations, qui garantit leur diversité. Le rêve totalitaire d'un gouvernement mondial est la promesse de l'esclavage, et la négation du droit des peuples à disposer d'eux-mêmes. Pour en finir avec cette utopie qui a fait tant de mal, l'Europe doit réaffirmer l'importance politique de frontières internationalement reconnues, de la citoyenneté comme appartenance nationale exclusive de tout marché, et le principe de non-ingérence dans les affaires intérieures des Etats.»

EXPLORER - *Dossier bibliographique*

- HEISBOURG, François. *Comment perdre la guerre contre le terrorisme*. Stock, coll. « Essais - Documents », 2016, 128 p.
- MOREAS, Georges. *Dans les coulisses de la lutte antiterroriste : De la rue des rosiers à l'état d'urgence*. First Editions, coll. « First Document », 2016, 280 p.
- HANNE, Olivier, POUCHOL, Thierry. *Islam et radicalisation dans le monde du travail*. Bernard Giovanangeli Editeur, 2016, 144 p.
- RAFLIK, Jenny. *Terrorisme et mondialisation*. Gallimard, coll. « Bibliothèque des Sciences humaines », 2016, 416 p.

TEMPS FORTS



© Vague de Kanagawa – Hokusai

Ouverture du 7e cycle de spécialisation « Sécurité des usages numériques »

en partenariat avec le CIGREF

21 novembre 2016 – École militaire - PARIS

L'information est désormais au cœur des actifs immatériels de l'entreprise et constitue un élément clé de sa performance. L'évolution de l'Internet a par ailleurs conféré aux systèmes d'information une dimension incontournable du développement de l'économie. La sécurité numérique représente donc un enjeu majeur pour la pérennité et la compétitivité des entreprises.

Pour cela, le département Intelligence et sécurité économiques supervise, en partenariat avec le CIGREF, le Club informatique des grandes entreprises françaises, le cycle de spécialisation «*Sécurité des usages numériques*», afin de délivrer les savoir-faire visant l'identification, l'évaluation et la maîtrise de l'ensemble des risques et des malveillances à tous ceux qui veulent mieux comprendre les enjeux de la Sécurité Numérique au sein des entreprises.

Le 21 novembre 2016, les auditeurs de la 7e promotion de ce cycle annuel de spécialisation ont été chaleureusement accueillis par Frédéric DESAUNETTES, directeur adjoint de l'Institut, Jean-Claude LAROCHE, administrateur du CIGREF et directeur des Systèmes d'Information chez EDF ainsi que Jean-François PEPIN, délégué général du CIGREF. ■

Colloque des conférenciers en sécurité économique

4 octobre 2016 - École militaire - PARIS

Dans l'esprit de diffusion de la culture d'intelligence et de sécurité économiques, nous avons mis en place en 2011 en partenariat avec la Délégation interministérielle à l'Intelligence économique, aujourd'hui le Service de l'information stratégique et de la sécurité économiques mais également en concertation avec les services spécialisés de l'État, une session de formation, baptisée EUCLES, visant à former des conférenciers labellisés, essentiellement issus du secteur privé, qui soient capables de délivrer un message général et uniformisé sur la sécurité économique dans le but de démultiplier les actions de sensibilisation des services de l'État qui ne peuvent pas répondre à toutes les sollicitations des entreprises. Et pour animer ce réseau de labellisés sur l'ensemble du territoire, nous avons créé, il y a un an maintenant, une plate-forme collaborative afin de permettre à ces conférenciers d'accéder à de l'information mais également d'échanger entre eux. À terme, cette plate-forme pourrait être ouverte aux services de l'État en charge de ces problématiques d'IE et de sensibilisation des entreprises aux enjeux de sécurité économique, ce qui créerait une véritable synergie public/privé entre ces différents acteurs et permettrait aux uns et aux autres de mieux se connaître et de partager information et bonnes pratiques.

En réunissant les labellisés conférenciers en sécurité économique lors de cette journée, le Directeur de l'INHESJ, le Préfet Cyrille SCHOTT et le Commissaire à l'information stratégique et la sécurité économiques, Jean-Baptiste CARPENTIER, ont souhaité manifester leur volonté commune de redynamiser le dispositif EUCLES pour en faire un véritable exemple de synergie public/privé dynamique et efficace au service de nos entreprises.

Ce colloque a été également l'occasion pour Jean-Baptiste CARPENTIER d'annoncer la naissance des délégués à l'information stratégique et la sécurité économiques (DISSE), qui remplaceront les Chargés de mission régionaux à l'intelligence économique (CRIE), en fonction dans les DIRECCTE, et qui constitueront de véritables relais du dispositif au sein des territoires, puisqu'ils forment le nouveau réseau territorial du Service de l'information stratégique et de la sécurité économiques (SISSE), créé en janvier 2016.

