

# CAHIERS DE LA SÉCURITÉ ET DE LA JUSTICE

Revue de l'Institut national des hautes études de la sécurité et de la justice \_\_\_\_\_ n°34

## Protéger les entreprises *La sécurité économique*

### Le dossier

Les entreprises et la cybercriminalité  
Noémie NATHAN

Les atteintes à la réputation  
Christian HARBULOT, Augustin ROCH

La machine de guerre économique américaine  
Ali LAÏDI

### Sécurité intérieure

L'apport de la psychologie et de la psychiatrie  
dans la connaissance des phénomènes de  
radicalisation et de terrorisme  
Michel BÉNÉZECH, Nicolas ESTANO

Directeur de la publication :  
**Cyrille SCHOTT**

Rédacteur en chef :  
**Manuel PALACIO**

Comité de rédaction :

**AMADIEU Jean-Baptiste**, Agrégé de lettres, chargé de recherches au CNRS

**BERLIÈRE Jean-Marc**, Professeur émérite d'histoire contemporaine,  
Université de Bourgogne

**BERTHELET Pierre**, Chercheur au centre de documentation et de recherches  
européennes (CRDE), Université de Pau

**BONY Lucie**, Géographe, Centre de recherche sur l'habitat, CNRS

**COOLS Marc**, Professeur en criminologie, Université libre de Bruxelles,  
Université de Gand

**DE BEAUFORT Vivianne**, Professeur à l'Essec, co-directeur du CEDE

**DE MAILLARD Jacques**, Professeur de Science politique, Université de  
Versailles Saint-Quentin

**DIAZ Charles**, Contrôleur Général, Inspection Générale de la Police Nationale

**DIEU François**, Professeur de sociologie, Université Toulouse 1 Capitale

**EVANS Martine**, Professeur de droit pénal et de criminologie, Université de Reims

**HERNU Patrice**, Administrateur INSEE

**LATOUR Xavier**, Professeur de droit, Université de Nice

**LOUBET DEL BAYLE Jean-Louis**, Professeur émérite de Science politique,  
Université de Toulouse I, Capitole

**NAZAT Dominique**, Docteur en Sciences odontologiques, expert au Groupe  
de travail permanent pour la révision des normes d'identification du DVI  
d'INTERPOL

**PARDINI Gérard**, Chef du service des affaires immobilières de la Prefecture  
de police de Paris

**PICARD Jean-Marc**, Enseignant-chercheur à l'Université de Technologie de  
Compiègne

**RENAUDIE Olivier**, Professeur de droit public à l'Université de Lorraine, Nancy

**REVEL Claude**, Conseillère maître en service extraordinaire à la Cour des comptes

**RIDEL Laurent**, Directeur interrégional de l'Administration pénitentiaire

**DE LA ROBERTIE Catherine**, Recteur Professeur des universités, Paris I,

Directrice du Master2 Gestion et méthodes de décision d'entreprise

**ROCHE Jean-Jacques**, Directeur de la formation, des études et de la

recherche de l'Institut des hautes études de la défense nationale (IHEDN)

**SAURON Jean-Luc**, Professeur de droit à l'Université Paris Dauphine

**TEYSSIER Arnaud**, Inspecteur Général de l'Administration, Professeur Associé  
à l'Université Paris I

**VALLAR Christian**, Doyen de la Faculté de droit, Nice Sophia Antipolis

**VELTCHEFF Caroline**, Agrégée de Lettres, inspectrice d'académie

**WARUSFEL Bertrand**, Professeur agrégé des facultés de droit, Université Lille 2

Responsable de la communication : Axelle de FONTGALLAND

Conception graphique et fabrication : Laetitia BÉGOT, Marine OSTAPOWICZ,  
Daniel VIZET

© Direction de l'information légale et administrative, Paris, 2015

Conditions de publication : Les Cahiers de la sécurité publient des articles, des comptes rendus de colloques ou de séminaires et des notes bibliographiques relatifs aux différents aspects nationaux et comparés de la sécurité et de ses acteurs. Les offres de contribution sont à proposer à la rédaction pour évaluation. Les manuscrits soumis ne sont pas retournés à leurs auteurs.

Toute correspondance est à adresser à l'INHESJ à la rédaction de la revue.

Tél. : +33 (0)1 76 64 89 00 - Fax : +33 (0)1 76 64 89 31

publications@inhesj.fr - www.cahiersdelasecuriteetdelajustice.fr

## Sommaire

3 Editorial - Cyrille SCHOTT

### Dossier

Dossier coordonné par Xavier LATOUR et Catherine DE LA ROBERTIE

- 5 L'entreprise et la sécurité  
Catherine DE LA ROBERTIE, Xavier LATOUR
- 7 L'entreprise, une cible permanente - Alain BAUER
- 10 L'intelligence économique, enjeu de sûreté - Alain JUILLET
- 16 La « radicalisation » dans l'entreprise  
Mustapha BENCHENANE
- 22 Les entreprises à l'épreuve de la cybercriminalité  
Noémie NATHAN
- 29 Les atteintes à la réputation - Christian HARBULOT,  
Augustin ROCH, Artus HUOT De SAINT ALBIN
- 36 Le patriotisme économique - Bernard CARAYON
- 41 L'entreprise, coproductrice de la sécurité - Bertrand PAUVERT
- 48 L'entreprise collaboratrice du service public de la sécurité :  
l'exemple des aéroports - Florence NICOUUD
- 56 Les entreprises et la sûreté... Entre rêve et réalités  
Jean-Philippe BÉRILLON
- 61 L'entreprise au cœur de la coproduction de sécurité -  
quels enjeux, quels leviers ? - Thierry COUDERT
- 68 Construire un nouveau contrat de confiance public-privé en  
matière de sécurité - Groupe de veille et d'analyse Richelieu.  
18<sup>e</sup> session nationale spécialisée « Protection des entreprises  
et Intelligence économique » des auditeurs de l'INHESJ





**79** La souveraineté économique de la nation.  
Une question centrale  
Entretien avec Jean-Baptiste CARPENTIER

**83** La mission intelligence économique de la gendarmerie nationale au prisme des entreprises  
Catherine de LA ROBERTIE, Norbert LEBRUMENT, Stéphane MORTIER

**93** Douanes et protection de l'entreprise  
Bruno DOMINGO

**104** Les services de sécurité privée en Europe : faits et chiffres – Marc COOLS, Harald OLSCHOK, Veerle PASHLEY et Dany VANDORMAEL

**117** La machine de guerre économique américaine – Ali LAÏDI

**127** Une sécurité sans frontières pour les entreprises  
Philippe CHAPLEAU

**130** La consolidation du droit applicable aux activités d'importance vitale – Xavier LATOUR

**138** Entre guerre et affaires. *Pourquoi les doctrines militaires inspirent souvent le monde des affaires* – Jelle JANSSENS, Veerle PASHLEY, Marc COOLS



## International

**151** Les néo-fondamentalistes, version EIIL – Hamza SHAREEF HASAN

**156** Salafisme (s) et violence. La construction historique d'une axiomatique de la violence.  
*Des frères musulmans à Al-Qaida : d'une conception utilitaire de la violence à une vision organique ?* – Mohamed-Ali ADRAOU

## Sécurité intérieure

**162** L'apport de la psychologie et de la psychiatrie dans la connaissance des phénomènes de radicalisation et de terrorisme  
Michel BÉNÉZECH, Nicolas ESTANO





## Éditorial

La réflexion relative à la sécurité se décline, à travers différents champs disciplinaires, sur de multiples objets. Parmi ces derniers, l'entreprise constitue un sujet d'importance stratégique, tant les menaces et les attaques qui la visent mettent en jeu les équilibres fondamentaux de l'économie et de la société. C'est pourquoi les questions touchant à la sécurité des entreprises ont été intégrées dans les missions de formation et de recherche de l'institut, lorsque celui-ci a élargi son domaine d'action par la prise en compte de la notion de sécurité globale. C'est en 2010 que l'Institut crée un département spécifiquement dédié à la sécurité des entreprises. Il le fait, en intégrant en son sein l'Institut d'étude et de recherche pour la sécurité des entreprises (IERSE), dont la mission était de répondre de manière adaptée, notamment par le biais de la formation, aux nouvelles problématiques de sécurité/sûreté se posant aux entreprises. L'actuel département *Intelligence et sécurité économiques* de l'INHESJ s'inscrit dans le droit fil de cette histoire et poursuit l'objectif de construire les nécessaires synergies public-privé au service de la protection et de la compétitivité des entreprises.

Ce vaste champ de réflexion et d'action comprend deux domaines particuliers qui sont, d'une part, la sécurité privée et, d'autre part, la protection de l'entreprise et de ses intérêts fondamentaux. Ce dernier domaine est plus spécialement exploré dans

le dossier de ce numéro des *Cahiers de la sécurité et de la justice*. Il constitue l'un des axes stratégiques de l'activité du département *Intelligence et sécurité économiques*. Ce travail s'inscrit dans une logique de contribution à la politique publique de sécurité et d'intelligence économiques, en s'efforçant d'enrichir la culture nécessaire à l'ensemble des acteurs, quels que soient leur secteur d'activité ou la taille de leur structure, pour appréhender les nouveaux enjeux et protéger leur patrimoine et leur capital immatériel. Cet objectif est poursuivi principalement à travers une activité de formation à multiples étages, dont la base est constituée par la session nationale spécialisée *Protection des entreprises et Intelligence économique*, au bénéfice d'auditeurs venus du monde de l'entreprise et concernés, dans les responsabilités qu'ils assument, par les questions de sécurité. Cette session a pour ambition de délivrer aux auditeurs les clés de compréhension indispensables à une analyse pertinente des situations à risques, d'origine interne ou externe à l'entreprise, mais également de leur transmettre les savoir-faire, aussi bien théoriques qu'opérationnels, nécessaires à la mise en place efficace de dispositifs de prévention et de protection. Pour ce faire, les auditeurs sont amenés à développer la vision la plus exhaustive possible des enjeux de la sécurité/sûreté, par le biais d'un programme de formation qui articule entre elles plusieurs thématiques fondamentales, telles la veille, la mise en place d'un dispositif de protection globale, la cybersécurité,

la protection des entreprises à l'international, ou encore les stratégies d'influence et le management de crise.

Ce numéro revient sur ces thématiques pour en actualiser l'analyse et apporter des éclairages nouveaux fournis, conformément à l'esprit de la revue, par des experts du monde universitaire et des responsables institutionnels, privés et publics. Il cible plus particulièrement les menaces que les évolutions des sociétés modernes font peser sur les entreprises et les stratégies de prévention et de riposte que les différentes entités responsables, au sein de l'État et de la sphère économique au sens large, mettent en place. Comme le rappellent les professeurs Xavier Latour et Catherine de La Robertie, dans leur introduction à ce dossier qu'ils ont coordonné, face

à ces nouvelles formes de menaces et d'agressions, *« toutes les composantes de la société tentent de produire des anticorps. L'entreprise se protège en adoptant une posture d'anticipation. Cela impacte son organisation et, plus largement, les choix opérés par la puissance publique. L'État et l'entreprise sont liés par les enjeux de sécurité ».*

Les travaux qui sont présentés dans ce numéro consacré aux entreprises s'inscrivent, au même titre que l'activité de formation et de recherche spécifique menée au sein de l'Institut, dans l'ambition et la nécessité de diffuser la culture d'intelligence et de sécurité économiques, diffusion qui représente un enjeu majeur pour l'avenir de notre pays et de son économie.

Cyrille SCHOTT,  
*Préfet, directeur de l'INHESJ*

# L'entreprise et la sécurité

Catherine DE LA ROBERTIE, Xavier LATOUR

Les sociétés sont des ensembles complexes. Elles mettent en relation des individus et des entités abstraites. Ces dernières, personnes morales de droit public ou de droit privé ont beau être des fictions juridiques, elles n'en ont pas moins une réalité économique et sociale. Parmi elles, les entreprises, quelle que soit leur taille, ont un rôle essentiel.

Lieu de création de richesses, d'activités professionnelles, de vie pour celles et ceux qui y travaillent, les entreprises vivent au rythme des enjeux de société. Elles insufflent espoir ou inquiétude au tissu social, elles subissent les crises, connaissent des cycles d'optimisme ou de pessimisme. Parce que les entreprises vivent, elles sont sensibles aux mêmes doutes que les individus qui les composent.

En matière de sécurité, l'entreprise est une cible comme les autres, d'autant plus exposée qu'elle est insérée dans un ensemble d'interdépendances nationales et internationales. Comme les individus, elle est confrontée à des menaces de plus en plus variées.

De l'intérieur ou de l'extérieur, celles-ci prennent la forme de vols, de chantages, de kidnapping de données. Dans notre monde, le déploiement depuis une vingtaine d'années des technologies sans cesse plus performantes

de l'information et de la communication a modifié la perception du concept d'espace-temps et provoqué un déplacement de référent. Tout un chacun devient potentiellement producteur d'information, où l'information est devenue matière stratégique et un enjeu de compétitivité. Les entreprises, grandes ou petites, sont les cibles de menaces protéiformes, telles que l'espionnage économique et les phénomènes de cyber-criminalité, ou bien encore les actions d'influence, de désinformation, d'atteinte à la réputation. Par leur fragilité potentielle, les femmes et les hommes qui les composent sont également vecteurs ou cibles, comme en témoigne le développement de comportements radicaux sur les lieux de travail. L'activité des entreprises est conséquemment également concernée par divers risques, technologiques, environnementaux, ou encore humains.

Dès lors, l'entreprise est pleinement un objet de la sécurité globale, et la sûreté dans sa globalité une priorité stratégique.

Dans ce contexte, toutes les composantes de la société tentent de produire des anticorps. L'entreprise se protège en adoptant une posture d'anticipation. Cela impacte son organisation et, plus largement, les choix opérés par la puissance publique. L'État et l'entreprise sont liés par les enjeux de sécurité.

En effet, le monde économique a besoin d'un cadre conceptuel et juridique clair ainsi que, parfois, de l'appui matériel de l'État pour se protéger. La politique publique d'intelligence économique mise en place est une des réponses à cette attente, les missions de la gendarmerie y contribuent, en particulier au niveau des territoires.

À ce titre, la France a tout à gagner à tourner son regard vers l'étranger. La mondialisation est une réalité qui l'oblige à appréhender ce que font ses partenaires, ses concurrents (ce sont parfois les mêmes), et, en tout état de cause, ses ennemis.

Il ne peut y avoir de sécurité de l'entreprise dans un cadre exclusivement national. L'Europe et le monde font intégralement partie du paysage quotidien.

Néanmoins, la prévention n'étant pas infaillible, la sécurité de l'entreprise peut être prise en défaut. Dans la crise, elle doit alors réagir pour préserver son patrimoine, humain, matériel et immatériel, tout en inscrivant sa capacité de résilience dans un environnement de solidarité collective.

C'est tout l'enjeu du plan de continuité de l'activité. En la matière aussi, l'entreprise n'est pas isolée, ni sur le

territoire national, ni à l'égard de l'extérieur. L'intégration européenne impacte ses obligations et son organisation. La crise est une notion commune aux États membres de l'Union européenne, surtout lorsqu'il s'agit de faire fonctionner des activités sensibles, voire vitales.

De même une approche communautaire du concept de patriotisme économique pourrait contribuer à mettre en œuvre une politique de puissance, constituant une condition de l'indépendance et de la cohésion sociale.

Ce numéro a pour ambition de cerner ces différents phénomènes. Sans prétendre à une exhaustivité scientifique inatteignable, il s'inscrit pleinement dans la logique des *Cahiers de la sécurité et de la justice* en cherchant à éclairer et à faire réfléchir grâce à des analyses transdisciplinaires élaborées à la fois par des chercheurs et des praticiens.

Nous vous en souhaitons une bonne lecture ■

# L'entreprise, une cible permanente

Alain BAUER



## Alain BAUER



Professeur titulaire de la chaire de criminologie du Conservatoire national des arts et métiers (depuis 2009), directeur du Master de

sciences criminelles et criminologie, directeur scientifique et vice-président du Conseil scientifique du pôle sécurité défense du CNAM, Alain Bauer est professeur titulaire de la chaire de sciences policières et criminelles du MBA spécialisé Management de la sécurité (Paris II, HEC, EOGN). Senior Research Fellow au Center of Terrorism du John Jay College of Criminal Justice à New York (États-Unis), à l'Académie de police criminelle de Chine et à l'université de Droit de Beijing, il est également éditeur de l'International Journal on Criminology et membre du Conseil éditorial de PRISM (NDU).

L'entreprise a toujours constitué une cible. Militaire, d'abord, pour détruire ses moyens de production. Économique, ensuite, afin de la voler, la piller ou la rançonner. Ce n'est que plus récemment, à savoir depuis les attentats du 11 septembre 2001, qu'elle est également devenue vulnérable pour ses dirigeants, ses agents clés (dans les avions ou sur les sites de direction), sa valeur boursière ou encore son image. Il ne s'agit alors pas d'attaques contre des usines mais bien sûr des cerveaux.

L'entreprise est entrée dans le monde moderne et virtuel du crime et du terrorisme (celui ne constituant guère qu'une filiale du précédent) en 2001. Désormais, on voit le crime, on lit le crime, on vit le crime dans sa quasi-

immédiateté. Internet, les réseaux sociaux, Twitter ont rétréci le temps et l'espace. Ce qui mettait quelques mois, quelques semaines, quelques jours, puis quelques heures à être connu du grand public, entre désormais partout et tout de suite dans la vie de tout un chacun. Cette rapidité a quelques qualités, mais également un rédhitoire défaut : la perte de cohérence de l'information par l'absence de toute mise en perspective, annihilant ainsi toute véritable connaissance. Une information, rarement vérifiée, et plusieurs démentis sont autant d'éléments qui nourrissent le flux à égalité. Chacun veut aller plus vite, plus fort et, surtout, assurer coûte que coûte un débit ininterrompu. Du coup, noyant les quelques experts appelés en renfort, souvent prudents et attendant de savoir avant de parler, apparaissent alors des commentateurs de commentaires, affirmant tout en pensant interroger, déclamant en pensant informer, noyant en pensant éclairer.

Si aucun domaine n'est épargné, les questions criminelles ou terroristes semblent les plus touchées en raison de leur côté spectaculaire et de l'appétence du monde médiatique pour l'événement qui permet l'édition spéciale. On a pu ainsi beaucoup s'étendre sur les origines et les mutations du crime organisé (« le dernier parrain » fait très souvent la « Une » avant d'être, fort vite, remplacé par son successeur), sur les évolutions du terrorisme (on a découvert beaucoup de « loups solitaires » même quand ils agissaient à plusieurs et avaient pris soin de faire quelques voyages de formation), ou sur tout événement criminel immédiatement classé comme exceptionnel ou sans précédent. Dans le même temps, sont négligées ou ignorées des évolutions majeures de ce qu'on appelle la « face noire de la mondialisation ». Il faut donc cheminer autour de divers sujets particulièrement importants.

Le crime, le terrorisme et l'entreprise vivent suivant des règles communes et se sont mondialisés ensemble. Ce phénomène, qui a commencé avec la première mondialisation industrielle à la fin du XIX<sup>e</sup> siècle, n'est plus seulement un sujet pour les grandes villes ou les États nationaux ; le vol d'identité, l'immigration illégale, le trafic de stupéfiants, les attaques terroristes, le trafic d'êtres humains et la criminalité financière se développent entre les continents et les hémisphères.

La génération précédant la Première Guerre mondiale fut la première à affronter le crime à l'échelle internationale. À la fin du XIX<sup>e</sup> siècle, gouvernements, observateurs et leaders d'opinion ont commencé à s'inquiéter d'une « réduction du monde » due aux avancées technologiques de l'époque et à leurs effets culturels, sociaux et économiques sur le comportement criminel. Ils ont alors constaté des changements alarmants sur la criminalité ordinaire et l'apparition de nouvelles formes de criminalité (anarchisme, esclavage blanc, criminalité des étrangers). Des nouveaux experts, qui se dénommaient « criminologues », utilisèrent le langage de la science pour tenter de se forger une vision planétaire du problème. Dans un remarquable petit ouvrage passé inaperçu, le professeur anglais Paul Knepper décrit l'émergence de la criminalité internationale dans la Grande-Bretagne impériale des années 1881-1914. Plus précisément, il explore comment la dimension internationale constitue le seul moyen pratique de comprendre le crime en Grande-Bretagne durant cette période et après. Il faut pour cela revisiter les évolutions en matière de transports, de communication et de relations commerciales débouchant sur un monde interconnecté. Dès cette époque, policiers, journalistes, romanciers et autres observateurs ont décrit la montée en puissance de criminels professionnels, escrocs internationaux utilisant les nouvelles technologies de l'époque contre leurs victimes. Mais cette internationalisation ne fut

pas seulement technologique, elle avait également une dimension impériale.

La recherche « coloniale » permet alors des comparaisons entre criminalité interne et perception d'une « classe criminelle globalisée ». Longtemps, on a vu le criminel comme un individu singulier, parfois épaulé par un petit groupe (une bande, un gang, un « posse »...) qui, au rythme d'une carrière plus ou moins spectaculaire, construisait une légende ou un mythe. Chefs de gangs, meurtriers en série ou de masse ont ainsi construit leur image au rythme du développement des moyens de communication.

Quel média, théâtre, opéra, film, série télévisée, roman pourrait survivre sans sa (ses) part (s) de faits divers ? Mais, loin du spectacle, les empires du crime contrôlent des régions entières et se sont invités au banquet de la géopolitique mondiale. Public, journalistes et, parfois, policiers étaient eux-mêmes fascinés par ces « beaux voyous » et quelques *road movies* plus ou moins romancés mais fondés sur des faits réels, condensés dans le temps et dans l'espace. Depuis la reconnaissance, un peu forcée, par J. Edgar Hoover de l'existence de la Mafia aux États-Unis, après le « raid d'Apalachin » fin 1957, le crime organisé est désormais reconnu comme tel. Mais pendant longtemps, il n'était identifié que par des chefs de file de familles ayant développé des « business models » marqués par des opérations criminelles classiques (racket, prostitution, trafics) largement sous-estimées. Depuis il a beaucoup progressé.