La nouvelle lettre de mission des DISSE représente la déclinaison au niveau territorial de la feuille de route du Commissaire à l'Information Stratégique et à la Sécurité Économiques (CISSE). Elle met notamment en avant des actions phares attendues dans le domaine de la veille sur les entreprises stratégiques et le traitement de dossiers d'investissements étrangers en France. ■

Ouverture des sessions nationales

27-30 septembre 2016 - École militaire - PARIS

De gauche à droite :
Jean-Yves LE DRIAN, ministre de la Défense
et **Cyrille SCHOTT**, directeur de l'INHESJ.

La fin du mois de septembre 2016 a été marquée par l'ouverture des trois sessions nationales de l'INHESJ, «*Sécurité et Justice*», «*Protection des entreprises et Intelligence économique*» et «*Management stratégique de la crise*».

À cette occasion, au-delà des présentations de l'Institut et de chacune des sessions, les auditeurs ont pu entendre les différents directeurs généraux de la Gendarmerie nationale, de la Police nationale et de la sécurité civile et de la gestion de crise. Le commissaire à l'information stratégique et à la sécurité économiques, Jean-Baptiste CARPENTIER et le Préfet Christian CHOCQUET, conseiller du gouvernement, haut fonctionnaire de défense adjoint et chef du service du haut fonctionnaire de défense au secrétariat général du ministère de l'Intérieur, qui anime le dispositif territorial d'intelligence économique, sont également intervenus lors de ces journées de rentrée. Ces dernières se sont clôturées par l'ouverture commune des sessions nationales de l'INHESJ et de l'IHEDN par le ministre de la Défense, Jean-Yves LE DRIAN. ■

Les Référents Intelligence Économique de la Gendarmerie nationale

16 septembre 2016 - Ecole militaire - Paris

Dernière promotion des ***Référents IE de la Gendarmerie nationale*** lors de la cérémonie de clôture du cycle le 16 septembre 2016, au centre, le **Général Jacques VIRE**, adjoint au directeur des opérations et de l'emploi (DGGN), monsieur le Préfet et directeur de l'INHESJ **Cyrille SCHOTT** et madame **Angélique LAFONT**, chef du département Intelligence et sécurité économiques.

Le département Intelligence et sécurité économiques a reçu la 11e session des *Référents Intelligence Économique de la Gendarmerie nationale.* Créé en 2005, ce cycle d'expertise de 70 heures axé sur la sécurité économique permet aux officiers de mieux appréhender la matière de l'Intelligence Économique, développer leurs connaissances et de recevoir des outils méthodologiques et opérationnels qu'ils pourront mettre à profit auprès des entreprises et plus particulièrement des PME/TPE. Cette formation, qui s'est clôturée vendredi 16 septembre dernier par la remise des diplômes et un cocktail a été l'occasion pour le Préfet Cyrille SCHOTT, directeur de l'Institut, en présence du Général de Brigade Jacques VIRE, adjoint au directeur des opérations et de l'emploi (DGGN), de réaffirmer les liens étroits unissant les deux structures depuis de nombreuses années.

Clôture du 6e cycle de spécialisation « Sécurité des usages numériques »

en partenariat avec le CIGREF

14 juin 2016 - École militaire - PARIS

Le Préfet **Cyrille SCHOTT**, directeur de l'INHESJ, **Jean-Claude LAROCHE**, membre du conseil d'administration du CIGREF et directeur des Systèmes d'Information du groupe EDF, **Jean-François PÉPIN**, délégué général du CIGREF, **Angélique LAFONT**, chef du département Intelligence et sécurité économiques et **Nicolas ARPAGIAN**, directeur scientifique de la formation, accompagnés de la 6e promotion du cycle « *Sécurité des usages numériques* ».

Chaque année depuis 2010, le département Intelligence et sécurité économiques supervise, en partenariat avec le CIGREF, le cycle de spécialisation «*Sécurité des usages numériques*» dans lequel une vingtaine d'auditeurs, issus de la sphère publique et du secteur privé, sont formés aux enjeux majeurs de la sécurité numérique au sein des entreprises. Au cours de cette formation, les auditeurs sont amenés à réaliser un travail de groupe à la suite duquel ils produisent un rapport en fin d'année.

Le cycle de la 6e promotion, constituée d'une vingtaine d'auditeurs, s'est clôturé par une cérémonie de remise de certificats en présence du Préfet Cyrille SCHOTT, directeur de l'INHESJ, de Jean-Claude LAROCHE, membre du conseil d'administration du CIGREF et directeur des Systèmes d'Information du groupe EDF, de Jean-François PÉPIN, délégué général du CIGREF, d'Angélique LAFONT, chef du département Intelligence et sécurité économiques et de Nicolas ARPAGIAN, directeur scientifique de la formation. Lors de son discours, le directeur de l'Institut a tenu à réaffirmer l'importance du partenariat unissant les trois acteurs du monde numérique tout en soulignant l'engagement de l'INHESJ dans la formation en matière de lutte contre la cyber criminalité. ■

Séminaire de clôture des sessions nationales

9 juin 2016 - École militaire - PARIS

Au centre, **Jacques BUISSON**, président du conseil d'administration, **Cyrille SCHOTT**, directeur de l'INHESJ et **Angélique LAFONT**, chef du département Intelligence et sécurité économiques, accompagnés de la 19e session nationale spécialisée « Protection des entreprises et Intelligence économique ».

La cérémonie de remise des diplômes et des insignes des trois sessions nationales a eu lieu le 9 juin 2016. Elle a été suivie des traditionnelles photos de fin d'année puis d'une soirée festive organisée par le département formation. ■

Séminaire de clôture des sessions nationales

9 juin 2016 - École militaire - PARIS

Au centre, **Jacques BUISSON**, président du conseil d'administration, **Cyrille SCHOTT**, directeur de l'INHESJ et **Marc BARBIER**, chef du département formation accompagnés de la 27e session nationale « *Sécurité et Justice* ».

Au centre, **Carole DAUTUN**, chef du département Risques et crises et **Cyrille SCHOTT**, directeur de l'INHESJ et **Jacques BUISSON**, président du conseil d'administration, accompagnés de la 3e session nationale spécialisée « *Management stratégique de la crise* ».

7e cycle d'expertise « Security Manager »

21 au 23 mars et 30 mai au 1er juin 2016 - École militaire - PARIS

Le département Intelligence et sécurité économiques de l'INHESJ a reçu 20 auditeurs dans le cadre de son *7e cycle d'expertise «Security manager»* en partenariat avec le Club des Directeurs de Sécurité des Entreprises. Ce cycle a pour objectif l'acquisition de connaissances et méthodes complémentaires en termes de construction d'une politique de sûreté/sécurité pour les cadres intermédiaires d'une direction sûreté-sécurité. Depuis 2009, l'INHESJ et le CDSE s'engagent ensemble à mieux répondre aux attentes des entreprises dans le domaine de la sécurité économique.

Le cycle s'est clôturé par une cérémonie de remise de certificats en présence de monsieur Alain JUILLET, président du CDSE et de monsieur le Préfet Cyrille SCHOTT. Lors de son discours, monsieur le Préfet a tenu à réaffirmer l'importance des liens unissant les deux structures depuis de nombreuses années. ■

Au centre, **Alain JUILLET**, président du CDSE, le **Préfet Cyrille SCHOTT**, directeur de l'INHESJ et **Angélique LAFONT**, chef du département Intelligence et sécurité économiques, accompagnés des auditeurs du 7e cycle d'expertise « Security manager »

Sessions nationales spécialisées

9 au 13 mai 2016 - Madrid - Espagne

Réception des auditeurs à la résidence de France à Madrid.

Au cours du voyage d'étude organisé à Madrid, les auditeurs des deux sessions nationales spécialisées « Protection des entreprises et Intelligence économique » et « Management stratégique de la crise » ont pu bénéficier de conférences et visites leur permettant d'avoir un riche aperçu de la manière dont les autorités espagnoles peuvent traiter les questions d'intelligence économique et de gestion de crise. ■

De gauche à droite : **Jean-François COLLIN**, ministre conseiller en charge des affaires économiques, **Isaac Martin BARBERO**, directeur général du développement international, fait une intervention à l'ICEX, *España Exportación e Inversiones*, organisme public qui promeut l'exportation des entreprises espagnoles et le **Préfet Cyrille SCHOTT**, directeur de l'INHESJ.

Séminaire commun des sessions nationales « Protection des entreprises et intelligence économique » et « Management stratégique de la crise »

9 au 12 février 2016 - Bruxelles - Belgique

Le département Intelligence et sécurité économiques et le département Risques et crises ont organisé un séminaire commun pour les auditeurs de leurs sessions nationales spécialisées respectives. Ce séminaire fût l'occasion de favoriser les échanges constructifs entre auditeurs de promotions différentes et d'appréhender le rôle des institutions européennes dans divers domaines majeurs pour la pérennité et le développement de nos entreprises. Les auditeurs furent accueillis à la Représentation permanente de la France à Bruxelles ainsi qu'à la Commission européenne où ils ont notamment pu visiter le centre de gestion de crise. ■

Le 15 décembre 2016

Colloque annuel du CDSE, L'entreprise face aux phénomènes de radicalisation De l'incivilité à l'ultraviolence