Non seulement la mondialisation criminelle n'a pas attendu celle des États, mais elle les a atteints au cœur. De plus, considérant la faiblesse de certains États, les cartels criminels ont décidé de recréer des territoires qui ne sont plus limités à quelques jungles difficiles d'accès, comme ce fut le cas des Forces armées révolutionnaires de Colombie (FARC) ou du Triangle d'or birman. Dans le même temps, de la « récession Yakuza » des années 1980, en passant à la même époque par les Savings and Loans (caisses d'épargne américaines), puis par le Mexique, la Russie ou la Thaïlande, une série de crises financières à dimension criminelle, plus ou moins prononcée, a ébranlé les principaux pays du monde durant les trente dernières années. Et cela sans que les régulateurs centraux n'y prêtent la moindre attention, alors même que le Fonds monétaire international (FMI) estime la masse d'« argent sale » entre 1 % et 5 % du produit intérieur brut (PIB) mondial. Le monde du crime est devenu un acteur financier de première importance. Et sa relation avec les entreprises le fait passer de voleur à investisseur avec une *maestria* de plus en plus développée. Et le nombre de banques condamnées à payer de fortes amendes pour avoir joué avec le crime organisé ne manque pas de surprendre par leur diversité.

Depuis l'apparition, après la chute du mur de Berlin en 1989, d'un terrorisme d'une nature différente des précédents (indépendant des grands empires, qui pouvaient permettre ou empêcher une action en tenant les camps d'entraînement, les faux papiers, l'argent, les armes et les explosifs), on s'interroge beaucoup sur la nature des terroristes implantés qui ont peu à peu remplacé les opérateurs importés. Les organisateurs de la tragédie du 11 septembre 2001 se sont, pour l'essentiel, appuyés sur des agents envoyés en Occident. Depuis, le nombre d'opérateurs nés en Occident ou y résidant depuis leur enfance, certains convertis, a fortement progressé. Si beaucoup d'entre eux continuent à voyager vers des pays disposant de prédicateurs qui les confortent dans leur volonté criminelle, d'autres, de plus en plus nombreux, sont connectés à travers leurs ordinateurs sans avoir besoin de se déplacer et donc avec de moindres chances d'être identifiés. La situation n'est certes pas nouvelle, mais la capacité d'amnésie des dispositifs de lutte semble sans limites et les services restent relativement imperméables aux évolutions précédant une tragédie, avant de se réadapter à marche forcée, passant ainsi de l'extrême déni à son extrême inverse.

Avec Khaled Khelkal en 1995, puis le Gang de Roubaix en 1996, Mohammed Merah en 2012, les attentats de janvier 2015, la France a connu la douloureuse expérience des hybrides, mi-gangsters, mi-terroristes, naviguant entre deux fichiers et échappant ainsi à l'attention des services incapables de faire la connexion et de dépasser les cloisonnements comme cela avait d'ailleurs été longuement rappelé dans l'étude de Mitch Silber que j'avais supervisée en 2006 pour le NYPD (police de New York) sur la Radicalisation en Occident et la menace intérieure.

Sur le « terrain cyber », encore en friche et dont l'essentiel relève de l'arnaque classique avec assistance de la victime, il ne se passe pas de jours sans une information signalant la réussite d'une opération de pénétration dans des serveurs sécurisés publics ou privés, le pillage de distributeurs de billets de banque, l'annonce d'une prise de contrôle de commandes de réseaux d'eau, d'électricité, de dispositifs

*Non seulement la mondialisation criminelle n'a pas attendu celle des États, mais elle les a atteints au cœur. De plus, considérant la faiblesse de certains États, les cartels criminels ont décidé de recréer des territoires qui ne sont plus limités à quelques jungles difficiles d'accès*

médicaux, ou même de surveillance... Mais l'essentiel, le cœur du réseau et sa partie cachée, est rarement évoqué et l'on feint à chaque fois de découvrir le problème, après Échelon, Carnivore, Prism, autant d'outils de plus en plus intrusifs et dont nul ne connaît l'efficacité réelle proclamée, notamment en matière de lutte contre le terrorisme. Si les annonces apocalyptiques des premières années de prise de conscience des mécanismes de *backing* n'ont guère rencontré d'écho, et si les effets réels des opérations de cyberfraude ont en général nécessité le soutien involontaire de nombreuses victimes intéressées à l'expansion de leur outil reproducteur, à leurs capacités nocturnes ou à l'aubaine de récupérer quelques millions de dollars volés par un illustre inconnu subitement décédé et dont la veuve réclame le

soutien par Internet, des évolutions plus récentes semblent montrer qu'un nouveau palier a été atteint. À la fois en termes d'expansion du nombre de comptes visés, notamment en falsifiant des courriels officiels, mais également en termes de moyens techniques utilisés, comme le « rançonniciel » masqué derrière la puissance publique (impôts ou douanes). Le blanchiment, notamment via l'utilisation de cartes prépayées, est également devenu un élément de préoccupation, principalement en raison des effets pervers de mesures de libéralisation de l'Union européenne.

L'entreprise, surtout en Europe, fait confiance à l'État pour la protéger. Avec retard, ce dernier prend peu à peu conscience de l'ampleur des risques générés par des systèmes ouverts inventés pour le commerce et non pour la sécurité. L'entreprise, qui investit, emploie, crée, cherche et vend, est une cible pour toutes ces raisons mêmes.

Voilà qui précisément méritait un cahier particulier ■

# L'intelligence économique, enjeu de sûreté

Alain JUILLET

périmètre beaucoup plus vaste et plus délicat à gérer qui devient un enjeu stratégique majeur pour l'entreprise dans sa globalité : la sûreté.

**D**ans le monde globalisé qui est devenu le nôtre, l'entreprise ne peut plus se contenter de produire et de vendre des articles de qualité. Au-delà des catastrophes naturelles, des accidents conjoncturels, des ruptures énergétiques, ou des problèmes de transport, elle est sans cesse sous la menace de contrefaçons plus ou moins assumées, de piratage d'informations utiles aux concurrents, ou de divulgations de secrets techniques ou stratégiques. Elle doit en permanence améliorer la compétitivité de ses produits et sa capacité d'innovation tout en se défendant contre des agressions multiples et diversifiées dont l'ampleur est directement liée à son positionnement et à son potentiel sur le segment qu'elle occupe.

Nous sommes passés de la sécurité classique à une problématique au

## L'intelligence économique

L'approche de l'intelligence économique du rapport d'Henri Martre se focalisait essentiellement sur la veille économique, d'un secteur ou d'une activité spécifique, et le renseignement sur des concurrents. Elle a considérablement évolué suite à trois bouleversements parallèles : l'arrivée de l'informatique puis l'entrée dans le cyberspace, la globalisation de l'économie et l'utilisation croissante de tous les moyens concurrentiels pour réussir, la déstabilisation des entreprises et de leur personnel ou dirigeants à des fins politico-idéologico-financières.

De ce fait il est vite apparu que la veille devait être permanente et couvrir un champ plus large en étant plus offensive pour être compétitive et efficace. Dans le

Alain JUILLET



Ancien Haut Responsable chargé de la sécurité économique, Président

du Forum international des Technologies de Sécurité (FITS) et du Club des Directeurs de Sécurité des Entreprises (CDSE).



même temps il est devenu évident qu'il fallait développer une politique de sécurité du patrimoine adaptée en séparant la sécurité classique des biens et des personnes et la cybersécurité orientée vers l'immatériel. Enfin, pour éviter de mauvaises surprises, il fallait mener une diplomatie d'influence pour identifier puis contrer les agressions contre l'image ou la crédibilité des groupes et de leurs dirigeants. Cette évolution a amené à l'utilisation de nouveaux outils qu'il a fallu apprendre à maîtriser et à sélectionner les opérateurs à travers leur expertise réelle.

## L'exigence d'informations

Nous sommes arrivés à un niveau où, dans tous les domaines, les entreprises nationales et internationales fonctionnent avec les mêmes ratios, les mêmes objectifs, et quasiment les mêmes moyens selon leur taille et leur type d'activités. Le véritable problème est donc de se créer un nouvel avantage concurrentiel offensif et défensif qui va permettre la rupture avec les autres compétiteurs. Ceci suppose de connaître parfaitement son marché, sa filière, et ses concurrents pour identifier les points forts et les points faibles, les menaces et les opportunités. En apportant la capacité de compréhension et d'anticipation,

le renseignement devient la clé du succès et prend toute son importance stratégique.

Cependant, dans le même temps, les concurrents les plus efficaces utilisent les mêmes méthodes pour avoir l'information sur nous dont ils ont besoin. Pour se créer un déséquilibre favorable il faut donc acquérir parallèlement à la capacité offensive une capacité plus défensive pour bloquer les recherches d'un adversaire qui a rarement le même souci de la légalité. Ceci suppose l'identification et la hiérarchisation de ce qui est réellement essentiel à la vie de l'entreprise, la mise en place de procédures protégeant spécifiquement les secrets essentiels de l'entreprise, et la sensibilisation du personnel qui doit comprendre l'impact d'une fuite sur la pérennité et l'emploi futur.

## Le combat concurrentiel

Face à cette évolution et pour assurer son long terme, l'entrepreneur doit se donner les moyens nécessaires sous peine de disparaître. Encore faut-il qu'il comprenne les enjeux et la réalité de la concurrence internationale dans un milieu hostile riche d'opportunités, mais aussi de menaces équivalentes. Il doit être conscient qu'il est en

conflit réel avec tous les autres qui veulent améliorer leur propre position afin de faire croître leurs parts de marché, leurs marges, et l'emploi sur leurs sites. Il a l'obligation d'être réaliste face à des concurrents dont certains ne reculeront pas devant l'utilisation de techniques et moyens frauduleux.

Dans ce combat concurrentiel dans lequel chacun est dos au mur la progression ne peut se réaliser qu'en étant meilleur que l'autre dans la plupart, voire la totalité des fonctions de l'entreprise. La bonne idée d'ingénieur qui garantit le succès, dans le long terme sans remise en cause, est remplacée par une idée innovante ou de rupture qu'on va améliorer sans cesse par la recherche et les idées récupérées ailleurs. Cette amélioration permanente de l'existant repose donc sur le renseignement environnemental et concurrentiel qui va nourrir les laboratoires, les centres de production et le marketing.

## La perte d'éthique

Tout cela serait parfait si, parallèlement à cette évolution plutôt positive, nous n'assistions pas à l'émergence de son pendant négatif dans tous les domaines concernant la vie de l'entreprise. À la transparence des uns s'oppose la corruption des autres. Les apôtres de l'éthique et de la morale sont confrontés aux mauvais génies du tout est permis pour ce qui les concerne. La pratique des actions illégales est considérée comme licite par de plus en plus de responsables soucieux d'obtenir des résultats rapides sur le marché local ou international. L'abus du droit à la différence ou des pratiques de la diversité permet de s'abstenir du respect des règles en le justifiant par le rapport du faible au fort.

La désinformation devient un mode de communication pour détruire l'adversaire en commençant par son image et sa réputation. Le coût des cyberattaques devient explosif et met en danger l'entreprise et ses dirigeants. Il s'y ajoute de la part de certains États une défense impérialiste de leurs entreprises en imposant leurs propres règles pour casser les équilibres concurrentiels au nom de la loi du plus fort.

## La sécurité physique et matérielle

Avec le temps l'entreprise avait appris à maîtriser la sécurité des biens matériels et des personnes physiques en implantant des procédures et en utilisant des équipes de sécurité internes ou externes. Elle avait été aidée par les compagnies d'assurance qui acceptaient de prendre en charge financièrement la quasi-totalité du risque sous réserve d'un formatage de l'entreprise respectant leurs règles de fonctionnement et leurs modes d'expertise. Elle y avait été encouragée par l'État et surtout par l'opinion publique qui, au nom du principe de précaution, refuse la moindre prise de risque par l'entreprise en la jugeant coupable en cas de problème imprévu.

L'arrivée de systèmes de contrôle identitaire biométrique, la mise en place de robots de surveillance fixes et mobiles, l'implantation de systèmes de détection d'intrusion ou d'incendies ont considérablement amélioré l'efficacité de cette partie de la sécurité dont l'usage exige un personnel qualifié et entraîné.

Avec ces outils, pour celui qui peut y consacrer les moyens financiers nécessaires, le risque devient extrêmement réduit.

## La sécurité immatérielle

Aujourd'hui, le problème sécuritaire a pris une autre forme avec le développement des dérives éthiques, des attaques contre les biens immatériels, les agressions physiques ou morales contre les personnels et les dirigeants, et un environnement international de plus en plus violent et fluctuant. Les grandes affaires récentes comme Renault, Ikea, TV5, Gemalto ou Alstom en montrent l'impact dans tous les domaines et la difficulté des dirigeants à affronter ces types de crise auxquels ils ne sont généralement pas préparés.

Il est vrai qu'ils sont confrontés à une révolution digitale s'appuyant sur les possibilités ouvertes par l'Internet, les capacités de stockage et de recherche offertes par le *big*

AUJOURD'HUI, LE PROBLÈME SÉCURITAIRE A PRIS UNE AUTRE FORME AVEC LE DÉVELOPPEMENT DES DÉRIVES ÉTHIQUES, DES ATTAQUES CONTRE LES BIENS IMMATÉRIELS, LES AGRESSIONS PHYSIQUES OU MORALES CONTRE LES PERSONNELS ET LES DIRIGEANTS, ET UN ENVIRONNEMENT INTERNATIONAL DE PLUS EN PLUS VIOLENT ET FLUCTUANT.

*data*, le suivi des objets dans le web 3.0, et les inventions qui se succèdent pour optimiser le cyberspace.

La réduction croissante du délai de traitement fait qu'on travaille plus vite sans avoir le temps de tout valider. On redécouvre l'importance de la prospective pour définir le cadre de l'action à mener et les objectifs à atteindre dans un temps qui s'accélère. En quelques heures l'information fait le tour du monde par les réseaux sociaux. On échange et analyse des masses croissantes de données avec l'aide d'algorithmes. Les signaux faibles, chers à l'analyste du début du siècle, sont devenus des signaux forts pour ne pas dire assourdissants. Mais cette formidable évolution a son talon d'Achille : l'identification de chaque émetteur et récepteur et la sécurisation des flux en y incluant le stockage.

## La cybersécurité

Dans cette floraison digitale la cybercriminalité vit une croissance exponentielle facilitée par l'insuffisance de mise en place de procédures de sensibilisation et de prévention. Le chaos généré par la multiplicité des outils, des programmes et des nouvelles techniques favorise les experts du *Dark web* qui se spécialisent et s'organisent. Les accords entre industriels et États permettent à certains de bénéficier de données confidentielles ou secrètes obtenues en toute illégalité. Par leur ampleur, les escroqueries financières ont un impact réel sur les résultats des entreprises. Le vol de données et le piratage d'informations mettent en danger le développement et la pérennité des sociétés.

À ce stade, de même qu'on a créé des missions d'audit pour contrôler les directions comptables et financières, nous devons faire de même pour gérer la cybersécurité, car les directions des systèmes d'information sont inefficaces face à des attaques qui les déstabilisent. Il va falloir apprendre à gérer sérieusement la sécurité numérique, de la mise en place de procédures jusqu'à la crise. Il va falloir enfin bloquer les pratiques d'espionnage industriel pratiquées contractuellement par des individus ou des sociétés pour le compte de clients se refusant à pratiquer une concurrence loyale.

## La sécurité contre la fraude et la corruption

La criminalité traditionnelle qui s'améliore grâce à de nouveaux outils continue de faire des victimes. Au-delà des

vols de produits ou de matériels sur les sites ou durant le transport, des braquages qui ont toujours existé, la fraude existe partout, parfois encouragée par des règles trop contraignantes ou le laxisme des contrôles. La contrefaçon pratiquée à grande échelle au plan international coûte cher en dépit des actions menées dans le cadre légal. Du contournement des brevets à la copie de produits en passant par le non-paiement de taxes, certains industriels, qu'il faut identifier, utilisent sciemment ces possibilités pour améliorer leur marge ou leur part de marché.

La corruption est partout à des degrés divers. Culturelle dans certains pays, organisée dans d'autres, assimilée à de la débrouillardise chez certains, elle est une réalité qui déséquilibre le jeu concurrentiel dans les marchés. Malgré les actions menées à grande échelle par l'Organisation des Nations unies (ONU) et l'Organisation de coopération et de développement économiques (OCDE), et les actions d'Organisations non gouvernementales (ONG) à la finalité pas toujours très claire dans leur condamnation systématique de certains et leur mansuétude pour d'autres, la corruption continue dans la plus grande partie du monde sous des formes variées. La sécurité de l'entreprise implique d'en cartographier les réseaux et mettre en place des procédures et contrôles empêchant de s'y trouver impliqué sans pour cela être naïf.

## La sécurité des relations humaines

La sûreté comprend également certains problèmes lorsqu'ils sortent du domaine normal d'une fonction. La gestion du fait religieux avec ses conséquences est menée par la direction des ressources humaines, mais celle-ci a besoin d'informations sur les meneurs, les objectifs et leur environnement, toutes questions qui relèvent de la sûreté. La situation est la même en cas de rupture du dialogue social ou l'entreprise doit négocier en étant confrontée à des blocages, des séquestrations de cadres, ou des actions de malveillance allant jusqu'au sabotage. Dans le strict respect de la légalité, il s'agit de trouver des opportunités de négociation, d'avoir une meilleure connaissance de ceux avec qui on va négocier, d'anticiper leur futur comportement.

Bien qu'il soit souvent rattaché à la « compliance » on ne peut évacuer le problème des lanceurs d'alerte qui sont à la fois une source d'information et de désinformation selon le mobile qui les pousse. Le traitement de leurs plaintes ne peut pas être réalisé par une fonction de l'entreprise par suite du risque de les voir étouffées ou surexploitées. C'est un problème qui relève de la sûreté, mais doit bénéficier

d'un traitement spécial et normé réalisé en liaison avec la direction générale de l'entreprise.

## La sécurité des expatriés

On ne peut traiter de la sûreté aujourd'hui sans évoquer la mise en place d'expatriés ou le passage de missionnaires dans des zones à risque et des marchés émergents. Notre pays est exposé par sa politique à des représailles et actions variées visant à nous intimider ou nous faire changer d'approche. Le principe de précaution et la morale obligent nos sociétés, qui n'ont pas d'autre choix que d'aller à l'international, de mettre en place de véritables plans d'actions pour protéger physiquement leur personnel expatrié et local.

Au-delà de l'évaluation des menaces et risques terroristes ou d'instabilité locale, il faut sensibiliser et former les personnels concernés et leurs familles pour les différents niveaux d'alerte. Il faut construire des plans de récupération en cas de crise adaptés aux degrés successifs de la montée en puissance de celle-ci. Il faut enfin être capable d'anticiper et de gérer les prises d'otages. Tout ceci se construit en liaison étroite avec les autorités françaises et locales concernées dans un partenariat public-privé qui est essentiel.

## La sécurité environnementale

Un autre domaine insuffisamment analysé et étudié dans la plupart de nos entreprises concerne les questions environnementales. Je n'évoque pas ici les incendies de sites ou les inondations relativement prévisibles ou envisageables dans la cartographie des risques et leur criticité. Nous rentrons dans les problématiques que l'on incorpore dans le développement durable et qui vont prendre de plus en plus d'importance pour nos concitoyens. Loin d'une vision minimaliste ou réductrice d'ingénieur ou de financier, c'est à la sûreté de sensibiliser, et de proposer des mesures pour améliorer la situation, mettre en place des systèmes de surveillance et prévenir les accidents.

Qu'il s'agisse de gérer les problèmes d'épidémie, de pollution ou de catastrophe naturelle, l'identification par anticipation du problème, la mise en place d'une cellule de gestion de crise, le pilotage avec les pouvoirs publics relèvent de la sécurité et de son responsable.

## L'évaluation d'efficacité

Dans la mise en œuvre du concept de sûreté globale de l'entreprise, il est impératif d'évaluer la pertinence des mesures de sécurité pour chaque situation et chaque problématique. Il faut ensuite mettre en place les ressources nécessaires, ce qui présuppose d'évaluer les risques, localiser les failles, et fixer les priorités pour construire les plans d'actions à court, moyen, et long terme. Parallèlement, chaque incident, chaque accident, chaque attaque doit faire l'objet d'un bilan détaillé permettant de mettre en place les mesures de correction. Nous sommes dans un processus d'amélioration permanente à l'épreuve des faits.

AU-DELÀ DU RENSEIGNEMENT QUI NOURRIT LA CAPACITÉ D'ANTICIPATION ET PERMET DE COMPRENDRE L'ADVERSAIRE ET LES DIFFÉRENTS TYPES DE SÛRETÉ QU'EXIGE L'ENTREPRISE, LA SÛRETÉ DANS SA GLOBALITÉ EST DEVENUE UNE PRIORITÉ STRATÉGIQUE. ELLE REPOSE SUR LA CAPACITÉ D'ANTICIPATION, LA PRÉSERVATION DE LA COMPÉTITIVITÉ, ET LA CAPACITÉ DE GÉRER TOUS LES TYPES DE CRISES.

## Les dirigeants face à la sûreté

Au-delà du renseignement qui nourrit la capacité d'anticipation et permet de comprendre l'adversaire et les différents types de sécurité qu'exige l'entreprise, la sûreté dans sa globalité est devenue une priorité stratégique. Elle repose sur la capacité d'anticipation, la préservation de la compétitivité, et la capacité de gérer tous les types

de crises. De l'escroquerie informatique à la prise d'otages en passant par les séquestrations de dirigeants ou les plans épidémies, ceci implique d'avoir des responsables capables de répondre directement ou indirectement à la totalité de ces problèmes.

Le dirigeant d'entreprise n'a pas été formé aux problèmes de sûreté et de sécurité. Il a donc besoin d'un conseiller capable de lui apporter les avis ou les éléments de réponse nécessaires dans les délais requis. Ce sont des situations dans lesquelles il faut réagir vite et bien, l'échec pouvant être désastreux pour l'ensemble de l'entreprise. Comme

L'ont bien compris les Américains, la sûreté se traite au niveau du comité de direction.