OCDE, Paris

Programme et inscription :
https://www.cdse.fr/colloque-annuel-2016-du-cdse

Du 1er mars au 4 mai 2017

Inscriptions ouvertes

Cycle d'expertise Security manager

INHESJ, Ecole militaire

Programme et inscription :
https://www.inhesj.fr/sites/default/files/fichiers_site/formation/Intelligence_et_securite_economiques/presentation_sm_2017.pdf

Du 20 novembre 2017 au 5 juin 2018

Inscriptions ouvertes

Cycle de spécialisation Sécurité des usages numériques

INHESJ, École militaire

Programme et inscription :
https://www.inhesj.fr/fr/departements/securite-economique/specialisation

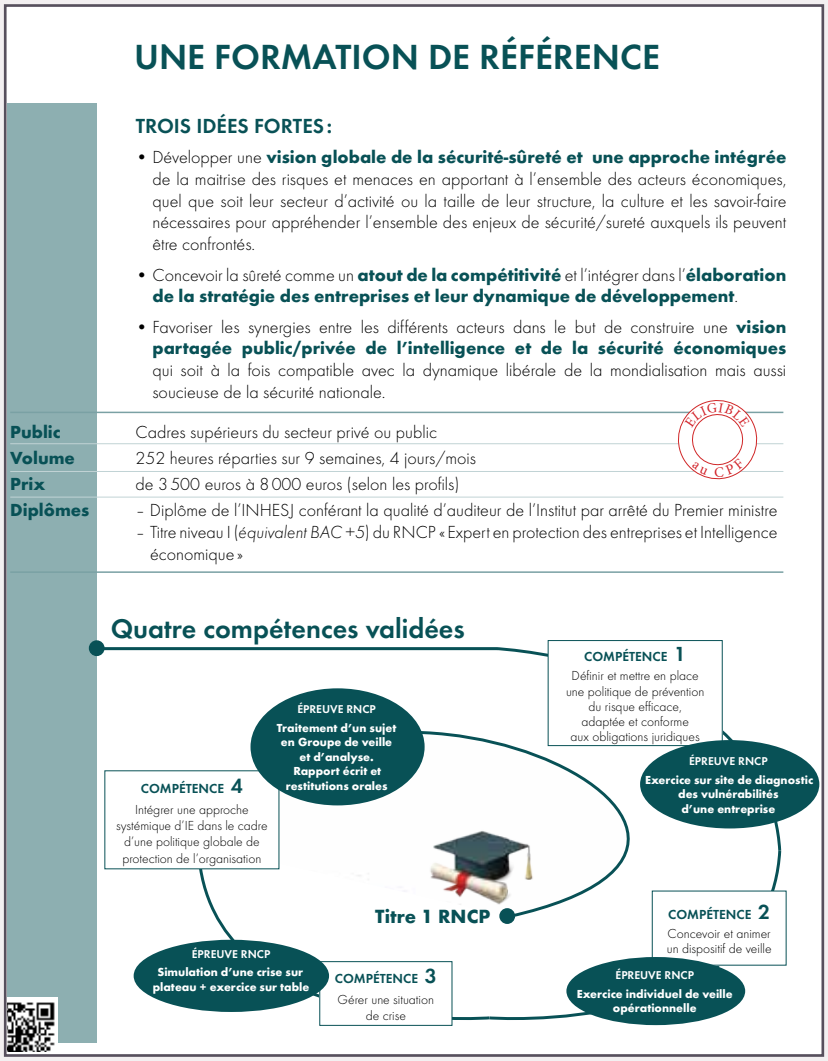
Du 26 septembre 2017 au 14 juin 2018

Inscriptions ouvertes

Session nationale spécialisée (SNS) « Protection des entreprises et intelligence économique »

INHESJ, Ecole militaire

Programme et inscription :
https://www.inhesj.fr/fr/departements/securite-economique/session_national_spe



Défis

Déjà parus

L'Intelligence stratégique au service de la compétitivité

- **n°6 :** CRIME ENVIRONNEMENTAL : enjeux de sécurité pour les organisations
- **n°5 :** CRIME PHARMACEUTIQUE : une épidémie silencieuse
- **n°4 :** MONDIALISATION ET RICHESSES DES NATIONS Le patriotisme économique : avenir du libéralisme ?
- **n°3 :** LE SECRET DES AFFAIRES : vers une concurrence loyale
- **n°2 :** BUSINESS EN MILIEU HOSTILE: la protection des entreprises à l'internationale
- **n°1 :** LA CYBERSÉCURITÉ

Défis Abonnez-vous à cette adresse

www.inhesj.fr

JE M'ABONNE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

INHESJ

Département Intelligence et sécurité économiques