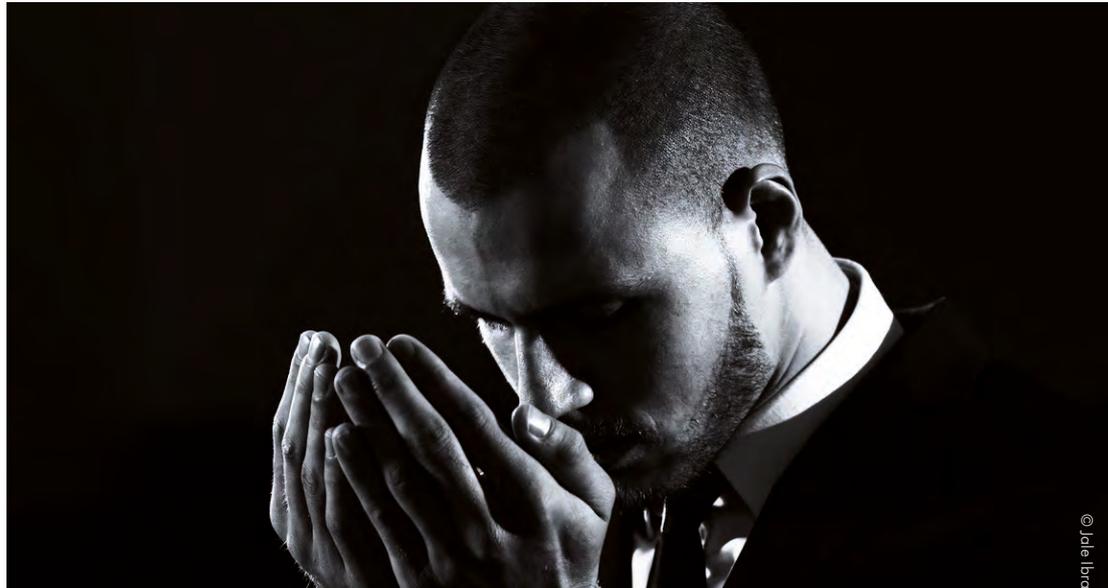
## Le directeur sûreté

Lorsqu'on évoque les menaces pesant sur les entreprises et les collectivités, on pense en priorité à la sécurité des sites et des biens d'équipement et depuis quelques mois à la protection des infrastructures névralgiques ou organisations d'importance vitale, mais on a tendance à oublier tous les autres problèmes qui se posent au niveau de la sûreté et de la sécurité de nos entreprises. Or, ils sont nombreux, variés, et exigent dans chaque domaine des connaissances approfondies ou pour le moins la capacité de les comprendre. Ceci pose le problème de la formation préalable permettant la mise à niveau pour ceux qui ne maîtrisent qu'une partie du spectre des activités couvertes par un métier qui se complexifie en devenant une direction transversale au niveau du comité exécutif.

Le responsable sûreté doit être un généraliste, spécialiste de la gestion de crise, ayant une bonne connaissance personnelle des situations, mais possédant aussi un excellent réseau de conseils et d'experts extérieurs. Il doit

pouvoir s'appuyer dans l'instant sur des professionnels allant de l'expert aux collègues d'autres entreprises en passant par des contacts avec les différentes administrations concernées. C'est dans ce cadre d'échanges que des organisations comme le Club des directeurs de sécurité des entreprises (CDSE) se révèlent essentielles.

Pour conclure, il paraît important de faire comprendre à nos concitoyens et à nos entreprises que les différentes facettes de la sécurité traditionnelle sont en train de passer au second plan face à l'émergence de nouveaux problèmes qui exigent des réponses adaptées construites par des personnes ayant été formées pour ces types de situation. Le management de la sûreté dans sa globalité requiert certes une polyvalence sécuritaire, mais surtout une capacité de gestion de tout type de crise qui présuppose la constitution et l'entraînement d'équipes spécialisées. Elle exige aussi la capacité de piloter des recherches d'informations à l'extérieur et l'intérieur de l'entreprise dans le strict respect des lois françaises et de l'éthique qui reste la garantie fondamentale du bon fonctionnement de cette activité. C'est pourquoi la pratique de l'intelligence économique est indispensable pour un bon fonctionnement de la sûreté ■



# La « radicalisation » dans l'entreprise

Mustapha BENCHENANE

dans le monde de l'entreprise et, plus généralement, dans les espaces dédiés au travail ?

L'État et la société française semblent considérer que l'islam est un problème préoccupant sinon inquiétant. Cette perception va en s'exacerbant au fil du temps dans la mesure où les signes visibles d'appartenance à cette religion produisent des réactions de plus en plus négatives. Les attentats terroristes contribuent grandement au sentiment diffus ou clairement exprimé de rejet de tout ce qui rappelle de près ou de loin l'islam et les musulmans. Ceux parmi ces derniers qui se distinguent soit en portant le « Hidjab » – et encore plus le « voile intégral » – pour les femmes, ou l'accoutrement pakistano-afghan, pour les hommes, justifient la suspicion que certains nourrissent à leur égard. En même temps, ils se plaignent en se disant victimes de discriminations.

Peut-on parler, comme le font tous ceux qui s'expriment sur le sujet, de « radicalisation »

Le terme « radicalisation » est aussi utilisé pour désigner des jeunes qui se réclament de l'islam au nom duquel ils partent faire le « Djihad » en Syrie, ou commettent des attentats terroristes dans des pays européens où ils sont nés et dont ils sont des citoyens...

Si la « radicalisation » fait référence au processus menant au « Djihad » ou au terrorisme en général, le simple fait de réclamer un lieu de prière à l'intérieur de l'entreprise ou de porter un signe d'appartenance à la religion musulmane ne relèverait pas de la « radicalisation ». Il s'agirait plutôt d'une inadaptation à l'environnement social et culturel occidental ou d'un refus conscient de l'intégration dont on parle beaucoup et que l'on définit rarement. Une personne est intégrée si elle est utile socialement et si elle adhère aux normes, valeurs et codes de la société au sein de laquelle elle est censée vivre.

**Mustapha BENCHENANE**



Docteur d'État en Science politique et conférencier au Collège de défense de l'Organisation du traité de l'Atlantique nord (OTAN).

S'agissant plus précisément en France de la question religieuse c'est-à-dire l'islam et l'entreprise, qu'en est-il ?

L'appartenance à l'islam revendiquée par des salariés du secteur privé et rendue visible par des demandes et/ou des comportements, des vêtements, empêche-t-elle l'entreprise d'atteindre ses objectifs de résultats ? Est-ce qu'il s'agit d'autre chose que du critère d'efficacité et que dit le droit ?

## La difficile restriction des libertés dans l'entreprise

### Une liberté qui dérange

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 liberté de religion et de conviction est reconnue par le préambule de la constitution du 27 octobre 1946.

La Haute autorité de lutte contre les discriminations (HALDE) rappelle, dans une délibération du 6 avril 2009, que, comme toute personne, le salarié a le droit à la liberté de ses opinions, qu'elles soient religieuses ou politiques. En entreprise, cela signifie que chaque salarié peut porter un insigne ou un vêtement, exprimant de façon visible son appartenance à une religion.

L'article L 1121 du Code du travail établit : « *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* ». Néanmoins, l'exercice de cette liberté donne lieu à des malentendus, à des tensions et, parfois, à des conflits sur lesquels la justice est appelée à se prononcer. Par exemple, l'entreprise EDF a publié un document intitulé : « Repères sur le fait religieux dans l'entreprise à l'usage des managers et des responsables des ressources humaines ». Des cas concrets de comportements qui dérangent sont cités :

- un salarié refuse de serrer la main des femmes en se référant à sa religion ;

- un salarié demande des aménagements d'horaires de travail parce qu'il fait le ramadan ;

- des salariés utilisent, sans autorisation, les vestiaires pour faire leurs prières ;

- un garçon boucher refuse de servir du porc.

Ces exemples ne sont pas exhaustifs. Le principe du respect de la liberté religieuse l'emporte dans la majorité des cas, y compris quand l'entreprise doit avoir un règlement intérieur. En effet, selon l'article L 1311-1 du Code du travail, toute entreprise d'au moins vingt salariés est dans l'obligation d'élaborer un règlement intérieur. Quant à l'article L 1321-1, il précise que des dispositions de ce règlement ont un caractère limitativement défini et ne doivent pas notamment introduire des discriminations à raison des mœurs, des opinions ou de la religion des salariés.

Dans le premier arrêt « Baby Loup » (une salariée portant le « foulard islamique » dans une crèche a été licenciée), la Cour de cassation a estimé que « *la laïcité* » ne saurait justifier une telle « *restriction* ». La Cour considère que le « *principe de laïcité instauré par l'article 1<sup>er</sup> de la Constitution n'est pas applicable aux salariés des employeurs de droit privé qui ne gèrent pas un service public. Ce principe ne peut dès lors être invoqué pour priver les salariés de la protection que leur assurent les dispositions du code du travail*<sup>1</sup> ». ».

Par ordonnance de référé du 17 décembre 2002, le Conseil des Prud'hommes a jugé qu'un licenciement en raison des « *convictions religieuses* » oblige l'entreprise à réintégrer le salarié. La Cour d'appel de Paris – Arrêt 19 juin 2003 – a confirmé l'ordonnance en considérant que le licenciement était manifestement illicite en ce que la restriction sur les vêtements cachait une atteinte à la liberté religieuse.

Cependant, cette liberté n'est pas absolue. Dans certains cas des restrictions sont jugées conformes à la légalité.

### Des restrictions conformes à la légalité

La HALDE, dans sa délibération du 6 avril 2009, a pris position sur les restrictions de la liberté religieuse dans l'entreprise. Elle précise que cette liberté ne doit, en aucun cas, prévaloir sur le « *bon fonctionnement de l'entreprise* ».

Par exemple, un salarié ne peut pas invoquer sa religion pour refuser tout ou partie de ses obligations légales ou contractuelles :

(1) Cass.soc, 19 mars 2013, premier arrêt « Baby Loup ».

- la visite médicale ;
- s'autoriser des absences pour certaines fêtes ;
- réclamer des aménagements de son temps de travail pour des prières.

À partir du moment où le salarié ne pourrait plus s'acquitter de ses obligations contractuelles, l'employeur peut, à bon droit, lui refuser les demandes qu'il exprime. L'« intérêt de l'entreprise » prime, dans la plupart des cas, sur le principe de la liberté religieuse dans le milieu du travail. Ont ainsi été jugés inacceptables, car contraires aux intérêts de l'entreprise, des abus de liberté d'expression (des propos injurieux, diffamations), des actes de prosélytisme, des actes de pression sur les autres salariés.

En général, les restrictions sont justifiées au regard de la jurisprudence, dans deux cas : 1) les impératifs de sécurité et de santé, par exemple lorsque le port d'un signe religieux est incompatible avec l'équipement de sécurité obligatoire ; 2) La nature de l'activité que le salarié doit accomplir. C'est ainsi que la Cour d'appel de Paris a estimé justifiée l'interdiction du foulard islamique à une vendeuse d'un centre commercial et à une technicienne de laboratoire.

Les juges ont décidé que ces deux salariées étaient en contact direct avec la clientèle, donc à un large public de convictions variées. Le port du « foulard islamique » pouvait nuire à l'image de l'entreprise<sup>2</sup>.

La justice se prononce au cas par cas et s'attache aux critères de pertinence et de proportionnalité. Les juges considèrent, en effet, que le simple fait d'être en contact avec la clientèle ne suffit pas, dans tous les cas, à justifier une décision portant atteinte à la liberté de religion et de conviction du salarié. Une restriction de cette nature est vérifiée par le juge qui se préoccupe de savoir s'il y a des éléments objectifs légitimant cette restriction et il veille au respect du principe de non-discrimination.

Les décisions des employeurs doivent être inspirées uniquement par le but de « bon fonctionnement », de « bonne marche » de l'entreprise et non par des considérations étrangères à ces objectifs. Par exemple, le

refus d'accorder un jour de congé pour une fête religieuse doit être justifié par le bon fonctionnement de l'entreprise, entre autres, si l'effectif étant insuffisant, le suivi des dossiers en cours ne pouvait pas être assuré. Dans un autre cas, le juge a estimé que l'employeur n'aurait pas dû interdire le port du « foulard islamique » à une salariée d'un « Call Center », car la salariée était en contact avec les « clients » uniquement par téléphone.

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*<sup>3</sup> ». L'employeur qui serait reconnu coupable de discrimination pourrait être condamné à une peine de trois années d'emprisonnement et à une amende de 45 000 euros.

Comme on le constate, les décisions de justice ne permettent pas toujours aux chefs d'entreprise de savoir clairement quelle est l'étendue de leur pouvoir lorsqu'il s'agit d'apporter des restrictions à la liberté de religion au sein de l'entreprise.

*La HALDE, dans sa délibération du 6 avril 2009, a pris position sur les restrictions de la liberté religieuse dans l'entreprise. Elle précise que cette liberté ne doit, en aucun cas, prévaloir sur le « bon fonctionnement de l'entreprise ».*

Dans le rapport qu'il a remis au gouvernement le 25 juin 2013, l'Observatoire de la laïcité préconise la diffusion de « guides » expliquant ce qui est permis ou non dans ce domaine. Le « comité diversité » du Mouvement des entreprises de France (MEDEF) suggère la « *création de guides managériaux regroupant des outils utiles et concrets* » rappelant le cadre légal et réglementaire. Selon le MEDEF, trois règles doivent « *éclairer la gestion managériale* » :

1. « *Partir des demandes particulières exprimées pour rechercher une solution apportant un bénéfice universel y compris pour ceux qui n'ont rien demandé* » ;
2. « *Invoquer le principe d'équidistance : neutralité et discrétion par rapport à ses confrères, à ses clients, à ses fournisseurs, etc.* ;
3. « *Ne pas tenter d'interpréter les textes religieux et s'en tenir à la situation de travail dans l'entreprise* ».

(2) Cour d'appel de Paris, 16-03-2001.

(3) Cour d'appel de Paris, Arrêt 19 juin 2003.

Il y a, par ailleurs, le cas spécifique des « entreprises de tendance », c'est-à-dire des entreprises qui défendent des principes idéologiques, religieux ou philosophiques spécifiques. Par exemple, en se fondant sur le principe catholique d'indissolubilité du mariage, la Cour de cassation a estimé fondé le licenciement d'une enseignante qui s'était remariée après un divorce. La Cour de cassation a justifié son arrêt en se référant au « caractère propre » de l'établissement confessionnel.

Dans l'affaire de la crèche Baby Loup, la Cour d'appel avait décidé fin 2013 que la crèche pouvait revendiquer le statut « d'entreprise de conviction » et ainsi instaurer une « obligation de neutralité ». Dès lors, le licenciement ne portait « pas atteinte à la liberté religieuse ». La Cour de cassation a été saisie d'un pourvoi en cassation par les avocats de la salariée. Le Procureur général de cette Cour conteste dans son avis que la crèche puisse être considérée comme une « entreprise de conviction ». « Elle n'est pas une entreprise de combat militant en faveur de la laïcité ; son objet est plus social que politique ».

Cette affaire a été fortement médiatisée, elle a mobilisé tous les échelons de la justice et, chose rare, l'arrêt de la Cour de cassation du 19 mars 2013 a été contredit par celui de la Cour d'appel le 27 novembre 2013 devant laquelle le dossier avait été renvoyé. En fin de compte, la Cour de cassation, réunie en assemblée plénière le 25 juin 2014, a donné raison à la Cour d'appel qui avait osé contredire l'arrêt rendu en 2013 par la chambre sociale de cette même Cour de cassation... « L'Assemblée plénière approuve la Cour d'appel d'avoir déduit du règlement intérieur que la restriction à la liberté de manifester sa religion qu'il édictait ne présentait pas un caractère général, mais était suffisamment précise, justifiée par la nature des tâches accomplies par les salariés de l'association et proportionnée au but de recherche ».

Les étapes de ce « marathon » judiciaire furent les suivantes :

- la salariée est licenciée pour « faute grave » en décembre 2008 ;
- les Prud'hommes confirment le licenciement le 13 décembre 2008 ;
- le licenciement est confirmé par la Cour d'appel de Versailles le 27 octobre 2011 ;
- 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 ;

- la Cour d'appel de Paris rend un « arrêt de rébellion » le 27 novembre 2013 ;

- la Cour de cassation, de nouveau saisie, suit l'arrêt de la Cour d'appel de Paris, par un arrêt rendu le 25 septembre 2014.

Ces décisions judiciaires qui disent une chose et son contraire, ont été rendues dans un climat passionnel, la dimension politique ayant fortement pesé sur les débats... Mais, en dernière analyse, on peut légitimement se demander si le recours au principe de laïcité est pertinent, le contexte actuel étant marqué par une exacerbation des sensibilités.

## Exacerbation des sensibilités et confusion

### Une exacerbation des sensibilités

En amont des attentats terroristes du 13 novembre 2015 et surtout depuis ces événements tragiques, on constate une mise en exergue des difficultés liées au fait religieux dans l'entreprise. Toute revendication ou attitude reliée, à tort ou à raison, à la religion musulmane est qualifiée de « radicalisation » et peut déclencher une enquête approfondie des services de sécurité.

Le 20 novembre 2015, *Le Figaro* titrait : « Les salafistes font de l'entrisme à la RATP...<sup>4</sup> L'un des terroristes du 13 novembre avait été chauffeur de bus dans cette entreprise pendant quinze mois. Dès lors, l'attention de chacun a été attirée par des incidents liés au comportement de quelques salariés : le refus de serrer la main de collègues féminines ; le refus de prendre le bus qui a été conduit par une femme ; des interrogations sur le calendrier des fêtes religieuses ; des demandes de remplacement pendant le mois du Ramadan, etc. Un salarié a été licencié pour avoir fait sa prière lors d'un service, dans le bus. La RATP serait l'une des entreprises qui emploie le plus de personnes fichées S. La direction fait valoir qu'une quarantaine de cas aurait fait l'objet d'un signalement « soit 0,1 % des 45 000 agents de la RATP en Ile-de-France ». Les dirigeants précisent que « la RATP revendique sa diversité. Il ne faut pas faire d'amalgame entre la diversité et des comportements communautaires marginaux ».

Une clause de laïcité, intégrée depuis 2005 au contrat de travail, stipule que les employés doivent avoir « un

(4) *Le Figaro*, le 20 novembre 2015.

*comportement et des attitudes visant au respect de la liberté et de la dignité de chacun », ainsi qu'un devoir de neutralité. « Vous vous engagez à proscrire toute attitude ou port de signes ostentatoires pouvant révéler l'appartenance à une religion ».*

On retrouve les mêmes problèmes à Air France, à la SNCF, à la Poste.

Air France a élaboré une « Charte de la laïcité ». Depuis le début de l'année 2015, une soixantaine de salariés des aéroports de Roissy et d'Orly ont perdu leur agrément, le « badge rouge » donnant accès aux plates-formes aéroportuaires. Certains de ces retraits avaient pour cause une « radicalisation ». Exemple : le refus de travailler sous les ordres d'une femme. Des réflexions violentes concernant les attentats contre *Charlie Hebdo*.

Dès lors que ces comportements sont signalés au préfet de Police, une enquête poussée est déclenchée. Pourtant, afin d'obtenir l'agrément permettant de travailler dans l'enceinte de l'aéroport, trois enquêtes sont lancées par le préfet et le procureur ; la première au terme de la certification obtenue après une formation ; la deuxième se déroule lors du recrutement et la troisième pour obtenir le badge d'accès au site, valable trois ans, avant une nouvelle enquête.

Au jour le jour, des interprétations sans discernement peuvent donner lieu à des abus. C'est ainsi que l'entreprise Securitas a licencié des agents travaillant à Orly pour barbe trop longue, la formule utilisée étant : « *non-respect du référentiel vestimentaire* » (décembre 2015).

Bien avant les attentats du 13 novembre 2015, au Mans et à Grenoble, des responsables de l'association Restos du cœur ont refusé de prendre des jeunes filles voilées comme bénévoles sous prétexte que le port du « foulard islamique », enfreint la « Charte du bénévole » qui prévoit une « *indépendance complète à l'égard du politique et du religieux* ».

Le « fait religieux » ou la « radicalisation » dans l'entreprise sont réglés à l'amiable ou de façon conflictuelle en fonction de la perception qu'en ont les responsables hiérarchiques. En avril 2015, 23 % des managers déclaraient être confrontés à un fait religieux au moins une fois par mois dans leur entreprise, presque deux fois plus qu'en 2014 (12 % des sondés<sup>5</sup>).

Depuis le 13 novembre 2015, le gouvernement s'est déclaré résolu à améliorer « la détection de la radicalisation

dans les entreprises ». Un guide sur la « gestion du fait religieux dans les entreprises » doit être élaboré par le ministère du Travail.

Le 5 juin 2015, sept syndicats ont adopté un texte intitulé « Après le 11 janvier 2015 : vivre ensemble, travailler ensemble », dans lequel la question de la liberté au travail fait l'objet d'un chapitre...

Cependant, il y a une question, pourtant fondamentale, que les « experts », les politiques, les journalistes, ne se posent pas : est-ce que le fait religieux dans l'entreprise doit être traité sur le registre de la laïcité ?

### **La laïcité, mal comprise ou instrumentalisée ?**

Dans son premier rapport remis au gouvernement le 25 juin 2013, l'Observatoire de la laïcité émet des réserves : « *les atteintes à la laïcité ont peut-être été surestimées* » et surtout, il invite à ne pas faire de la laïcité un « *mot valise* » pour des problèmes qui « *relèvent d'abord de l'intégration ou de politiques économiques et sociales* »...

Dans son livre, *La laïcité falsifiée*, l'un des meilleurs spécialistes de cette question, Jean Bauberot, écrit : « *La laïcité est de l'ordre du politique. En séparant les diverses croyances et l'État, en mettant celui-ci en position de neutralité arbitrale, elle vise à permettre la liberté de conscience de chacun et l'égalité des droits et des devoirs de tous devant la loi. C'est une forme de régulation politique, d'ordonnement de la société démocratique*<sup>6</sup> ». Ce qui ressort de cette définition, c'est que la laïcité est « *de l'ordre du politique* » et elle vise à séparer les « *diverses croyances de l'État* ». Il n'y a rien, dans cette conception, qui renvoie à ce qui pourrait se passer à l'école, à l'hôpital ou dans l'entreprise.

Les deux penseurs qui ont fortement inspiré les rédacteurs de la loi de « séparation des Églises et de l'État » (décembre 1905), Ernest Renan et Ferdinand Buisson, donnent une définition encore plus claire. Ernest Renan, dans sa réponse au discours de réception de Louis Pasteur à

Le « fait religieux » ou la « radicalisation » dans l'entreprise sont réglés à l'amiable ou de façon conflictuelle en fonction de la perception qu'en ont les responsables hiérarchiques. En avril 2015, 23 % des managers déclaraient être confrontés à un fait religieux au moins une fois par mois dans leur entreprise, presque deux fois plus qu'en 2014 (12 % des sondés).

(5) Enquête annuelle de l'Observatoire du fait religieux en entreprise (OFRE), *Le Monde*, 25 novembre 2015.

(6) Bauberot (J.), 2012, *La laïcité falsifiée*, Paris, Éditions La Découverte, p. 145.

l'Académie française le 27 avril 1882, déclare que la laïcité c'est « *l'État neutre entre les religions, tolérant pour tous les cultes et forçant l'Église à lui obéir en ce point capital* ». Ferdinand Buisson donne, en 1883, sa définition de la laïcité : « *L'État neutre entre tous les cultes, indépendant de tous les clergés, dégagé de toute conception théologique* »... Ce qui permet « *l'égalité de tous les Français devant la loi, la liberté de tous les cultes*<sup>7</sup> ». La loi de décembre 1905 qui s'inspire de la conception de la laïcité de ces deux personnalités ne consacre aucun de ces articles à autre chose qu'à la séparation de l'État et des Églises.

Bien avant E. Renan et F. Buisson, John Locke (1632-1704), l'un des principaux précurseurs des « Lumières » et chrétien proclamé, annonçait la laïcisation de l'État moderne : « *Tout le pouvoir du gouvernement civil n'a rapport qu'aux intérêts civils, se borne aux choses de ce moment, et n'a rien à voir avec le monde à venir*<sup>8</sup> ».

L'un de nos contemporains reconnu comme une référence académique respectable, Marcel Gauchet, dit la même chose avec d'autres mots. Il définit ainsi la laïcité : « *L'ordre politique n'est pas déterminé par la religion, et cet ordre politique ne poursuit pas des fins religieuses*<sup>9</sup> ».

Pierre Manent s'inscrit dans cette approche et va encore plus loin s'agissant de l'Islam en France : « *La laïcité, au sens originel, c'est la séparation de l'Église et de l'État. Elle laisse la société à ses expressions religieuses spontanées. La III<sup>e</sup> République n'a pas empêché la France de rester un pays catholique. La laïcité que l'on propose aux musulmans vise à neutraliser la religion dans l'espace social. Ce n'est pas le propos de la laïcité, mais une entreprise nouvelle, dont la légitimité me paraît douteuse, et qui en tout cas est impossible à mettre en œuvre. On ne rendra pas la religion invisible*<sup>10</sup> ».

La philosophe allemande Hannah Arendt inscrit sa pensée dans cette orientation lorsqu'elle évoque la « *sécularisation* ». Elle affirme : « *La sécularisation signifie en premier lieu simplement la séparation de la religion et de la politique* ». Elle précise que cette séparation n'a pas pour autant transformé la religion entièrement en une « *affaire privée* ». Elle constate que, lorsque c'est le cas, c'est un régime tyrannique qui gouverne : « *Ce type d'intimité dans la religion se produit seulement quand un régime tyrannique interdit le fonctionnement public des églises et refuse au croyant l'espace public où il peut apparaître avec d'autres et être vu par eux*<sup>11</sup> ».

On constate donc que toutes ces définitions de la laïcité convergent vers une seule et même conception de ce principe. Son utilisation ayant pour objectif d'éradiquer les signes d'appartenance à une religion dans l'entreprise, à l'hôpital, dans les piscines, etc. relève, sinon d'une instrumentalisation, du moins d'une dérive du concept. Si problèmes il y a en ces lieux, ils doivent être abordés et traités sur un autre registre.

Ne serait-ce que dans un souci d'efficacité, il conviendrait de ne pas utiliser le concept de « laïcité » de façon inappropriée. Il en est de même du phénomène dit de « radicalisation » que l'on devrait réserver au processus menant un individu à l'embrigadement dans un réseau terroriste, ou à agir seul, sans appartenance à un groupe. Il faut donc distinguer, dans l'immense majorité des cas, le fait religieux dans l'entreprise de la « radicalisation ». Faute de quoi, tout musulman dont la foi inspire et guide les comportements serait tenu en suspicion. Ce n'est pas le meilleur moyen de l'encourager à s'intégrer. En revanche, la « radicalisation » doit faire l'objet d'anticipation par le renseignement et, quand il le faut, de répression à la hauteur de la menace et des crimes qui seraient préparés ou commis ■

(7) In Jean Bauberot, op cit, p. 50.

(8) John Locke, *Lettre sur la tolérance*.

(9) Gauchet (M.), 1998, « La religion dans la démocratie », éditions Gallimard, Paris, p.12.

(10) Pierre Manent, interview au « Point », le 24 septembre 2015.

(11) Arendt (H.) , *La crise de la culture*, p. 94-95



# Les entreprises à l'épreuve de la cybercriminalité

Noémie NATHAN

La notion d'entreprise est une notion juridique large qui ne saurait se confondre avec la notion de société communément utilisée, notamment en droit commercial, et dont l'acception est plus stricte ; la société correspondant à différentes formes de personnes morales dont le statut est précisément défini juridiquement. L'entreprise peut se définir comme une unité économique impliquant la mise en œuvre de moyens humains et matériels de production et de distribution de richesses reposant sur une organisation préalable. Elle peut ou non revêtir une forme sociale et disposer ainsi de la personnalité morale. C'est cette organisation

structurée, permettant la concentration au sein d'une même entité d'un nombre important de personnes physiques et de richesses matérielles qui fait l'objet d'un traitement spécifique par le droit pénal. L'entreprise, lorsqu'elle est dotée de la personnalité morale, est ainsi susceptible d'acquérir le statut d'auteur d'infraction, mais elle peut également devenir une victime d'un genre particulier. C'est à travers cette qualité de victime qu'il apparaît intéressant d'étudier les liens entre cette entité économique et la cybercriminalité.

Il est possible d'isoler deux grandes catégories d'incriminations pénales qui visent plus spécifiquement les entreprises : celles qui relèvent de la délinquance économique et financière et celles qui relèvent de

## Noémie NATHAN



Magistrate. Précédemment en poste comme juge d'instruction au pôle

financier à Paris, elle dirige actuellement le département Études et recherches de l'Institut national des hautes études de la sécurité et de la justice.

la cybercriminalité<sup>1</sup>. Ainsi, certaines infractions qui ressortent de la sphère économique et financière sont-elles fréquemment commises au préjudice des entreprises en raison de l'importance de leur patrimoine. Les entreprises sont également les cibles d'infractions commises par le biais d'Internet.

La notion de cybercriminalité renvoie aux infractions liées à l'utilisation du réseau internet et aux délinquants qui peuvent prendre pour cibles des entreprises présentant une grande vulnérabilité dans le domaine des agissements dématérialisés. En effet, la communication portant sur l'objet de production est une condition de viabilité économique de l'entreprise et la cybercriminalité s'attaque spécifiquement aux réseaux de communication mis en place.

Le rôle du juge pénal consiste à appréhender et qualifier les actions des individus à travers le prisme de la législation et de l'action répressive. Il s'agit donc de déterminer quels sont les comportements susceptibles d'être assimilés à telle ou telle incrimination pénale. Les infractions pénales traditionnelles touchent une valeur sociale à laquelle le législateur a souhaité apporter une protection particulière. Celles qui entrent dans la catégorie de « cybercrime » touchent le vecteur (Internet) de transmission et de facilitation du crime mais, au-delà et dans une conception stricte de la cybercriminalité, c'est également un « système » qui est protégé. L'infraction qui entre dans le champ de la cybercriminalité proprement dite compte ainsi parmi ses éléments constitutifs la notion de « système de traitement automatisé de données ». Ce type de système, le réseau internet, qui centralise et assure le traitement de données est aujourd'hui au cœur des entreprises<sup>2</sup>, quels que soient leur taille, leur nature et leur objet. Les failles relatives à leurs systèmes informatiques, à leurs réseaux internes ou à leurs données immatérielles font l'objet de préoccupations constantes. Les entreprises concentrent en effet une énergie importante ainsi que des moyens matériels et humains conséquents à la protection de leurs réseaux et systèmes, ceux-ci étant alors susceptibles d'être les cibles d'infractions pénales qui entrent dans la catégorie de cybercriminalité.

Si l'analyse de l'activité pénale dans le champ de la cybercriminalité permet d'affirmer que les entreprises sont souvent les victimes des agissements de « hackers », on observe également que de nombreuses infractions

qui n'entrent pas strictement dans ce champ, mais pour lesquelles le réseau internet constitue un vecteur, prennent fréquemment pour cibles les entreprises. Il s'agit dans ce cas d'agissements dont l'existence n'est pas subordonnée à l'utilisation du réseau internet mais qu'il facilite. En effet, l'analyse de ces affaires amène à constater que, si les auteurs peuvent avoir l'intention de prendre pour cible des individus et d'attaquer des personnes physiques (que le moteur en soit l'appât du gain ou un mobile idéologique ou même politique), ils visent en priorité des structures ou des personnes morales. La dimension symbolique est importante et le fait d'impacter une structure de taille conséquente dotée d'un fort potentiel économique peut conduire ceux qui commettent ces actes à franchir les limites de la légalité. Ainsi, attaquer l'entreprise permet à la fois de s'approprier un patrimoine conséquent et de donner à son acte une dimension politique susceptible d'être symbolique.

La cybercriminalité qui s'attaque aux entreprises regroupe les infractions qui utilisent le réseau internet pour commettre des actes pénalement répréhensibles ; ces agissements peuvent être appréhendés à travers deux catégories. En premier lieu, on observe les actes qui utilisent le web comme un vecteur, un facilitateur ; il s'agit alors des infractions économiques et financières dont les entreprises sont traditionnellement victimes, mais dont l'ampleur est démultipliée par Internet. En deuxième lieu, le réseau internet peut lui-même être le cœur de la cible visée par les auteurs. Dans ce cas, l'entreprise n'est alors victime qu'en tant que support d'un système d'information, support qui permet au surplus aux auteurs de s'attaquer symboliquement aux valeurs inhérentes à l'entreprise visée. Enfin, la cybercriminalité, entendue au sens strict comme un mode d'action criminelle dédiée, recouvre également des infractions d'ordre idéologique ou politique commises à l'encontre d'entités économiques.

## La cybercriminalité au service du mobile financier

Le délinquant, comme toute personne évoluant dans notre monde moderne, a vu sa sphère d'activité s'élargir avec l'expansion d'Internet. De l'art de gouverner à l'étude des interactions, des communications et de leurs modes de contrôle, la cybernétique, qui a offert son

(1) Ces deux catégories d'infractions sont susceptibles de se recouper puisque de nombreuses infractions pénales qui entrent dans la catégorie de la cybercriminalité relèvent d'un mobile crapuleux.

(2) Aussi bien pour les entreprises traditionnelles qui ont dû adapter leur système de communication aux moyens modernes que pour les entreprises plus récentes.

étymologie au préfixe « cyber », englobe bien davantage que la simple notion d'un vecteur de transmission d'idées ou de matériaux. Elle vise ainsi à proposer un mode de compréhension des différentes interactions sociales (parfois exclusivement virtuelles). L'objectif du « cyberdélinquant » est de développer et d'affiner des méthodes criminelles préexistantes, en particulier à travers les infractions traditionnellement qualifiées d'« astucieuses » ou de « crapuleuses », pour assurer une meilleure efficacité à l'acte criminel visant à récupérer des fonds.

Ainsi, les infractions traditionnelles d'atteintes aux biens sont-elles susceptibles d'intégrer un nouveau paramètre, un volet « cyber » permettant d'en accroître la dimension. Ces infractions économiques et financières d'un genre particulier peuvent impliquer une atteinte préalable à l'intimité de la vie privée. Leurs éléments constitutifs principaux recouvrent en outre des techniques de fraudes commises par le biais d'Internet qui supposent un minimum de connaissance dans le domaine du « hacking ».

### D'une violation de l'intimité de la vie privée

La loi n° 2015-912 relative au renseignement du 24 juillet 2015 dans son article premier rappelle l'attachement de l'autorité publique au « respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile<sup>3</sup> ». Au regard de l'évolution de ces infractions d'atteintes à la vie privée et à la dimension qu'elles ont prise avec les nouvelles technologies, la puissance publique rappelle ainsi son attachement à la protection contre les atteintes susceptibles d'y être portées en indiquant qu'elles doivent

être justifiées par une nécessité d'intérêt public prévue par la loi dans le respect du principe de proportionnalité. Du fait de la montée en puissance de ces infractions facilitées par le web, l'autorité publique doit être vigilante dans les atteintes qu'elle porte à cette valeur. C'est d'ailleurs par rapport à l'exigence du respect de la vie privée que le président de la République a sollicité l'examen par le Conseil constitutionnel de la loi<sup>4</sup>.

De nombreuses infractions véhiculées par Internet nécessitent dans leur réalisation une intrusion préalable dans un système protégé. Pour les infractions qui poursuivent un mobile financier, la violation de l'intimité de la vie privée, sans être l'objectif de l'incrimination, peut être l'un des éléments constitutifs ou une condition préalable<sup>5</sup>. Ainsi en est-il notamment de l'infraction d'accès ou maintien frauduleux dans un système de traitement automatisé de données qui suppose l'intrusion dans un système sécurisé pour prendre connaissance de certaines données. Cette infraction est, en outre, susceptible de précéder une autre incrimination pénale et, dans ce cas, d'être plus sévèrement réprimée, lorsqu'il en est résulté la modification ou la suppression de données, ou encore, l'altération du système<sup>6</sup>.

La loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a

DE L'ART DE GOUVERNER  
À L'ÉTUDE DES  
INTERACTIONS, DES  
COMMUNICATIONS  
ET DE LEURS MODES  
DE CONTRÔLE, LA  
CYBERNÉTIQUE,  
QUI A OFFERT SON  
ÉTYMOLOGIE AU PRÉFIXE  
« CYBER », ENGLOBE  
BIEN DAVANTAGE QUE  
LA SIMPLE NOTION  
D'UN VECTEUR DE  
TRANSMISSION D'IDÉES  
OU DE MATÉRIAUX.

(3) Article 1<sup>er</sup> de la loi : Le Code de la sécurité intérieure est complété par un livre VIII intitulé : « Du renseignement » et comprenant un article L. 801-1 ainsi rédigé :

« Art. L. 801-1. - Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité.

« L'autorisation et la mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées aux chapitres I<sup>er</sup> à III du titre V du présent livre ne peuvent être décidées que si :

« 1° Elles procèdent d'une autorité ayant légalement compétence pour le faire ;

« 2° Elles résultent d'une procédure conforme au titre II du même livre ;

« 3° Elles respectent les missions confiées aux services mentionnés à l'article L. 811-2 ou aux services désignés par le décret en Conseil d'État prévu à l'article L. 811-4 ;

« 4° Elles sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation mentionnés à l'article L. 811-3 ;

« 5° Les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoqués.

« La Commission nationale de contrôle des techniques de renseignement s'assure, dans les conditions prévues au présent livre, du respect de ces principes. Le Conseil d'État statue sur les recours formés contre les décisions relatives à l'autorisation et à la mise en œuvre de ces techniques et ceux portant sur la conservation des renseignements collectés. »

(4) Cons. const., 23 juillet 2015 n° 2015-713 DC.

(5) Sur l'infraction principale et générale d'atteinte à l'intimité de la vie privée, il convient de se référer aux éléments constitutifs de l'incrimination prévue à l'article 226-1 du Code pénal, mais également aux infractions suivantes de la section I de ce chapitre du Code pénal qui porte sur les atteintes à la vie privée.

modifié la définition du délit d'introduction frauduleuse dans un système informatique en ajoutant parmi les éléments constitutifs de l'infraction, l'extraction, la détention, la reproduction, la transmission et la suppression de données alors qu'auparavant l'infraction ne visait alternativement que l'introduction frauduleuse de données ou la suppression ou la modification de données contenues dans le système de traitement automatisé de données. En précisant cette infraction, le législateur devait ainsi en faciliter la caractérisation au regard de sa complexité. En mentionnant le fait « *d'extraire, de détenir, de reproduire et de transmettre frauduleusement* » ces données, le vol de données informatiques était ainsi reconnu<sup>7</sup>.

Enfin la violation de la vie privée peut se combiner au mobile économique et financier et constituer un moyen d'obtenir les résultats de l'infraction dont le mobile principal est susceptible d'être crapuleux. C'est le cas des vols de données personnelles susceptibles d'être monétisées, par exemple les vols de listes de clients sur des sites de jeux et de paris en ligne, susceptibles d'être revendues et de rapporter des commissions sur le nombre de futurs clients du site. Ces agissements susceptibles d'être qualifiés d'envois massifs de publicité, ou encore « spamming » non autorisés, peuvent avoir été précédés d'atteintes à un système de traitement automatisé de données dans le but de dérober ces dernières.

Cette violation est donc susceptible d'intégrer la définition de l'incrimination pénale et, par conséquent, d'en devenir l'un des éléments constitutifs ; elle ne saurait pour autant se confondre avec l'élément matériel principal qui fait basculer l'agissement délictueux dans le champ de la « cyberdélinquance ».

## Vers une technique de hacking efficace

L'objectif principal des infractions que nous étudions ici est financier et le préjudice qui en résulte est d'autant plus important que le patrimoine d'une entreprise peut

être conséquent. Ce but est atteint dans le domaine de la cybercriminalité grâce à une technicité avancée en matière informatique à travers diverses activités de piratage.

L'activité la plus commune et qui utilise le moyen de paiement le plus répandu est qualifiée de « carding » ; c'est le piratage des cartes bancaires. Il s'agit soit d'attaques virtuelles visant à récupérer sur des sites, notamment de e-commerce, des numéros de cartes bancaires, soit d'achats sur des forums dédiés de numéros de cartes bancaires ainsi que des moyens d'exploiter des failles de sécurité de sites commerciaux. Cette activité peut être accompagnée de faits qualifiés de « skimming » impliquant des copies de pistes magnétiques de cartes de paiement sur des terminaux de paiement équipés d'un « skimmer ». Les cartes ainsi copiées peuvent être utilisées dans des magasins et restaurants après avoir été encodées et éventuellement embossées<sup>8</sup>. Cette dernière étape est facultative, des achats dématérialisés étant également possibles à l'aide simplement des numéros de cartes bancaires. Les victimes de ce type d'infractions peuvent être des particuliers ou des entreprises et leurs moyens de paiement peuvent ainsi être compromis. Les entreprises de e-commerce sur les sites desquelles ont été récupérés les numéros de cartes sont particulièrement atteintes par ces attaques, la révélation de la vulnérabilité de leurs sites ayant en outre des conséquences économiques non négligeables.

L'activité de « phishing », ou hameçonnage, peut également être évoquée dans la mesure où elle prend également des entreprises pour cible. Il s'agit d'un mode d'usurpation d'identité numérique. Ce terme qui mélange les mots « fishing » (pêcher) et « phreaking » (utilisation frauduleuse des lignes téléphoniques) décrit une technique consistant à adresser un mail à un internaute l'invitant à se connecter à un site, lequel est une copie parfaite d'un site connu de l'internaute, et à lui réclamer, sous divers prétextes, notamment des vérifications en cours, des informations confidentielles (en particulier ses coordonnées bancaires). Cette récupération de données personnelles peut

(6) Aux termes de l'article 323-1 du Code pénal : « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende. Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende ».

(7) Aux termes de l'article 323-3 du Code pénal : « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende. Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende ». Cette disposition a fait l'objet d'une question prioritaire de constitutionnalité motivée notamment par le caractère général et imprécis de sa définition qui n'a pas été transmise au Conseil constitutionnel, la Cour de cassation ayant estimé que cette question ne présentait pas le caractère sérieux nécessaire (Cass. crim. 10 avril 2013 n° 12-85.618).

(8) Il s'agit d'imprimer en relief, sur une carte de paiement, des indications permettant d'identifier le titulaire de la carte bancaire.

également se faire grâce à l'utilisation d'une fausse page d'accueil. L'activité de « pharming » a le même objectif que le « phishing », mais elle vise plus spécifiquement l'exploitation d'une faille de sécurité ; l'internaute est ici redirigé vers un serveur compromis ou un site piège sur lequel va s'opérer la récupération des données. Ces activités qui touchent le patrimoine de la victime directe affectent également la crédibilité de l'entité propriétaire du site internet attaqué, qu'il s'agisse d'une banque, d'une entreprise ou d'un service public.

Enfin, la fraude à la fausse charité constitue également une illustration de la cybercriminalité à mobiles financiers. Il s'agit, dans la version la plus simple, d'inviter l'internaute à entrer ses coordonnées bancaires après avoir fait appel à ses dons. Elle peut concerner également des entreprises qui n'ont pas de systèmes de sécurité efficaces.

Pour chacune des actions décrites qui opèrent dans le champ de la cybercriminalité, le mobile financier représente le moteur principal de la transgression de la norme pénale. Il n'en est pas, pour autant, le seul. En effet, l'analyse des arguments de défense invoqués par les auteurs de ce type d'infractions, outre la nature même de leurs comportements atteste de l'importance du mobile technique et idéologique comme levier du passage à l'acte délictueux. Les « cyber-délinquants » invoquent en effet fréquemment l'existence de valeurs supérieures déterminantes dans leur comportement, ce qui justifierait une atténuation de la sanction.

## La cybercriminalité au service de valeurs supérieures

Pour l'infraction « cyber » proprement dite, celle qui naît avec l'utilisation du réseau de communication et d'information immatériel, le système de traitement automatisé de données n'est pas seulement un moyen de commettre l'infraction, mais il en constitue l'essence même. Cette infraction peut viser une entreprise et avoir pour effet de toucher son patrimoine et certains de ses éléments matériels ; pourtant les auteurs arguent souvent d'un mobile idéologique pour s'attaquer à la dimension immatérielle de la structure, à son réseau de communication. Ils invoquent alors, par exemple, leur désir d'améliorer leurs connaissances en informatique et de tester des failles dans la sécurité des systèmes. C'est le mobile du défi technique qui est l'une des justifications fréquemment invoquées. Mais le professionnel sera également confronté à des mobiles idéologiques et politiques qui confèrent à ces infractions une tout autre nature, ce qui conduit les juridictions à les appréhender et à

les sanctionner très différemment de celles précédemment décrites, en raison de la dangerosité particulièrement importante qu'elles recèlent.

### Du défi technique

Le défi technique est souvent mis en avant par les auteurs pour justifier des actes revendiqués sur Internet. Commettre de telles infractions permet à leurs auteurs d'acquiescer puis de conforter une réputation de « hackers » efficaces et de valoriser des actes qui ne sont pas considérés sur la toile comme délictueux. Ils n'ont, la plupart du temps, pas conscience d'avoir franchi la barrière de la légalité et parviennent souvent à fédérer autour d'eux une communauté solidaire qui les soutient dans leurs actions, voire les admire. Ces auteurs souvent très jeunes, parfois même mineurs, passionnés d'informatique et particulièrement doués, peuvent avoir une connaissance très limitée des enjeux du monde professionnel et, notamment, de celui des entreprises qu'ils attaquent d'initiative ou sur commande. On observe en effet que, dans un certain nombre de cas, le véritable commanditaire de l'infraction n'est pas son auteur direct et qu'il peut être mû par un objectif très différent ; la finalité de l'instigateur peut être financière (bénéfice pour des sociétés concurrentes par exemple), ce qui n'est en rien incompatible avec le défi technique, relevé par l'auteur direct sollicité afin d'exploiter les failles de sécurité des sites des entreprises à attaquer. Les auteurs directs peuvent ainsi revendiquer le mobile du défi technique sans que ce dernier n'exclue par ailleurs la rémunération de leur activité délictueuse.

Les profils des auteurs directs ainsi que leurs revendications idéologique et technique exposées comme mobiles de leurs passages à l'acte face à des juridictions souvent peu familières de ce type d'agissements expliquent en grande partie le faible niveau de répression de ces comportements qui peuvent pourtant entraîner des préjudices considérables.

Il convient ainsi d'appréhender avec réserve le mobile du défi technique dans la mesure où il s'agit souvent d'actes très rémunérateurs, notamment les multiples achats sur Internet susceptibles d'être récupérés dans des « points relais » à l'aide de faux documents d'identité et de procurations. Si les objets de ces infractions sont des matériels de haute technologie, ils pourront être revendus à des tarifs élevés notamment sur des sites de e-commerce, ce qui entraînera d'importants niveaux de rémunération pour leurs auteurs, rémunération qui ne saurait constituer une motivation de second plan. Les campagnes de « spamming » impliquant au préalable des vols de données informatiques peuvent également engendrer des

gains conséquents pour les auteurs, gains dont l'attrait ne saurait disparaître totalement derrière la motivation de relever un défi technique. Celui-ci est souvent absent de l'esprit de l'instigateur et n'efface pas l'aspect financier des infractions commises, qui entraînent un préjudice conséquent pour la victime, en particulier lorsque celle-ci est un acteur économique.

Au-delà des infractions économiques et financières, des transgressions d'une autre nature, prenant appui sur Internet, sont apparues et tendent à se développer.

### Au mobile idéologique

Aux côtés du défi technique apparaît également un mobile idéologique qui peut s'avérer supérieur au mobile financier et constituer la motivation véritable de l'auteur de l'infraction, la raison même de son acte. C'est le cas pour la cybercriminalité de combat reposant sur un engagement dont l'objectif premier est d'exposer des revendications.

Ainsi un certain nombre d'infractions commises dans le champ de la cybercriminalité relèvent de celui de la revendication politique. C'est le cas notamment pour les « saturations » de sites internet qui sont ainsi rendus indisponibles en raison de requêtes en grand nombre par déni de service, attaques permettant de prendre le contrôle à distance d'ordinateurs « zombies » reliés entre eux (« botnets »). Ces attaques peuvent porter sur des sites gouvernementaux, par exemple en signe de protestation contre un projet de loi ; elles peuvent également se traduire par la diffusion de données personnelles relatives à des personnages publics, des entreprises ou des

personnes influentes appartenant à des groupes que les auteurs veulent mettre en cause. Elles sont dirigées contre la puissance publique, l'État ou ses représentants (par exemple stigmatisation de policiers ou de partis politiques) ou contre des entreprises, des puissances économiques (notamment mise en cause de dirigeants, de modes de production, d'activité particulière, révélation de chiffres d'affaires ou de rémunérations).

Certaines de ces attaques peuvent entraîner des défigurations de sites comme les actes revendiqués par la nébuleuse « anonymous » pour des mobiles idéologiques plus ou moins précis et compréhensibles.

De même, les revendications de libre accès à la culture qui impliquent la mise en ligne sur des sites dédiés de musiques, de films ou de logiciels au mépris des droits d'auteur s'inscrivent également dans cette catégorie. L'objectif proclamé est alors de diffuser des œuvres contrefaites au nom de la « culture pour tous ». Ces infractions qui, grâce au vecteur internet, atteignent une dimension nouvelle, touchent particulièrement les entreprises œuvrant dans le domaine culturel.

Enfin, les atteintes aux intérêts fondamentaux ou aux opérateurs d'importance vitale peuvent également constituer des mobiles de la « cyberdélinquance ». Le Code de la défense<sup>9</sup> définit ces opérateurs principalement à travers leurs activités de distribution de biens ou de services indispensables, de maintien du potentiel de défense, ou de sécurité de la nation. Ainsi en est-il des agissements visant aux exfiltrations de données nationales ou touchant aux intérêts supérieurs de l'État, notamment

LE DÉFI TECHNIQUE EST  
SOUVENT MIS EN AVANT  
PAR LES AUTEURS POUR  
JUSTIFIER DES ACTES  
REVENDIQUÉS SUR  
INTERNET. COMMETTRE  
DE TELLES INFRACTIONS  
PERMET À LEURS  
AUTEURS D'ACQUÉRIR  
PUIS DE CONFORTER  
UNE RÉPUTATION DE  
« HACKEURS » EFFICACES  
ET DE VALORISER DES  
ACTES QUI NE SONT PAS  
CONSIDÉRÉS SUR LA TOILE  
COMME DÉLICTEUX.

(9) - L'article R1332-2 du Code de la défense dispose que « I. Les opérateurs d'importance vitale sont désignés parmi : 1° Les opérateurs publics ou privés mentionnés à l'article L. 1332-1 ;

2° Les gestionnaires d'établissements mentionnés à l'article L. 1332-2.

II.- Un opérateur d'importance vitale :

1° Exerce des activités mentionnées à l'article R. 1332-2 et comprises dans un secteur d'activités d'importance vitale ;

2° Gère ou utilise au titre de cette activité un ou des établissements ou ouvrages, une ou des installations dont le dommage ou l'indisponibilité ou la destruction par suite d'un acte de malveillance, de sabotage ou de terrorisme risquerait, directement ou indirectement :

a) D'obérer gravement le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ;

b) Ou de mettre gravement en cause la santé ou la vie de la population ».

L'article R1332-2 du Code de la défense précise qu'« un secteur d'activités d'importance vitale, mentionné au 1° du II de l'article R. 1332-1, est constitué d'activités concourant à un même objectif, qui :

1° Ont trait à la production et la distribution de biens ou de services indispensables :

a) À la satisfaction des besoins essentiels pour la vie des populations ;

(suite page suivante)

à travers la récupération et l'exfiltration de données touchant à la sécurité nationale ou aboutissant à rendre inaccessibles par saturation des sites gouvernementaux (plusieurs sites étant susceptibles d'être hébergés sur le même serveur, ce qui implique qu'ils peuvent « tomber » en même temps). Lorsqu'il s'agit d'opérateurs d'importance vitale, c'est bien entendu la sécurité de la nation qui est visée, mais également la société ou l'entreprise qui en est la garante.

Qu'elle poursuive un mobile pécuniaire ou une revendication politique, la cybercriminalité nécessite la plupart du temps des techniciens pour sa mise en œuvre. La technique utilisée conduit ainsi à affaiblir significativement

les entreprises, même si le préjudice financier et matériel engendré n'était pas la finalité première recherchée par les auteurs. Ces comportements entraînaient jusqu'à une époque récente une faible répression, les tribunaux ne prenant pas toujours la mesure de la dangerosité de tels agissements et de l'importance des préjudices engendrés. Ceci tend cependant à évoluer et les sanctions prises sont de plus en plus sévères au regard notamment du développement de la cybercriminalité en lien avec les affaires de radicalisation et de terrorisme sur Internet susceptibles de prendre des entreprises pour cibles ■

---

(suite 9) b) Ou à l'exercice de l'autorité de l'État ;

c) Ou au fonctionnement de l'économie ;

d) Ou au maintien du potentiel de défense ;

e) Ou à la sécurité de la Nation,

dès lors que ces activités sont difficilement substituables ou remplaçables ;

2° Ou peuvent présenter un danger grave pour la population.

Le Premier ministre fixe, par arrêté pris après avis de la commission mentionnée à l'article R. 1332-10, les secteurs d'activités d'importance vitale. Cet arrêté désigne pour chaque secteur d'activités d'importance vitale un ministre coordonnateur qui veille à l'application des directives du gouvernement dans ce secteur, le cas échéant en liaison avec le ou les ministres dont le domaine de compétence recouvre les activités qui y sont exercées ».

Le ministre de la Défense est le ministre coordonnateur des secteurs d'activités d'importance vitale constitués d'activités qui participent de façon directe à la satisfaction des besoins des armées et des formations rattachées.



## Les atteintes à la réputation

Christian HARBULOT, Augustin ROCH, Artus HUOT De SAINT ALBIN

### Christian HARBULOT



Directeur de l'École de guerre économique et directeur associé du cabinet Spin Partners.

cabinet Spin Partners.

### Augustin ROCH



Responsable du Pôle Études chez Spin Partners.

Docteur en science politique, il est diplômé de l'École de guerre économique.

### Artus HUOT De SAINT ALBIN



Consultant chez Spin Partners. Diplômé de l'École de guerre économique.

La question de la réputation devient un problème récurrent dans la manière de gérer l'image d'une entreprise. L'émergence d'un monde immatériel dominé par la société de l'information crée de nouvelles vulnérabilités. Au cours des vingt dernières années, Internet et le développement des réseaux sociaux ont modifié l'environnement informationnel des entreprises. La société civile est devenue un interlocuteur à part entière en raison des démarches intrusives menées par des protestataires, des associations de consommateurs, des organisations non gouvernementales ou des salariés mécontents. Les acteurs économiques qui sont mis

sur la sellette se retrouvent en position de juge et partie et sont, la plupart du temps, enfermés dans une posture de justification à l'égard des médias. Comme le fait justement remarquer Bastien Ducournau, un de nos étudiants professionnels qui a travaillé sur le cas Greenpeace contre Leclerc, Leclerc sait que l'on peut avoir réglementairement et juridiquement raison mais médiatiquement tort, surtout contre des ONG. Les entreprises ont aujourd'hui le plus grand mal à faire entendre leur voix pour s'expliquer lors d'une crise informationnelle qui affecte leur image et leur réputation technologique ou commerciale. La démonstration scientifique qui servait d'élément d'arbitrage est de moins en moins audible. Les opposants et les protestataires utilisent le langage du parler vrai et ont déplacé le problème sur le terrain de la polémique. Ce décalage entre le monde

de l'entreprise et la société civile peut s'avérer très nuisible à terme si les pouvoirs publics et les différentes parties prenantes n'y prennent pas garde. Cet article s'appuie sur deux études de cas qui illustrent cette problématique et soulignent l'importance du savoir-faire pour gérer ce type de situation.

## Première étude de cas

### La notoriété sociétale comme instrument d'intimidation

La période préparatoire de la 21<sup>e</sup> Conférence des parties de la convention cadre des Nations unies sur les changements climatiques de 2015 (COP21) a été l'objet de nombreux messages<sup>1</sup> multi-supports en faveur de l'environnement, considéré comme un terreau fertile, pour lancer une attaque qui s'inscrirait dans une dimension environnementale porteuse en termes de retombées médiatiques. C'est dans ce contexte que Greenpeace a conçu et mis en application une campagne contre les hypermarchés E. Leclerc sur le thème de l'utilisation des pesticides dans l'agriculture. Cette opération s'inscrit dans un plan de communication de la campagne européenne « I know who grew it » que la multinationale verte a lancée simultanément.

### Une attaque éclair

Le processus de mise en accusation démarre le jeudi matin 15 octobre par une opération militante. Sept tonnes de terre sont déversées devant l'entrée de la SOCAMIL, une centrale d'achats de Leclerc installée à Tournefeuille, près de Toulouse. L'opération se poursuit le samedi 17 octobre. Des militants distribuent des tracts devant les entrées d'hypermarchés Leclerc dans seize villes de l'hexagone. Le samedi 24 octobre, Greenpeace accroche une banderole de 200 m<sup>2</sup> sur la façade d'un hypermarché près de Toulouse. Le mardi 27 octobre, des militants bloquent l'accès de la SOCAMIL aux camions jusqu'au lendemain. La campagne de Greenpeace, qui part en guerre contre Leclerc, aura duré douze jours pour quatre actions.

L'étude de ces dernières nous permet d'établir la cartographie des moyens utilisés :

- humains : l'organisation, forte de ses 3,2 millions de membres, n'aura mobilisé ponctuellement qu'une demi-

douzaine de militants locaux, et jusqu'à quarante, lors du dernier blocage de la SOCAMIL (le recouplement de différentes photos des événements permet d'ailleurs d'observer que certains militants ont participé à plusieurs actions) ;

- matériels : tracts, banderoles, équipements de rappel et terre déposée devant la SOCAMIL.

Cette économie de moyens fait écho à une impressionnante caisse de résonance médiatique. Les quatre actions de Greenpeace seront immédiatement reprises par plus de douze journaux et radios. D'abord régional (France bleu, France 3, Ouest France...), le relais médiatique devient très vite national (*Les Échos*, *Le Parisien*, *Le Figaro*, *Paris Match*, Europe 1, *Libération*, RTL). Le message relayé est exclusivement celui de Greenpeace. Sur Internet, ce message est également relayé, en plus des médias déjà mentionnés, par la page de Greenpeace France qui permet dès son accueil, en un clic, d'envoyer un e-mail au PDG de l'enseigne, personnellement nommé et visé.

### La réaction de Leclerc

Leclerc a riposté en trois phases :

1. Tout d'abord en déclarant aller déjà au-delà des réglementations françaises et européennes en vigueur quant à l'utilisation des pesticides avec une démarche visant à limiter au maximum le recours aux produits phytosanitaires, par la mise en œuvre de bonnes pratiques de culture et de moyens de lutte intégrés ;
2. Puis par la voie juridique, le 27 octobre, au travers d'un référé d'heure à heure, un outil très efficace pour obtenir une ordonnance et débloquent des situations de crise très rapidement, souvent utilisé en matière de diffamation ou de droit à l'image ;
3. Enfin par un engagement « à réduire fortement l'usage des pesticides dans l'agriculture » et à « créer une Commission, [...] qui rencontrera dans les prochains jours une commission de travail de l'ONG afin d'élaborer ensemble un plan d'action ».

L'attaque lancée par Greenpeace repose sur un seul argument : le rapport « Pommes empoisonnées : mettre fin à la contamination des vergers par les pesticides grâce à l'agriculture écologique » produit, en mai 2015, par la branche française de l'ONG et largement repris par la presse. À la suite de sa publication, Greenpeace a été

(1) Le petit film d'autodérision de Nicolas Hulot avec son « Break The Internet », réalisé à l'aide de Youtubers français, ou encore les spots vidéo d'entreprises, les articles ou le packaging refondu pour présenter des valeurs « COP 21 ».

attaqué en référé sur l'expression « *pommes empoisonnées* » par l'Association nationale pommes poires (ANPP).

L'association UFC-Que Choisir relance le débat : « Quand l'avocat de Greenpeace démolit les rapports... de Greenpeace ». « *Concernant les pommes, la ligne de Greenpeace est difficile à suivre. En mai 2015, la branche française de l'ONG a sorti un rapport dont le titre était "Pommes empoisonnées : mettre fin à la contamination des vergers par les pesticides grâce à l'agriculture écologique". Il a été largement repris par la presse. L'Association nationale pommes poires (ANPP) a attaqué Greenpeace en référé sur l'expression « pommes empoisonnées ». À la lecture, il apparaissait que Greenpeace n'avait en fait analysé aucune pomme. Tout était basé sur des prélèvements d'eau et de sol faits dans des vergers au printemps, alors que les arbres étaient en fleurs. L'audience s'est tenue en tout petit comité dans le bureau d'une juge du tribunal de grande instance de Paris, le 6 octobre. L'avocat de Greenpeace, M<sup>e</sup> Alexandre Faro, a développé une défense déconcertante. Selon lui, le but de Greenpeace "n'est évidemment pas de dénigrer ni les qualités, ni les propriétés des pommes". D'ailleurs, "l'ANPP ne peut pas sérieusement prétendre que ce rapport [celui de Greenpeace, NDLR] se voudrait objectif, informatif voire scientifique"! L'avocat l'a écrit dans ses conclusions. Manifestement, il était à court d'arguments pour justifier le titre "pommes empoisonnées". Devant le juge, M<sup>e</sup> Faro a fait un parallèle entre le rapport de Greenpeace et le dessin animé "Blanche-Neige", entre les pommes du titre et celle de la sorcière, suggérant que le but, dans les deux cas, était de frapper par une sorte d'allégorie les esprits des consommateurs. Fin octobre, sur son site, Greenpeace insistait pourtant encore, et lourdement, sur la valeur et le sérieux scientifique de ses mesures... Interrogée, Anaïs Fourest admet une certaine "complexité" »<sup>2</sup>.*

En offrant à Greenpeace l'engagement de principe de discuter avec l'ONG, alors qu'elle avait auparavant refusé tout dialogue, l'enseigne Leclerc fait une concession qui ne lui coûtera rien, mais permet à Greenpeace de clore avec les honneurs sa campagne éclair, tout en évitant le volet de réaction rapide juridique enclenché en parallèle. Cette forme de sortie de crise souligne la difficulté d'une entreprise à assumer publiquement une position défendable sur le fond, mais dans un rapport de force informationnel qu'elle juge défavorable en termes de communication.

## Deuxième étude de cas

### Le doute comme stratégie d'influence

En 1948, l'American Petroleum Institute (API<sup>3</sup>) prend connaissance des résultats d'une étude commandée à un professeur de l'Université de Harvard sur les dangers du benzène. Le verdict est clair : « *la seule concentration absolument sûre d'exposition au benzène est de zéro*<sup>4</sup> ». Or, le benzène est présent dans les carburants, dans la fabrication de plastiques, de pesticides, de cigarettes, de parfums, de médicaments... et des milliers de travailleurs y sont exposés quotidiennement. Par conséquent, éradiquer totalement son utilisation engendrerait des coûts extrêmement élevés pour les industriels.

L'API met alors en œuvre différentes actions, au cours des décennies suivantes, afin de contrer les tentatives de contrôle, voire d'interdiction du benzène. Notamment, face aux arguments scientifiques avancés par les opposants, le lobby adopte plusieurs stratégies visant à créer le doute et ainsi neutraliser, voire discréditer la thèse adverse. Ces agissements sont finalement exposés en décembre 2014, lorsque le Center for Public Integrity (CPI<sup>5</sup>) publie plus de 20 000 pages de documents (mails, mémos, témoignages...) sur cette affaire, mêlant enjeux sanitaires, économiques et moraux.

Analyser le cas du benzène permet de comprendre les logiques d'influence, c'est-à-dire comment des acteurs ont utilisé l'information pour promouvoir leurs intérêts, discréditer leurs contradicteurs tout en façonnant l'environnement médiatique, scientifique et politique à leur profit, et ce, pendant plus de soixante ans. En effet, actuellement, le benzène est toujours un des produits chimiques les plus fabriqués aux États-Unis et dans le monde.

### Le benzène et la fabrique du doute

Face à l'émergence d'un argumentaire anti-benzène et de contradicteurs de plus en plus organisés et influents<sup>6</sup>,

(2) Source : <http://www.quechoisir.org/commerce/magasin-grande-surface/actualite-operation-leclerc-obscur-greenpeace-est-il-si-transparent>

(3) Sous sa désignation d'organisme de normalisation, l'API est surtout le lobby le plus important de l'industrie pétrochimique aux États-Unis, dépensant chaque année plusieurs millions de dollars pour défendre ses intérêts. The Center for Responsive Politics, *American Petroleum Institute*, note d'analyse mise à jour en février 2015. Disponible à l'adresse suivante : <https://www.opensecrets.org/lobby/firmsum.php?id=D000031493&year=2014>

(4) American Petroleum Institute (Department of Safety), *API Toxicological Review on Benzene*, Harvard School of Public Health, septembre 1948. L'étude est réalisée par le professeur Marshall Clinton.

(5) Basée à Washington, le Center for Public Integrity est une organisation de journalistes d'investigation, sans but lucratif, fondée en 1989 : <http://www.publicintegrity.org/>

(6) Loury (R.), 2014, « Benzène : la fabrique du doute au grand jour », *Le journal de l'environnement*, 5 décembre.

L'American Petroleum Institute met en œuvre différentes actions afin d'atténuer et/ou prévenir les critiques. Alors qu'originellement il privilégie d'ignorer les attaques ou choisit la réponse judiciaire quand celles-ci sont véhémentes, l'API comprend que cette stratégie doit être complétée d'une autre : la création d'un socle scientifique favorable à ses intérêts, donnant une légitimité à la production de benzène. L'American Petroleum Institute a successivement ignoré la controverse, puis l'a combattue devant les tribunaux pour enfin s'engager dans la mise en œuvre d'un contre-argumentaire, quoiqu'embryonnaire et essentiellement en réaction aux arguments des opposants.

### Une polémique ignorée jusqu'en 1977

Les premières critiques à l'encontre du benzène émergent en 1897, lorsqu'une étude, menée en Suède, démontre qu'il s'agit d'un poison<sup>7</sup>. En 1926 et 1928, d'autres chercheurs confirment l'existence d'un lien entre exposition au benzène, d'une part, et destruction de globules blancs et risque accru de leucémie, d'autre part. Aux États-Unis, les premières restrictions apparaissent en 1946, avec un seuil maximal de 100 parts par million (ppm). En 1948, ce taux est même abaissé à 35 alors que l'API assure qu'une exposition inférieure à 50 ppm reste recommandée. En 1950, un consultant de la compagnie pétrolière Shell (membre de l'API) rapporte, dans un mémo, que le benzène est « un cancérigène bien connu », ajoutant que les employés de l'entreprise s'interrogent de plus en plus sur les risques de cancer. Pourtant, aucune disposition n'est prise. En fait, l'American Petroleum Institute semble préférer ignorer le problème, malgré la multiplication des études sanitaires dans les années 1950 et 1960.

### 1977-1987 : première opposition entre pro et anti-benzène

En 1977, Peter Infante, membre du National Institute for Occupational Safety and Health (NIOSH)<sup>8</sup>, réalise une étude au sein d'une usine Goodyear en Ohio<sup>9</sup>. Il constate que les travailleurs exposés à un taux de benzène de 10 ppm – soit la limite d'exposition autorisée – présentent un risque accru de cancer. En réponse, l'Occupational Safety and Health Administration (OSHA<sup>10</sup>) abaisse temporairement cette limite à 1 ppm, devenue permanente un an plus tard. En réponse, l'American Petroleum Institute saisit la justice et, après deux ans de procédure, la Cour suprême des États-Unis invalide la décision de l'OSHA. Il faut attendre 1987 pour que l'organisme américain renouvelle sa préconisation d'un taux à 1 ppm, suite à une pétition des syndicats de travailleurs. Ce qui pousse également la Cour suprême à revenir sur sa décision et entériner la limite d'exposition autorisée à 1 ppm<sup>11</sup>.

Ainsi, cette bataille juridique, marquée par les doutes de la justice et la mise en porte-à-faux de l'OSHA, illustre parfaitement l'opposition entre industriels et autorités sanitaires autour d'une incertitude scientifique<sup>12</sup>. Elle amène également l'API à changer de stratégie, dans le

but de créer un climat d'incertitude autour des méfaits du benzène.

### Disqualifier les thèses adverses : stratégie embryonnaire des années 1990

En 1990, l'American Petroleum Institute décide de mettre en place un programme de recherche dont le but, rapporté

ANALYSER LE CAS DU  
BENZÈNE PERMET DE  
COMPRENDRE LES  
LOGIQUES D'INFLUENCE,  
C'EST-À-DIRE COMMENT  
DES ACTEURS ONT UTILISÉ  
L'INFORMATION POUR  
PROMOUVOIR LEURS  
INTÉRÊTS, DISCRÉDITER  
LEURS CONTRADICTEURS  
TOUT EN FAÇONNANT  
L'ENVIRONNEMENT  
MÉDIATIQUE, SCIENTIFIQUE  
ET POLITIQUE À LEUR  
PROFIT, ET CE, PENDANT  
PLUS DE SOIXANTE ANS.

(7) Le cabinet d'avocats américain Hissey Kientz propose une chronologie sur le benzène : <http://bit.ly/1zfCPQ2>

(8) Le NIOSH est l'Institut national pour la sécurité et la santé au travail, une agence fédérale américaine.

(9) Infante (P.) et Alii, 1977, « Leukemia in benzene workers », *The Lancet*, Volume 310, n° 8028, juillet.

(10) L'OSHA est l'Administration pour la sécurité et la santé au travail, agence dépendant directement du ministère du Travail.

(11) Rom (W.N.), Markowitz (S.), 2006, *Environmental And Occupational Medicine*, Lippincott Williams & Wilkins, 4<sup>e</sup> édition, mai, p. 1652.

(12) Lombardi (K.), 2014, « Benzene and worker cancers: 'An American tragedy' », *The Center for Public Integrity*, 4 décembre. Sauf indication, toutes les citations ci-après sont tirées de cette enquête.

dans un mémo interne, est « *d'améliorer l'évaluation des risques et influencer la réglementation* », c'est-à-dire surveiller et contrer les travaux défavorables à ses intérêts. Un résultat éclairant de cette stratégie concerne l'étude du National Cancer Institute<sup>13</sup> sur la dangerosité d'une exposition au benzène au taux maximal autorisé par l'OSHA (soit 1 ppm). Les résultats, publiés en 1997, attestent non seulement d'un risque accru de contracter une leucémie, mais aussi d'autres maladies.

L'API réagit rapidement et propose 25 000 dollars à Otto Wong<sup>14</sup>, un épidémiologiste californien<sup>15</sup>, pour réaliser « une analyse critique » de l'étude. Dans un rapport d'une dizaine de pages, le scientifique dénonce plusieurs incohérences et approximations, affirmant que les conclusions « *sont peu fiables*<sup>16</sup> ». Ainsi, l'analyse d'Otto Wong sème suffisamment le doute pour que l'étude du National Cancer Institute ne soit pas prise en compte par l'agence américaine de protection de l'environnement.

Toutefois, l'API a bien conscience que cette stratégie reste une solution de court terme : elle est essentiellement dans la réaction face aux attaques des opposants, dans la justification permanente. Or, l'enjeu pour l'API est désormais d'alimenter le doute sur le long terme, c'est-à-dire de parasiter au maximum le débat scientifique en favorisant l'émergence d'études à contre-courant de celles menées par les organismes sanitaires.

## La bataille autour de la question de la légitimité scientifique

En 1999, l'American Petroleum Institute décide de réaliser une étude similaire à celle du National Cancer Institute – non pas aux États-Unis mais en Chine, sur des ouvriers de Shanghai – et qui lui servira de base scientifique pour contrer les opposants. Pour réaliser cette étude, qui doit

durer cinq ans, l'API fait appel à Otto Wong et à Richard Irons<sup>17</sup>, chercheurs avec qui elle a déjà travaillé par le passé. Par ailleurs, pour coordonner l'étude, l'API crée en 2001 le Benzene Health Research Consortium<sup>18</sup>. Celui-ci, dans une note publiée peu avant le début de l'étude, en détermine les trois objectifs :

- « *Fournir un fort soutien scientifique quant à l'absence de risque de développer une leucémie lors d'une exposition au taux actuel de benzène [1 ppm]* » ;

- « *Établir que la limite d'exposition autorisée ne fait peser aucun risque significatif* » ;

- « *Réfuter les allégations selon lesquelles l'exposition au benzène provoquerait des cancers autres que des leucémies* ».

En outre, afin de contrecarrer toute critique concernant l'intégrité des scientifiques et les risques de suspicion, le Consortium cherche à crédibiliser au maximum l'étude. En effet, en finançant son propre projet, le Consortium doit faire face à deux défis : cacher ses véritables motivations et laisser penser que les travaux des chercheurs sont réalisés en toute indépendance. Concernant le premier point, les membres du Consortium s'accordent donc sur des éléments de langage. Tandis qu'en public le but de l'étude est « *de comprendre les dangers des produits fabriqués et vendus* », en privé, les membres évoquent plutôt « *l'exposition des travailleurs au benzène et, surtout, le risque de demandes d'indemnisation* ». Concernant l'indépendance de l'étude, le Consortium crée plusieurs comités, composés d'experts indépendants et chargés de superviser le travail de recherche.

En 2009, après huit ans de recherche et un budget final de 35 millions de dollars, l'étude de Shanghai conclut qu'il est avéré qu'une exposition au benzène induit le développement de cancers, mais de certains types seulement. Ce dernier point est important, car il souligne

(13) L'Institut national du cancer est un institut fédéral américain créé en 1937.

(14) À l'époque, Otto Wong est connu de l'industrie pétrochimique pour avoir réalisé plusieurs études à charge contre elle. Par exemple, en 1987, alors qu'il est chercheur au sein de l'entreprise Environmental Health Associates, il dénonce la surexposition au benzène. En 1991, dans une étude sur l'impact sanitaire du chlorure de vinyle, il critique fortement l'industrie pétrochimique... avant de se rétracter et de revenir sur ses conclusions les plus graves. Dans leur ouvrage intitulé *Deceit and denial: the deadly politics of industrial pollution*, David Rosner et Gerald Markowitz, deux professeurs spécialisés en santé publique, parlent à ce propos de « *l'un des cas les plus curieux d'autocorrection* », suggérant que le chercheur fut soumis à de fortes pressions pour revenir sur ses affirmations.

(15) Otto Wong est chef épidémiologiste dans la société Applied Health Sciences, Inc., basée à San Mateo. Il est également professeur dans les universités de La Nouvelle Orléans et de Hong Kong.

(16) Wong (O.), 1999, « *A critique of the exposure assessment in the epidemiologic study of benzene-exposed workers in China conducted by the Chinese Academy of Preventive Medicine and the US National Cancer Institute* », *Regulatory Toxicology and Pharmacology*, Vol. 30, Issue 3, décembre.

(17) Richard Irons, professeur de toxicologie à l'université du Colorado, a écrit de nombreux articles sur le benzène et ses enjeux sanitaires.

(18) Le Consortium est financé par Shell, ExxonMobil, Chevron, ConocoPhillips et BP. Dow Chemical, pourtant membre de l'API, a refusé de participer, craignant que l'étude ne soit biaisée.

la stratégie de l'API : concéder les faits avérés<sup>19</sup> pour mieux préserver ce qui peut l'être. Ainsi, si l'étude précise les types de cancers causés par le benzène, elle devient un argumentaire précieux afin de dédouaner les fabricants dans un certain nombre de poursuites judiciaires. Dans les faits, l'étude subdivise au maximum les types de cancers, rendant certains statistiquement trop insignifiants pour être reliés au benzène. Cela génère ainsi le doute, ce qui représente la clé lors de procès pour empoisonnement.

Ainsi, en favorisant l'émergence d'une contre-offre informationnelle minimisant la plupart des effets du benzène, l'API remplit son objectif qui est de saper le socle scientifique sur lequel reposent les principales attaques.

### Faire douter pour influencer

Le doute est la stratégie d'influence la plus communément appliquée à travers le temps. En effet, elle consiste à amener la cible à s'interroger, à réfléchir, c'est-à-dire à sortir de son schéma de pensée et à redéfinir sa position quant à la problématique posée.

Le cas benzène démontre la capacité des industriels à façonner leur environnement au travers d'un contre-argumentaire efficace, lui-même s'appuyant sur un socle scientifique robuste (bien que discutable dans sa création). Ainsi, les résultats parlent d'eux-mêmes : la production de benzène est toujours autorisée, les procès minimisés et les opposants sont durablement fragilisés (leurs arguments ne portent plus).

Toutefois, cette stratégie élaborée n'est en aucun cas singulière. En effet, elle a également été appliquée par les industriels du tabac ou de l'amiante, qui sont des exemples particulièrement éclairants<sup>20</sup>, de même que le débat actuel

sur la fracturation hydraulique aux États-Unis ou dans d'autres pays<sup>21</sup>.

Douter a, dans nos sociétés, un caractère péjoratif. Il a pourtant un aspect positif essentiel, mais souvent occulté. En effet, douter, c'est ne pas être sûr de l'authenticité de quelque chose, de sa réalité, de sa vérité. Il y donc derrière le doute une réflexion pour atteindre cette vérité. Mais faire douter ? Dans ce cas-là, celui qui veut faire douter cherche à donner sa vérité, c'est-à-dire sa perception des choses. Or, celle-ci peut être sincère ou malhonnête. Le doute peut donc être manipulateur, opposé à l'objectif de « faire réfléchir » (vision positive visant à s'élever).

LE DOUTE EST LA STRATÉGIE D'INFLUENCE LA PLUS COMMUNÉMENT APPLIQUÉE À TRAVERS LE TEMPS. EN EFFET, ELLE CONSISTE À AMENER LA CIBLE À S'INTERROGER, À RÉFLÉCHIR, C'EST-À-DIRE À SORTIR DE SON SCHÉMA DE PENSÉE ET À REDÉFINIR SA POSITION QUANT À LA PROBLÉMATIQUE POSÉE.

Faire douter permet ainsi de déstabiliser l'autre, plus précisément sa pensée, donc son action. On est ainsi en plein cœur de l'influence. En effet, pour Alain Juillet, ancien haut responsable à l'Intelligence économique, « *l'influence, c'est un moyen d'amener ceux auxquels on s'adresse à envisager une autre vision des choses. [...] C'est amener celui que l'on veut influencer à changer son paradigme de pensée, à modifier ses fondamentaux. [...] L'influence, elle, consiste à amener l'auditeur à sortir de son schéma de pensée pour aller vers un autre. Ce changement est produit par des éléments qu'on lui présente et qui l'amènent à réfléchir. [...] Parce que l'influence fait appel à la capacité d'analyse de l'auditeur, qui doit faire le tri entre ce qu'il pense "habituellement" et les éléments nouveaux qui lui sont soumis, dont il lui appartient de mesurer la validité. Tout argument solide qui lui est proposé peut ainsi le conduire à revoir son jugement, donc son positionnement. C'est à partir de là que s'enclenche le processus de l'influence*<sup>22</sup> ».

Les outils numériques disponibles aujourd'hui permettent aux acteurs (États, entreprises et individus) de propager analyses de qualité ou contenus délibérément orientés et biaisés – voire des canulars – afin de promouvoir leur point de vue et donc leurs intérêts. Le contexte contemporain

(19) Une deuxième étude menée en 2004 par le National Cancer Institute établit déjà un lien entre exposition au benzène et risque de développer un cancer, et ce, même à un taux d'exposition inférieur à 1 ppm.

(20) Oreskes (N.), Conway (E.M.), 2012, *Les Marchands de doute : ou comment une poignée de scientifiques ont masqué la vérité sur des enjeux de société tels que le tabagisme et le réchauffement climatique*, Paris, Éditions Le Pommier.

(21) Schiffman (R.), 2013, « 'Frackademia': how Big Gas bought research on hydraulic fracturing », *The Guardian*, 9 janvier.

(22) Comes Communication, « Stratégies d'influence, le décryptage d'Alain Juillet », *Communication & Influence*, hors-série n° 1, juin 2009.

est donc un monde de rapports de force informationnels où chacun cherche à imposer sa vision des choses : non pas de manière autoritaire, mais par l'influence, en faisant douter les protagonistes. Par exemple, cela peut se manifester sur le terrain diplomatique (comme sur le conflit entre la Russie et l'Ukraine), sur le terrain politique entre des candidats à une élection, ou encore sur le terrain concurrentiel (exemple du *bad buzz* sur les McDonald's non halal dans les pays musulmans<sup>23</sup>).

Par ailleurs, au-delà de ce foisonnement d'argumentaires, ce nouvel environnement informationnel est marqué par une évolution du périmètre des acteurs à influencer. Ainsi, tandis que l'American Petroleum Institute, les fabricants de tabac ou les professionnels de l'amiante dirigeaient exclusivement leurs efforts à destination des décideurs politiques, il est désormais nécessaire de prendre en compte la société civile, dont l'opinion et la capacité d'actions facilitée par la révolution Internet peuvent dorénavant orienter les choix des politiques. L'exemple du débat sur la fracturation hydraulique est éclairant à ce sujet. En effet, les industriels du secteur ne cherchent pas tant à convaincre le législateur que les citoyens dans les zones d'exploration-production, où les réticences concernant le gaz de schiste sont les plus fortes.

## Conclusion

La stratégie menée par l'American Petroleum Institute durant plusieurs décennies met en lumière les pratiques d'influence de grandes organisations afin de minimiser tout discours négatif, contrecarrer les procès et renforcer leurs positions vis-à-vis de produits concurrents ou de possibles législations contraignantes. Surtout, cette

stratégie s'appuie sur le doute, fabriqué et orchestré, ce qui en soit n'est pas inhabituel. En effet, divers exemples pourraient être cités, quelles que soient les époques, les pays ou les problématiques (sanitaires, économiques...). Avec l'avènement d'Internet, la mise en œuvre de ce type de stratégie se transforme. En permettant effectivement aux individus et organisations de toutes tailles de faire la promotion de leurs arguments, Internet redéfinit la place et les rôles de chacun dans le sens où la création, la maîtrise et la diffusion d'informations ne sont plus l'apanage de grandes organisations ou de personnes faisant autorité.

Dorénavant, tout individu n'est plus seulement consommateur mais également producteur d'informations (certains diront même producteur de connaissances) : il est à la fois une cible et un relais d'influence. Ainsi, les personnes ou organisations qui faisaient autorité par le passé, parce qu'elles détenaient le savoir, sont graduellement mises en concurrence par d'autres sources d'information, tout aussi légitimes.

Néanmoins, s'imposer comme la source de référence dans son environnement n'est pas une chose aisée. Cela ne peut se réaliser que sur le temps long, car les schémas de pensée des acteurs en présence ne changent pas de manière instantanée. Aussi, Internet induit l'avènement d'un monde où le doute est généralisé et où il faut (ré)apprendre à douter, c'est-à-dire à chercher la (une) vérité. Il est intéressant de noter que des ONG comme Greenpeace qui cherchent à dénoncer les excès ou les erreurs commises par des groupes industriels recourent à des démarches informationnelles qui, par manque de fondement scientifique, peuvent être assimilées dans certains cas à de la pression psychologique ■

(23) Kanz (A.), 2013, 'McDonald's non halal': haro sur le bad buzz en Malaisie, 16 septembre.



© pico - Fotolia.com

## Le patriotisme économique

Bernard CARAYON

Issue, paraît-il, d'une moquerie d'Alphonse Allais à l'endroit de l'esprit cocardier de Paul Déroulède, l'expression de « patriotisme économique » n'est guère utilisée avant 2003<sup>1</sup> : le Premier ministre, Lionel Jospin, au lendemain des attentats du 11 septembre, appelle les entreprises françaises, au nom du « patriotisme économique », à maintenir leurs investissements, appel qu'Edouard Balladur juge « utile » à condition que son gouvernement renonce aux 35 heures. Longtemps ignorée par la classe politique, les universitaires et les journalistes, l'expression

est mobilisée par un autre Premier ministre, Dominique de Villepin, en juillet 2005, alors qu'une rumeur d'offre publique d'achat (OPA) hostile de Pepsi sur Danone se répand dans Paris. Utilisé, à mon sens, improprement au bénéfice d'une entreprise qui n'était ni stratégique ni menacée, le patriotisme économique constitue l'adossement de la politique publique française d'intelligence économique que je conçois, à la demande du gouvernement de Jean-Pierre Raffarin, au lendemain de l'affaire Gemplus. Une affaire qui avait légitimement traumatisé les pouvoirs publics.

J'y consacre un livre<sup>2</sup> où je dénonce notamment l'obsession des années 1990, présentées comme le début de la « *fin de*

(1) Cf. mon rapport au Premier ministre, 2003, « Intelligence économique, compétitivité et cohésion sociale », p. 11. « *Sans paranoïa ni panique, il est temps de réagir et, tout simplement, de réaliser "trois mariages et un enterrement"* : le mariage entre les administrations publiques, le mariage entre le public et le privé et le mariage de l'information blanche avec celle qui l'est un petit peu moins... L'enterrement alors, sera, celui des naïvetés françaises ! Que cette politique soit nationale, décentralisée ou internationale, elle ne pourra s'épargner un effort de formation et d'information calibré à cette ambition et adapté à une certitude : l'intelligence économique est un patriotisme économique. Je devine le sourire du lecteur à la découverte de ces mots. Que notre tropisme soit notre région, notre pays ou l'Europe, c'est pourtant ce patriotisme économique qui sera le garant de notre cohésion sociale. S'il n'en est convaincu par sa réflexion propre, qu'il examine, sans parti-pris, comment nos grands partenaires se comportent et réussissent. Le patriotisme économique n'est pas une idéologie, pas plus que l'intelligence économique n'est un concept : c'est une politique sociale. »

(2) 2006, *Patriotisme économique, de la guerre à la paix économique*, Paris, éd. du Rocher.

**Bernard CARAYON**



Ancien député (UMP) du Tarn, maire de Lavaur, avocat et

maître de conférences à Sciences-Po Paris, président de la Fondation Prometheus.

*l'Histoire* » (Francis Fukuyama) et de la « *destruction des États-nations* », jugée comme un « *bienfait pour l'Humanité* » par l'opinion libérale dominante<sup>3</sup>. Le débat sur le « patriotisme économique » est relancé à la faveur de la préparation par l'État d'un dispositif juridique de protection des secteurs sensibles de l'économie, qui suscite une violente hostilité de la Commission européenne. Les affaires Mittal puis Enel conduisent le gouvernement à renforcer l'épargne salariale et Dominique de Villepin à souligner que la politique économique française consiste à vouloir « *lutter à armes égales* » – titre de mon second rapport<sup>4</sup> – dans la compétition internationale. Un projet de loi anti-OPA, qui introduit un mécanisme de « pilule empoisonnée » est adopté, avec le soutien de l'opposition parlementaire.

Arnaud Montebourg, ministre du Redressement productif, relance l'expression quelques années plus tard, et pose en marinière afin de promouvoir le « made in France ».

Longtemps, et bien souvent encore confondu avec le protectionnisme, le patriotisme économique a pourtant été défendu par l'ancien défenseur attitré du libre-échange, Pascal Lamy, l'ancien directeur général de l'OMC<sup>5</sup> : « *Je n'ai rien contre le patriotisme économique* », assurait-il sur *Europe 1*. « *Par contre, si ça doit se transformer en protectionnisme patriotique, alors là non, parce que l'économie internationale aujourd'hui suppose que pour bien exporter, vous importiez plus* »<sup>6</sup>.

Enfin ! Cette déclaration, qui n'a fait, à l'époque, l'objet d'aucun commentaire des thuriféraires du libre-échange, constitue une vraie victoire politique pour ceux qui, depuis dix ans, plaident pour la défense, sans naïveté ni paranoïa, de nos intérêts nationaux et européens, mais dans le respect des règles internationales, sous condition de réciprocité.

Les mots, en ce domaine, pèsent lourd : selon l'expression du philosophe français Brice Parain, « *ils sont des pistolets chargés* ». En promouvant le « patriotisme économique », je me suis heurté aux sarcasmes ou aux critiques de ceux qui, volontairement ou non, confondaient patriotisme et nationalisme (quand on veut noyer son chien, on l'accuse de la rage !), et prêchaient dans la paix des cimetières de nos emplois le respect dogmatique et unilatéral des règles du marché. Des règles contournées partout allègrement, mais qui trouvent chez nous autant de complaisance que de cécité. Cécité des « libéraux » face aux méthodes internationales efficaces de nos concurrents anglo-

saxons... les plus libéraux ; cécité de l'État, incapable de penser une doctrine de sécurité économique ou une stratégie industrielle, et d'associer, dans l'anticipation, l'action et l'influence de nos entreprises ; cécité, souvent, des universitaires, prisonniers de leurs disciplines, des syndicats aussi, enfermés dans des logiques catégorielles.

Les Français ont la triste manie de traiter par l'idéologie les faits sociaux, chacun confrontant à l'autre la vision « purifiée » de son système. On a connu cela dans le passé quand le communisme trouvait chez nous des défenseurs, présentant le stalinisme comme son avatar et non comme son expression logique.

Libéralisme et socialisme ont ainsi leurs prêtres et leurs dogmes, leurs excommunications et leurs fidélités obsolètes. Un article du professeur Jacques Gareilo dans le *Figaro*<sup>7</sup> ne fait pas exception à la règle en dénonçant dans notre pays « *l'étatisme, la réglementation, la centralisation* », et dans le monde, le « *capitalisme frelaté* », celui des « *copains et des coquins* », la « *collusion entre le monde des affaires et les hommes de l'État* ». Il développe une vision éthérée du capitalisme, restaurant « *la créativité de l'être humain* », le « *sens du service de la communauté* », le « *libre-échange* »...

Parler de « guerre économique », c'était aussi pêcher par pessimisme, bellicisme ou anti-américanisme. Promouvoir le patriotisme économique relevait de la ringardise colbertiste alors que le patriotisme, « *c'est l'amour des siens, le nationalisme, la haine des autres* », écrivait Romain Gary. Et lors d'un colloque que j'avais organisé à l'Assemblée nationale en 2005, l'ambassadeur des États-Unis à Paris, Greg Stapelton, fervent républicain et libéral, avait déjà traité par l'ironie notre pudeur collective à l'égard du patriotisme : « *le patriotisme économique, nous connaissons très bien cela chez nous ; mais nous en parlons moins que nous ne le pratiquons* ». On observera que ce sont souvent d'ailleurs les mêmes personnes qui jugent ringard le patriotisme économique, et qui enfilent, les soirs où joue l'équipe de France de football, leur maillot bleu ! Le patriotisme économique dérange, en fait : ceux qui ne savent plus ce qu'est leur patrie – s'ils l'ont jamais aimée –, ceux aussi qui veulent purifier l'économie de toute influence politique, renonçant à construire la puissance et le rayonnement économiques de leur pays à travers le plus noble et le plus ancien des sentiments collectifs. Théoriciens d'un libéralisme de laboratoire, ils rêvent d'une mondialisation qui effacerait les États-nations, sacrifiant nos intérêts

(3) Salin (P.), 2000, *Libéralisme*, Paris, Odile Jacob.

(4) 2005, *À armes égales*, Rapport au Premier ministre, Paris, La documentation Française.

(5) Directeur général de l'Organisation mondiale du commerce du 1<sup>er</sup> septembre 2005 au 31 août 2013.

(6) 2012, *Le Point.fr*, 20 octobre.

(7) Gareilo (J.), 2013, « *Après l'échec du socialisme, si on essayait enfin le libéralisme ?* », *Le Figaro*, p. 16, 15 novembre.

et notre statut à l'intégrisme du tout-marché. « *Ab ! Les c... !* », comme disait Daladier de la foule qui l'accueillait à l'aéroport du Bourget, au retour des accords de Munich...

Un regard nouveau sur la mondialisation s'est pourtant, peu à peu, imposé au détriment de ces « bisounours ».

Depuis l'effondrement du bloc soviétique, la mondialisation nous avait été présentée comme pacifiée, dominée par le primat de la prospérité, le dogme du libre-échange et le nécessaire effacement des États-nations, pour le bonheur des peuples et la circulation sans entraves des hommes, des idées, des technologies et des capitaux. Une « *mondialisation heureuse* », selon l'expression – vraiment datée et fortement idéologique – d'Alain Minc.

La réalité est tout autre. Elle n'est pas dans l'alternative du paradis des ultralibéraux et de l'enfer des altermondialistes. Elle est celle du choc des puissances, du retour des frontières (sauf pour les réfugiés), de l'affirmation des intérêts des États-nations, de la guerre économique, expression qu'il fallait autrefois chuchoter, et que les médias, avec une hardiesse nouvelle, utilisent désormais sans guillemets !

Certains, à l'extrême gauche comme à droite, ont raillé la fameuse pose en marinier d'Arnaud Montebourg : elle partait pourtant d'un bon sentiment, et dans une civilisation de l'image, il ne faut pas toujours se priver des postures qui prêtent à sourire : le sac de riz sur l'épaule de Bernard Kouchner a popularisé l'engagement remarquable des « Médecins sans frontières ». Mais je ne suis pas convaincu que le consommateur soit, par nature, patriote. Dans un pays où il y a près de neuf millions de personnes vivant en dessous du seuil de pauvreté, le réflexe est à l'économie et non à la consommation de produits « bios » ou d'appellation contrôlée.

Le patriotisme économique s'adresse en fait moins aux consommateurs qu'à l'État. C'est l'État seul qui peut et doit distinguer les activités économiques où notre pays joue son destin (la défense, l'énergie, l'industrie pharmaceutique, l'aéronautique et le spatial, les technologies de l'information et de la communication) de celles qui ne génèrent « que »

prospérité et emplois. Les activités « stratégiques » sont mieux connues, mieux identifiées comme telles, après l'inlassable travail pédagogique conduit, en particulier, par la fondation que j'ai créée<sup>8</sup> il y a dix ans avec un parlementaire socialiste, Jean-Michel Boucheron. Ce sont ces secteurs industriels qui justifient de la part de l'État une meilleure protection juridique, technologique, financière, institutionnelle, politique. C'est là où l'action de l'État est, chez nous comme partout dans le monde, parfaitement légitime, parce que c'est là où nous jouons nos indépendances, nos émancipations, nos libertés et notre souveraineté.

Il reste encore beaucoup à faire pour ouvrir les yeux des dirigeants politiques, de gauche ou de droite, sur les réalités de la mondialisation, pour faire tomber les préjugés et faire litière des mauvaises solutions. L'effort doit être conduit en Europe, aussi, parce que l'Europe comme la France risquent de disparaître de l'Histoire. Quand la Commission européenne invoque les nécessités de la « compétitivité », nos grands concurrents ont fait le choix de la puissance, sans renoncer à aucun moyen d'y parvenir.

L'histoire est ancienne : l'Europe porte dans ses gènes – et dans le traité de Rome – sa « vassalité » à l'égard des États-Unis, comme l'illustre sa doctrine de la concurrence, aussi absurde qu'isolée dans le monde, interdisant les aides publiques sans distinguer les marchés stratégiques de ceux qui ne le sont pas, prohibant la concentration des entreprises européennes, quand il faudrait, au contraire, les encourager !

L'Europe semble bien avoir été conçue, hélas, pour défendre d'autres intérêts que les siens. Notre pauvre continent demeure le seul au monde aussi ouvert et offert aux vents, parfois dangereux, de la mondialisation.

Pourtant l'Europe, au-delà de son marché de consommateurs et de ses talents industriels et scientifiques, recèle une force qu'elle ne mobilise pas : celle de ses principes, d'un modèle politique et social fondé sur des normes sociales, éthiques et environnementales, à la légitimité incontestable. Plutôt que de vouloir ériger à nos frontières des murailles – qui ne résistent jamais, comme l'a montré l'Histoire – installons aux frontières

*Le patriotisme économique s'adresse en fait moins aux consommateurs qu'à l'État. C'est l'État seul qui peut et doit distinguer les activités économiques où notre pays joue son destin (la défense, l'énergie, l'industrie pharmaceutique, l'aéronautique et le spatial, les technologies de l'information et de la communication) de celles qui ne génèrent « que » prospérité et emplois.*

(8) [www.fondation-prometheus.org](http://www.fondation-prometheus.org)

de l'Europe des « filtres » précisément éthiques, sociaux, environnementaux. Battons-nous collectivement pour faire de la réciprocité un principe non pas relatif, mais absolu, régissant le commerce international.

L'Europe, c'est vrai, est divisée et ses intérêts épars. Elle a consommé beaucoup d'énergie à construire un marché unique : ne pourrait-elle se mobiliser pour promouvoir ses talents et défendre ses indépendances ? La question n'est pas théorique. Dès l'automne 1990, les Américains se saisissent pleinement du concept d'intelligence économique, sur la base d'une étude co-écrite par la Central Intelligence Agency (CIA) et le Rochester Institute of Technology. Baptisée « Japan 2000 DEFCON 1 », cette étude part de l'hyper-compétitivité japonaise avant d'affirmer que « *la connaissance deviendra le fondement primordial de la puissance économique* » ; c'est sur la base de ce rapport que l'Administration Clinton, à peine installée en 1992, voudra reproduire le modèle nippon d'un « *système politique d'agressivité commerciale institutionnalisée*<sup>9</sup> ».

Nous n'avons cessé d'être les témoins, au cours des dernières années, des ravages de la guerre économique en Europe et dans le monde : rachat d'entreprises stratégiques, et pillage technologique – à l'instar de Gemplus – par un fonds d'investissement qui place à sa tête un ancien administrateur du fonds de la CIA, In-Q-tel, ou de Pechiney, avalé par Alcan, bien vite déménagé outre-Atlantique ; industrie textile laminée par une concurrence nourrie de dumping fiscal et social ; positions aberrantes de la Commission européenne empêchant la constitution de groupes européens à taille mondiale (Schneider-Legrand) ; rachat d'Arcelor par Mittal présenté fallacieusement comme un groupe européen, démembrement d'Alstom au profit de Général Electric, scandales Wikileaks et Snowden, guerres monétaires ré-ouvertes, activisme des fonds vautours en Afrique et en Amérique du Sud, embargos contre l'Iran et la Russie imposés par les États-Unis à ses partenaires mais régulièrement contournés par eux-mêmes, condamnation de la BNP à une amende de neuf milliards de dollars sous couvert de l'extravagante extra-territorialité du droit américain, guerres et coups de force pour la maîtrise de l'énergie et des terres rares, construction de monopoles, en particulier dans les technologies de l'information et de la communication, autant de perversions d'un marché sans garde-fou, générant insécurités juridiques et financières, désordres, injustices et dépendances, aussi souvent brutaux que soigneusement dissimulés.

Notre patriotisme économique peut aussi s'adapter à une approche communautaire : par l'ouverture à nos partenaires des projets portés par le Grand emprunt, jadis lancé par le Président Sarkozy ; par la mise en place d'un « Small Business Act » en faveur des PME-PMI ; par une législation commune de sécurité économique ; par l'adaptation des textes communautaires sur la concurrence et notamment du critère du « marché pertinent » au marché mondial : il n'est pas indécent que les entreprises européennes se concentrent pour affronter leurs concurrents mondiaux, souvent devenus des géants.

Le « patriotisme économique » est la condition de notre indépendance et de notre cohésion sociale en France et en Europe, la promesse d'une intégration réussie dans la mondialisation.

C'est en fait une politique de « puissance » – un mot encore politiquement incorrect – nous affranchissant des tutelles dans les secteurs stratégiques, puissance faisant respecter nos valeurs : force du droit contre droit de la force, transparence contre opacité, réciprocité contre unilatéralisme. Puissance dénonçant les déloyautés de nos concurrents : interdiction d'OPA hostiles au Japon, subventions publiques massives à Boeing et Bombardier, contournement de la convention OCDE sur la corruption, subjectivité « organisée » des classements internationaux. Puissance, enfin, soumettant l'ouverture de nos marchés au respect de nos normes.

Le patriotisme économique, au fond, est bien mieux vécu et pratiqué à l'étranger, n'en déplaise à nos libéraux-pacifistes. Partout dans le monde, et surtout dans la grande patrie du libéralisme, les États-Unis, la puissance publique organise la protection de ses acteurs économiques majeurs ou symboliques, les accompagne dans la conquête des marchés mondiaux, pèse, dans les organisations internationales, sur l'élaboration des normes juridiques et des règles techniques, associe autour de stratégies collectives, entreprises, universités, ONG et fondations : l'Advocacy Center, administration publique, rassemble et trie l'information stratégique pour les entreprises américaines, le CFIUS<sup>10</sup> trie les investissements étrangers et peut leur opposer, sans cadre juridique, et donc, sans recours contentieux, au nom d'une seule notion – politique – la « sécurité américaine ». Nos libéraux protestent-ils ? Jamais. L'USAID<sup>11</sup>, sous couvert d'aide humanitaire, impose dans les pays détruits par la guerre ou la misère les entreprises américaines. 40 %

(9) Carayon (B.), 2006, *Patriotisme économique – De la guerre à la paix économique*, Paris, éditions du Rocher, p. 92-93.

(10) Comité sur l'investissement étranger aux États-Unis.

(11) Agence des États-Unis pour le développement international (United States Agency for International Development).

des ressources de la CIA et de la NSA sont consacrées au renseignement économique ou à la déstabilisation d'entreprises ou d'États. Une ONG, comme Transparency International, créée par le complexe militaro-industriel américain, élabore un indice de perception de la corruption dans la plus totale opacité afin de discréditer les concurrents des États-Unis. Avec leur *Buy American Act* (1933) et leur *Small Business Act* (1953), ceux-ci montrent la voie d'un soutien inconditionnel à leurs PME et de la protection des marchés publics nationaux<sup>12</sup>. Quand nous parlons de « compétitivité », les Américains parlent de « suprématie ». Sur le site de la Maison-Blanche...

L'État, paraît-il, ne serait pas légitime à intervenir sur le marché aux côtés des entreprises. Les faits ruinent cette assertion. Et ce n'est pas l'échec, ancien, du plan Calcul en France qui doit contredire cette nécessité pour l'État de se comporter en stratège, en anticipateur, en fédérateur, position qu'ont assumée jadis les politiques de Charles de Gaulle et Georges Pompidou. Quoi qu'on en dise souvent en France, les chefs d'entreprise ne sont pas attirés, le plus souvent, par la seule perspective du profit et tentés de désertir l'intérêt de leur pays. Mais l'action de l'État n'est pas toujours à la hauteur des difficultés qu'ils rencontrent...

Un faux argument rencontre un certain succès : le patriotisme économique exposerait notre pays à des mesures de rétorsion. Avons-nous été si patriotes dans le passé pour justifier d'être espionnés aussi méthodiquement et massivement, comme l'a révélé Edward Snowden ?

Les forts ne respectent que les forts : c'est une loi de l'histoire et une loi des comportements humains. Le patriotisme américain n'a jamais constitué un obstacle à la productivité, aux investissements étrangers et au dynamisme de l'industrie. Les Américains ont su empêcher en 2006 l'entreprise DP World (basée aux Émirats arabes unis) de racheter la société P & O, opératrice des principaux ports américains, sans craindre la moindre rétorsion des États évincés. Un exemple parmi des centaines d'autres. Mais sans susciter en Europe la moindre protestation des « libéraux ».

Ceux-ci nous expliquent aussi que le patriotisme économique sacrifierait l'intérêt du consommateur : mais qui peut opposer le consommateur au salarié et au citoyen ? Quel est le bilan social et industriel du rachat par le Canadien Alcan de notre industrie de l'aluminium ou d'Usinor par Mittal ? Les premiers salariés sacrifiés sur l'autel des restructurations sont toujours ceux des entreprises dont l'actionnariat est étranger...

Le vrai problème est bien aujourd'hui européen : on ne répète que ce que l'on croit ! La doctrine de la Commission européenne est stérile, en interdisant à nos entreprises toute concentration et toute aide publique. C'est précisément quand l'État s'assoit sur les traités européens, interprétés de manière théologique par la Commission, que l'on peut, comme il y a dix ans, sauver Alstom ou, en pleine crise financière, imposer un plan massif de consolidation des banques. Une crise où la Commission, justement, s'est tue dans l'impuissance.

Les libéraux contestent jusqu'à l'idée même d'une nationalité des entreprises : mais, dans le différend historique franco-américain sur l'Irak, les Américains n'avaient-ils pas engagé un boycott du groupe Sodexo, fortement implanté aux États-Unis et pourtant bien identifié comme français ? Que dire encore de la passivité des autorités communautaires face à l'anglo-saxonisation du droit et des normes qui pèsent sur la compétitivité de nos industries, de nos banques et de nos assurances ? Que dire de son silence gêné sur l'espionnage de nos dirigeants et de nos chefs d'entreprise ? Que dire de l'opacité du mandat de la Commission européenne pour négocier le TAFTA<sup>13</sup> avec les États-Unis ? Longtemps, la politique monétaire de la Banque centrale européenne n'a eu de politique que le nom. Son action récente montre que ses dirigeants ont enfin compris que l'amélioration de la parité euro-dollar était utile. Les États-Unis et la Chine, dont les monnaies sont faibles, ne sont-ils pas pour autant des puissances ? L'Europe, jusqu'à présent, s'est gargarisée de compétitivité alors qu'elle a pour vocation de devenir une puissance. Mais il est vrai, comme le soulignait Paul Valéry, qu'elle « *aspire visiblement à être gouvernée par une Commission américaine* » !

Si l'Europe et la France ne veulent pas disparaître de l'Histoire, il est urgent qu'elles trouvent enfin, dans la guerre économique, la force et l'intelligence de se battre à armes égales.

Le patriotisme économique exprime le primat du Politique, l'évidence que le capitalisme ne peut s'humaniser que s'il s'appuie sur des collectivités librement choisies<sup>14</sup>. Le Politique, c'est la démocratie ; le marché sans le Politique, c'est la jungle. Il faudrait décidément n'être ni démocrate, ni lucide, pour rester étranger au patriotisme économique ■

(12) 35 % seulement des marchés sont ouverts contre 85 % des marchés publics en Europe.

(13) Transatlantic Free Trade agreement.

(14) Lire sur ce sujet, *Changeons le monde*, Bernard Carayon, 2008, téléchargeable sur : <http://bit.ly/1XBymqQ>



# L'entreprise, coproductrice de la sécurité

Bertrand PAUVERT

**E**n 2006, à l'occasion de la parution du *Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, était rappelé le caractère « indispensable » d'une « politique de sécurité impliquant les entreprises des secteurs les plus sensibles<sup>1</sup> ». Témoignant d'une vision élargie des enjeux de sécurité et de défense, la consécration du concept de sécurité nationale par les Livres blancs de 2008 et 2013 conduisait à accorder une plus grande attention aux rapports entre la sécurité et les affaires économiques<sup>2</sup>; de fait, « si le *Livre blanc de 1994* n'évoquait que très rapidement la seule défense économique

et que l'opus de 2008 n'en soufflait mot, le *Livre blanc de 2013* y consacra au contraire trois pages pleines, attestant de la dimension aujourd'hui cardinale de la dimension économique de la sécurité nationale<sup>3</sup> ». La participation active des entreprises aux missions de sécurité a été trop souvent négligée et quand bien même cette préoccupation soit relativement récente dans le discours public, elle n'en est pas moins primordiale, car si la sécurité est bien l'affaire de tous, il est naturel d'y associer des structures privées comme les entreprises.

D'abord, dans une perception globale de la sécurité, la puissance publique ne peut rester indifférente aux entreprises composant le tissu économique du pays<sup>4</sup> et prendra des initiatives « d'une part pour protéger et défendre

Bertrand PAUVERT



Maître de conférences (HDR) en droit, il dirige le CERDACC (Centre

Européen de recherches sur le Risque, le Droit des Accidents Collectifs et des Catastrophes), à l'Université de Haute-Alsace (Mulhouse).

- (1) *La France face au terrorisme - Livre blanc du Gouvernement sur la sécurité intérieure face au terrorisme*, La doc. Française, 2006, p. 76.
- (2) On se permettra de renvoyer à notre étude, « 1972 - 2013 : Quarante ans de Livres Blanc, permanences et évolutions de l'impératif de Défense en France », *Le droit de la sécurité et de la défense en 2013*, Vallar (C.), Latour (X.) (dir.), 2014, PU Aix-Marseille, p. 51-62.
- (3) Pauvert (B.), 2015, « L'entreprise et la sécurité nationale », *Le droit de la sécurité et de la défense en 2014*, Gohin (O.), Pauvert (B.) (dir.), PU Aix-Marseille, p. 183-184 ; v. *Livre Blanc - Défense et sécurité nationale*, Direction de l'information légale et administrative, Paris, 2013, p. 105-107.
- (4) Les trois millions d'entreprises que compte la France représentent (pour les seules entreprises marchandes) 55 % du produit intérieur brut, pour un chiffre d'affaire atteignant près de quatre milliards d'euros ; v. INSEE, *Les entreprises en France*, éd. 2013, [www.insee.fr/fr/ffc/docs\\_ffc/ENTFRA13.pdf](http://www.insee.fr/fr/ffc/docs_ffc/ENTFRA13.pdf), p. 126.

*l'économie et les entreprises des atteintes de toute nature et, d'autre part, pour subvenir aux besoins de la défense nationale*<sup>5</sup> ». L'action de l'État vise alors à donner aux acteurs économiques les moyens de faire face à des crises de toutes sortes affectant l'économie du pays<sup>6</sup>. Ensuite, d'un point de vue pratique, il est certain que l'action des entreprises (ou à tout le moins de certaines) est au cœur des enjeux de sécurité. Toute entreprise doit prendre en compte la question de la sécurité des personnes et des biens, engageant sa responsabilité si son activité porte atteinte à la sécurité des tiers (pollution, explosion, non-respect des normes de sécurité...). La question de la sécurité se présente encore pour l'entreprise sous l'angle de la sécurité économique (protection des procédés et des sources, maintien d'un avantage concurrentiel...). Enfin, des entreprises exerçant leurs activités dans des lieux ouverts au public peuvent être soumises à différentes obligations légales leur enjoignant de prendre des mesures pour assurer la protection de leurs clients ou de leurs salariés<sup>7</sup>.

Par ailleurs, l'association de personnes privées à la réflexion sur la sécurité publique se justifie encore d'un point de vue théorique, car si « *la sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives*<sup>8</sup> », cela vise aussi les entreprises. Pour autant, la participation de personnes privées à la sécurité, consacrée par les textes<sup>9</sup>, ne traduit longtemps que l'hypothèse d'interventions subsidiaires conditionnées par l'urgence et la nécessité, sans nullement témoigner d'une quelconque

coproduction. Pour autant, ce tableau de l'association des acteurs privés aux questions de sécurité tend à être renouvelé par une autre dimension, celle de la participation active des entreprises à la sécurité publique.

## L'ÉTAT NE PARVENANT PAS À JUGULER CETTE VIOLENCE ENDÉMIQUE CHERCHE À METTRE À LA CHARGE D'AUTRES ACTEURS LE SOIN D'ASSURER LA SÉCURITÉ PUBLIQUE.

Cette participation est d'abord la résultante de l'essor sans précédent de la délinquance ainsi que de l'insécurité et des solutions recherchées pour y faire face. L'État ne parvenant pas à juguler cette violence endémique cherche à mettre à la charge d'autres acteurs le soin d'assurer la sécurité publique. C'est ainsi qu'il s'est tourné vers les services privés de sécurité, les chargeant de remplir une partie de ses missions traditionnelles et répondre à une demande de sécurité toujours accrue ; cela a d'ailleurs conduit à la création d'un véritable marché de la sécurité, secteur statistiquement reconnu

comme ayant eu la croissance la plus forte au cours des trente dernières années<sup>10</sup>. Au-delà de la question spécifique des entreprises de sécurité privée, la participation active des entreprises à la sécurité résulte également – et surtout – d'un renouvellement des politiques publiques. Comme le relève Pierre Simula, la période contemporaine donne naissance à « *un nouveau paradigme [qui] s'impose, celui de la coproduction, qui relie chacune des composantes de l'action à une même synergie globale*<sup>11</sup> ».

Par cette coproduction, l'État a mis à la charge des entreprises de nombreuses obligations visant à les faire contribuer à leur sécurité, considérant qu'étant tout à la

(5) Circulaire du 14 fév. 2002 relative à la défense économique (JO du 23, p. 5164).

(6) « *Responsable de la préparation et de l'exécution de la politique de sécurité économique* », le ministre de l'Économie « *prend les mesures de sa compétence garantissant la continuité de l'activité économique en cas de crise majeure et assure la protection des intérêts économiques de la Nation* », art. L. 1142-3 Code déf.

(7) Les exploitants de discothèques ou de débits de boissons doivent assurer le bon ordre dans leurs établissements ; de même, les entreprises recevant du public sont tenues de prendre des dispositions contre les risques d'incendie et de panique (art. R. 123-1 et suiv. du Code de la construction et de l'habitation). Par ailleurs, le juge considère que les banques sont tenues à une obligation de moyens pour assurer la sécurité de leurs clients dans leurs locaux (CA Paris, 4 mars 1987, RTD com., 1987, p. 560, obs. Rémy Cabrillac et Bernard Teyssié)...

(8) Art. 1<sup>er</sup> de la loi n° 95-73 du 21 janv. 1995 d'orientation et de programmation relative à la sécurité ; la loi ajoute d'ailleurs que l'État a le devoir d'assurer la sécurité.

(9) Ainsi, a toujours été reconnu à l'individu le droit à la légitime défense (art. L. 122-5 du Code pénal), tandis qu'en cas de flagrance, « *toute personne a qualité pour en appréhender l'auteur et le conduire devant l'officier de police judiciaire le plus proche* » (art. 73 du Code de procédure pénale) ; même si ces hypothèses ne sont que la conséquence de l'urgence et de l'impossibilité matérielle d'une intervention directe des services de police.

(10) Le rapport de branche 2013, établi par le Syndicat national des entreprises de sécurité fait état d'environ 10 000 entreprises employant 150 000 salariés, pour un poids de près de 5,5 milliards d'euros ; v. [www.e-snes.org/poids\\_eco.html](http://www.e-snes.org/poids_eco.html). Si ce chiffre ne dépasse pas celui des forces publiques de sécurité (police et gendarmerie comptent 250 000 agents ; il conviendrait d'ajouter 25 000 policiers municipaux), il est en nette croissance, de même que le chiffre d'affaire de la branche (10 % de croissance sur les cinq dernières années).

(11) Simula (P.), 1999, « *Offre de sécurité et forces publiques régaliennes* », *Les Cahiers de la sécurité intérieure*, n° 37, p. 136.

fois enjeux et bénéficiaires de la sécurité publique, ces entreprises se devaient d'y participer. Il fut ainsi choisi par les pouvoirs publics d'imposer aux entreprises de participer à la sécurité ; les entreprises se voyant, *volens volens*, associées à sa production. On constate donc que si les trente dernières années ont bien connu une extension sans précédent des obligations de sécurité mises à la charge des entreprises privées, ce mouvement s'est effectué en dehors de tout débat public réel ; or le bien fondé d'un tel mouvement mérite d'être interrogé.

## L'extension croissante des obligations de sécurité mises à la charge des entreprises

L'extension du marché de la sécurité privée fut la première des réponses apportées à l'essor de la délinquance et de l'insécurité ; apparu à la fin des années 1970, ce secteur s'est vu encadré par l'État, avant d'être pleinement associé à la production de sécurité<sup>12</sup>, la loi admettant que ces activités de sécurité privée « *concourent [...] à la sécurité générale*<sup>13</sup> ». Au-delà de cette coproduction revendiquée, l'État a mis directement à la charge de l'ensemble des acteurs sociaux – et les entreprises au premier chef, nombre d'obligations en matière de sécurité. Initié en 1995, le mouvement fit l'objet de multiples confirmations.

## L'institution d'une obligation de contribuer à la sécurité

L'adoption en 1995 de la loi d'orientation et de programmation relative à la sécurité<sup>14</sup> marqua un tournant dans l'approche faite par les pouvoirs publics de la participation des acteurs privés à la sécurité publique. Jusqu'à cette date, n'était imposé aux entreprises que le respect de dispositions générales visant à assurer la

sécurité de leurs employés et clientèle ; les questions de sécurité n'y étaient envisagées que sous l'angle des risques d'incendie et de panique<sup>15</sup>. La loi adoptée change profondément la nature des obligations mises à la charge des entreprises. Visant à favoriser la lutte contre la délinquance en général et le vol dans les commerces en particulier, elle le fait par deux techniques distinctes ; il s'agit d'abord d'encourager le recours à la vidéoprotection, il s'agit aussi d'obliger les entreprises à assurer leur sécurité. En effet, « *les propriétaires, exploitants ou affectataires, selon le cas, d'immeubles à usage d'habitation et de locaux administratifs, professionnels ou commerciaux doivent, lorsque l'importance de ces immeubles ou de ces locaux ou leur situation le justifient, assurer le gardiennage ou la surveillance de ceux-ci*<sup>16</sup> » ; ces établissements sont contraints d'assurer eux-mêmes leur surveillance ou gardiennage.

L'ampleur de ces obligations de faire à la charge des entreprises n'est pas négligeable. La loi « *organise une quasi-délégation de la compétence de police [...] [car] certains établissements ou exploitants de commerce sont désormais contraints – et à leur charge – de soumettre leurs locaux à la surveillance d'agences privées*<sup>17</sup> » et le pouvoir réglementaire précise les modalités de réalisation de cette obligation : gardiennage ou surveillance de leurs locaux sont imposés aux grandes surfaces établies dans des communes dépassant 25 000 habitants et dans certaines zones dont le taux de criminalité dépasse la moyenne nationale. La même obligation s'impose encore aux établissements présentant un risque particulier d'attaque (banques, bureaux de change, bijouteries), aux pharmacies et ensembles commerciaux<sup>18</sup>. Les exploitants visés sont mis en demeure de faire connaître aux pouvoirs publics les dispositions prises pour assurer le gardiennage ou la surveillance de leurs locaux, sachant que le non-respect de ces obligations rend l'exploitant passible d'amende<sup>19</sup>.

Ce mouvement déjà large et ayant pour effet de mettre à la charge des entreprises des obligations de sécurité ne se limitait pourtant pas à ce domaine déjà vaste, puisque cette même loi de janvier 1995 enjoignait encore

(12) V. Nicoud (F.), 2006, « La participation des personnes privées à la sécurité publique », *RDP*, p. 1247 ; Latour (X.), 2012, « Sécurité publique et sécurité privée, de l'ignorance à la coproduction », *Cahiers de la sécurité*, n° 19, p. 7.

(13) *Rapport sur les orientations de la politique de sécurité*, point I-3 : « Les activités privées de sécurité », rapport annexé à la loi n° 95-73 préc.

(14) Loi n° 95-73 préc.

(15) La réglementation relative aux établissements recevant du public est incorporée au Code de la construction et de l'habitation, dont elle constitue le ch. III, « Protection contre les risques d'incendie et de panique dans les immeubles recevant du public », du Titre 2 : « Sécurité et protection des immeubles », art. L. 123-1 et s.

(16) Art. L. 271-1 du Code de la sécurité intérieure (CSI).

(17) Nicoud (F.), « La participation des personnes privées à la sécurité publique », *op. cit.*, p. 1247.

(18) Art. R. 273-1 et suiv. CSI. Sont précisés la nature des locaux visés, les zones dans lesquelles l'obligation s'applique et les mesures de gardiennage et de surveillance à prendre. Les obligations incombant aux exploitants de garages ou de parcs de stationnement, ainsi que celles visant les immeubles d'habitation figurant respectivement aux articles R. 273-7 à 9 CSI et R. 271-1 à 3 CSI.

(19) Art. R. 271-7 et 8 CSI.

aux « *organismes de manifestations sportives, récréatives ou culturelles [...] d'y assurer un service d'ordre lorsque leur objet ou leur importance le justifie*<sup>20</sup> ». Si le principe même de tels mécanismes soulevait déjà l'interrogation, ils ne devaient pas rester limités au seul champ alors déterminé.

## L'extension des obligations de contribuer à la sécurité

Depuis 1995, de nombreuses entreprises privées se voient contraintes de procéder à l'installation de dispositifs de sécurité<sup>21</sup>, afin de prévenir la commission d'infractions. Cette réalité nouvelle, loin de ne rester cantonnée qu'au seul champ alors déterminé par le législateur, a depuis fait l'objet de continuelles extensions.

La première intervint en 2001, au lendemain des événements du 11 septembre. Lors de l'adoption de la loi sur la sécurité quotidienne<sup>22</sup>, les parlementaires revinrent sur l'obligation instituée en 1995 et complétèrent l'article L. 271-1 CSI, pour obliger ces mêmes propriétaires, exploitants ou affectataires, d'immeubles à usage d'habitation et de locaux administratifs, professionnels ou commerciaux à « *prendre les mesures permettant d'éviter les risques manifestes pour la sécurité et la tranquillité des locaux*<sup>23</sup> ». Là encore, des dispositions pénales sanctionnent le non-respect des dispositions instituées.

C'est ensuite en 2005, que le Code de la défense oblige opérateurs publics et privés d'installations d'importance vitale à participer à leurs frais à leur protection contre toute menace, notamment terroriste... En 2006, la loi permettra aux préfets d'obliger les exploitants d'installations classées ou d'importance vitale pour la défense à se doter d'un mécanisme de vidéoprotection<sup>24</sup>. Toutes ces obligations mises à la charge de l'entreprise le sont au nom de la

sécurité nationale et lui sont financièrement imputées, le législateur considérant qu'il s'agit d'une nécessaire contribution des entreprises à la sécurité collective.

Comme il fut noté, « *le souci public d'assurer une prévention efficace de la délinquance conduit ainsi à faire reposer cette charge sur certaines personnes privées devant elles-mêmes assurer la surveillance de leur commerce*<sup>25</sup> ». Grands ensembles de logements, supermarchés, complexes cinématographiques, pharmacies, banques, salles de spectacles ou stades, installations classées pour la protection de l'environnement... Loin d'une simple liste à la Prévert, l'énumération atteste que de très nombreuses entreprises se voient imposer chaque jour de nouvelles obligations en matière de prévention des activités délictueuses et *de facto* contribuer, aux côtés des forces de l'ordre, à la sécurité sur le territoire<sup>26</sup>.

Tous ces éléments attestent d'une extension croissante des obligations de sécurité mises à la charge des entreprises privées et on assiste, dans une indifférence quasi généralisée à un glissement témoignant d'une forme de désengagement de l'État en matière de sécurité, mouvement qui suscite certaines interrogations.

## L'interrogation restante des obligations de sécurité mises à la charge des entreprises

Depuis maintenant vingt ans se multiplient les obligations mises à la charge des entreprises en matière de sécurité. La principale cause explicative de ce mouvement réside dans l'affirmation de la nécessité de réunir l'ensemble des acteurs intéressés à la réduction et à la prévention de la délinquance afin de permettre une coproduction

(20) Pour être complet, on ajoutera que la même loi obligeait les promoteurs à effectuer une étude de sécurité publique lors de la conception de leurs projets, afin de réfléchir aux problèmes de sécurité qu'ils pourraient engendrer et aux moyens de prévenir la délinquance dans la future zone construite. Si une telle étude doit être approuvée en tant qu'elle facilitera l'intervention ultérieure des forces de l'ordre, elle n'en a pas moins pour effet de transférer la charge matérielle de la réflexion sur la délinquance et les moyens de la prévenir sur des opérateurs privés ; art. L. 114-1 à 4 du Code de l'urbanisme.

(21) Soit en régie, par la mise en place d'un service de sécurité interne, soit en faisant appel à des sociétés extérieures spécialisées dans le marché de la sécurité.

(22) Loi n° 2001-1062 du 15 nov. 2001 relative à la sécurité quotidienne.

(23) Art. L. 271-1 CSI nouveau, issu de l'art. 52 de la loi n° 2001-1062. Les modalités de mise en œuvre de cette obligation figurent aux articles R. 271-4 à 8 CSI. Adoptée au motif « *d'impérieuses nécessités de sécurité publique* » cette loi n'a pas été déférée au contrôle du juge constitutionnel.

(24) Art. L. 223-2 CSI (loi n° 2006-64 du 23 janv. 2006 relative à la lutte contre le terrorisme) ; le préfet peut mettre l'exploitant en demeure de réaliser l'installation, à peine d'amende de 150 000 € (art. L. 223-6 et 7 CSI).

(25) Nicoud (F.), « La participation des personnes privées à la sécurité publique », *op. cit.*, p. 1259.

(26) Encore une fois, aucune de ces dispositions n'a fait l'objet d'un contrôle par le Conseil constitutionnel ; si celui-ci ne s'est jamais vu explicitement questionné sur la constitutionnalité de la mise à la charge des entreprises privées d'obligations en matière de police, on peut regretter qu'il n'ait jamais soulevé d'office cette question.

permettant d'assurer la sécurité commune. Au-delà de ce discours, chacun reconnaît sans difficulté que cette situation résulte surtout d'une incapacité de l'État à faire face aux obligations qui sont les siennes. Dès lors, c'est la réalité de cette coproduction qui doit être envisagée, car ce vocable dissimule mal la démission de l'État d'une de ses fonctions régaliennes ; la justification de l'obligation des entreprises de contribuer à la sécurité mérite d'être discutée.

### La justification de l'obligation de contribuer à la sécurité

Il y a sans doute lieu de se réjouir que les personnes privées soient associées à la réflexion sur la sécurité publique. Pour autant, le mouvement initié en 1995 et sans cesse renforcé depuis mérite une étude approfondie. En particulier, il semble que ce mouvement n'ait pas fait l'objet de débat public réel et que l'on n'ait peut-être pas estimé toute sa portée.

La lecture des travaux parlementaires est parfois édifiante et le fait de mettre à la charge des entreprises des obligations positives en matière de sécurité n'a fait l'objet d'aucun débat public sérieux. La première mention d'une telle possibilité figure dans le *Rapport sur les orientations de la politique de sécurité*, annexé à la loi de janvier 1995<sup>27</sup> ; il y est simplement écrit « *de façon générale, les réglementations qui interviennent dans les domaines les plus divers de l'activité sociale ne prennent pas en compte, ou les prennent de façon insuffisante, les problèmes relatifs à la sécurité des personnes et des biens, et, faute d'intégrer cette dimension, laissent se développer des pratiques qui ont pour effet de porter atteinte à la sécurité ou facilitent, de fait, certaines formes de délinquance. Le Gouvernement se fixe en conséquence pour objectif de faire en sorte que les lois et règlements portant sur quelque objet que ce soit prennent en compte les aspects de*

*sécurité, et, le cas échéant, déterminent les procédures et les obligations qui sont susceptibles de concourir à la sécurité*<sup>28</sup> ». Les rapports établis au cours de la procédure parlementaire sont muets sur les enjeux de la mesure, voire sur sa légitimité<sup>29</sup> ; seule l'hypothèse de mettre à la charge des organisateurs de manifestations sportives, récréatives ou culturelles l'obligation d'y assurer un service d'ordre lorsque leur importance le justifie se voyant clairement revendiquée<sup>30</sup>.

La lecture des rapports parlementaires et du compte rendu des débats intervenus successivement en 2001, 2005 et 2006 atteste de la même manière que cette mise à la charge des entreprises privées d'obligations de sécurité n'y souleva la moindre objection. En 2006, le rapporteur de la loi devant l'Assemblée nationale se bornera à relever que « *la législation et la réglementation prévoient déjà de très nombreuses prescriptions de sécurité qui ne font l'objet d'aucune compensation* » et que, par voie de conséquence, ces opérateurs « *sont d'ores et déjà tenus de coopérer à leurs frais [...] à la protection desdits établissements. [et qu'ainsi] la possibilité de leur imposer la vidéosurveillance ne sera donc qu'une modalité parmi d'autres d'application d'une obligation déjà existante*<sup>31</sup> ». Les lois obligent ainsi, dans des secteurs de plus en plus larges, les personnes privées, mettant à leur charge des obligations toujours plus lourdes en matière de sécurité ; cette approche nouvelle fut vue comme traduisant une forme d'institutionnalisation de « *la coopération des citoyens à la sécurité*<sup>32</sup> ».

S'il existe une coproduction de la sécurité traduisant un partenariat entre acteurs publics et privés de la sécurité<sup>33</sup> ; il existe au-delà un mouvement de mise à la charge des acteurs privés d'obligations nouvelles en matière de sécurité. Ce sont bien les pouvoirs publics qui obligent les opérateurs privés à réaliser des mesures de sûreté ; ceci signifie concrètement que la personne privée ne peut mettre en œuvre son activité si elle ne se soumet pas préalablement aux obligations de sécurité que la loi

(27) Le rapport est annexé au projet de loi n° 543, déposé au Sénat le 22 juin 1994 ; il est ensuite publié au *Journal officiel*, à la suite de la loi n° 95-73 préc. (JO du 24 janv. 1995, p. 1254).

(28) *Rapport sur les orientations de la politique de sécurité*, préc., termes soulignés par nos soins. Le rapport précise simplement : « *des dispositions seront immédiatement proposées au Parlement* » en matière d'obligation de gardiennage ou d'étude d'impact sur la sécurité à l'occasion des projets d'aménagement urbain.

(29) Paul Masson, rapport n° 564, Sénat, 30 juin 1994, Gérard Léonard, rapport n° 1531, Ass. nat., 22 sept. 1994. De même, la lecture exhaustive du compte rendu intégral des séances de l'Assemblée permet de vérifier que cette mise à la charge des entreprises d'obligations de sécurité ne s'est pas vue contestée le moins du monde dans son principe. Un seul orateur intervint en ce sens au cours des débats au Palais-Bourbon ; Rémy Auchédé dénonçait « *un véritable transfert de charges* », regrettant qu'aucun moyen financier ne soit prévu pour permettre aux propriétaires de faire face à cette charge nouvelle : JO débats, Ass. nat., compte rendu intégral des séances du 10 oct. 1984, p. 5178.

(30) Le ministre de l'Intérieur déclarait aux députés : « *il n'est pas normal que la communauté nationale doive, par l'intermédiaire du budget de l'État, assumer le coût des mesures de sécurité entraînées par l'organisation de manifestations à but lucratif dont les organisateurs n'ont rien prévu en termes de sécurité* », compte rendu intégral des séances du 10 oct. 1994, p. 5217 ; v. aussi P. Masson, rapport n° 564 préc., p. 75-76.

(31) Alain Marsaud, rapport n° 2681 sur le projet de loi relatif à la lutte contre le terrorisme, Ass. nat., 16 nov. 2005, p. 50-51.

(32) Decocq (A.), Montreuil (J.), Buisson (J.), 1998, *Le droit de la police*, Litec, n° 192, p. 111.

(33) Si tant est que ce vocable de « coproduction » désigne une réalité concrète et ne dissimule pas la mise à la charge d'acteurs non étatiques d'obligations jusqu'alors exercées sans partage par la puissance publique.

fait peser sur elle. Cette évolution suscite l'interrogation : est-il légitime de subordonner et conditionner la mise en œuvre d'activités privées à la réalisation par l'entreprise de mesures de police administrative<sup>34</sup> ? N'appartient-il pas à l'État et à lui seul de prévenir la réalisation des risques ?

## La discussion de l'obligation de contribuer à la sécurité

La surprise causée par un tel bouleversement du principe fondamental de droit public en vertu duquel le maintien de l'ordre public est une prérogative essentielle de l'État n'a d'égal que l'indifférence dans laquelle s'opéra l'adoption de cette mesure.

Quelques sénateurs s'inquiétèrent, relevant « *qu'obliger les propriétaires à assurer eux-mêmes la sécurité représentait une atteinte au droit à la sécurité des citoyens, une remise en cause de la responsabilité essentielle de la police nationale en matière de sécurité des personnes et des biens*<sup>35</sup> », cet argument pourtant essentiel ne fut curieusement pas repris par les élus lors de leur saisine du Conseil constitutionnel<sup>36</sup> ; de manière identique, le Conseil se montra tout aussi indifférent à cette question lors de son examen de la constitutionnalité des lois mettant de telles obligations à la charge des entreprises<sup>37</sup>. Certes, le Conseil validera ultérieurement le transfert d'une mission de police administrative à une personne privée,

mais il ne le fera pas sans répondre à la question de la constitutionnalité de la mise à la charge d'opérateurs privés d'obligations de police administrative<sup>38</sup>. À l'occasion de son contrôle de la loi d'avril 2005 relative aux aéroports, il valide la loi en s'appuyant sur l'existence d'un cahier des charges précisant la teneur des obligations de la société *Aéroports de Paris* ; cahier des charges fixant les conditions dans lesquelles cette société « *assurera les services publics liés aux aéroports qu'elle exploite et exécutera les missions de police administrative qui lui incombent*<sup>39</sup> ». Ces dispositions de la loi ne seront d'ailleurs validées que sous la seule dimension de l'absence de méconnaissance du principe de continuité du service public<sup>40</sup>, sans que soit envisagée la question de la mise à la charge des entreprises d'obligations de police...

Si aucune saisine du Conseil n'est encore intervenue sur ce point, l'obligation faite aux entreprises n'en suscite pas moins interrogations et réserves. D'ailleurs, on ne s'étonnera pas que ces dispositions suscitèrent de vives réserves de la part des représentants des entreprises, pour lesquelles le respect de ces obligations peut s'avérer particulièrement coûteux. La Chambre de commerce et d'industrie de Paris contesta ce mouvement, considérant qu'il opérait un transfert de compétences régaliennes vers les particuliers – transfert occasionnant des charges indues<sup>41</sup> –, mais sans parvenir à réellement se faire entendre. Or, si la police est une activité qui relève par nature de la compétence de l'État, son entretien relève nécessairement de la communauté des citoyens<sup>42</sup> et il

(34) Cette question ne se pose pas sous le seul angle de sa légitimité, en dépit du fait que la légalité d'une telle mesure paraisse acquise, au regard des nombreuses lois fixant ces obligations. La constitutionnalité du procédé se pose encore : le brevet de constitutionnalité qui résulte du silence gardé par le Conseil constitutionnel sur ces questions ne saurait en effet constituer qu'une présomption réfragable...

(35) Meyer (C.), 1997, « Gardiennage et surveillance des locaux commerciaux et des parcs de stationnement », *AJPI*, p. 933, citant les propos de sénateurs socialistes : *JO débats*, Sénat, 8 juil. 1994, p. 3669 et s.

(36) La lecture de la saisine révèle que si sénateurs et députés contestèrent le principe de l'extension du recours à la vidéoprotection, ils ne le faisaient que sur le double fondement de la violation du principe de nécessité et de proportionnalité des mesures de police, ainsi que de l'insuffisance des garanties fondamentales. Nulle part les requérants ne mentionnèrent un quelconque dessaisissement de l'État d'une de ses compétences régaliennes, d'ailleurs, seuls les articles 8, 13 et 15 furent visés par la saisine et non les différents articles chargeant les entreprises de prévenir elles-mêmes la commission d'infraction (v. les saisines en date du 23 déc. 1994, *JO* du 21 janv. 1995, p. 1156 & 1159). Le même constat peut être dressé à propos de la loi n° 2006-64 du 23 janv. 2006 ; si elle fut soumise aux Sages, les requérants ne mirent pas en cause la constitutionnalité de l'art. 2 obligeant les entreprises à assurer elles-mêmes leur sécurité. Les lois n° 2001-1062 du 15 nov. 2001 et n° 2005-1550 du 12 déc. 2005 ne furent pas déferées au contrôle du Conseil.

(37) La décision rendue par le Conseil en 1995 permet de vérifier ce point. Seuls certains détails techniques relatifs aux modalités de mise en œuvre de la vidéoprotection furent censurés, sans qu'aucune objection ne soit soulevée d'office à l'encontre de l'art. 12 de la loi transférant au privé une mission de police administrative : C. const., décision n° 94-352 DC, 18 janv. 1995, *loi d'orientation et de programmation relative à la sécurité*, Rec. p. 170 ; *idem* en 2006, le Conseil ne soulevant d'office aucun grief à l'encontre de la disposition en cause, C. const., décision n° 2005-532 DC, 19 janv. 2006, *loi relative à la lutte contre le terrorisme*, Rec. p. 31.

(38) Une fois de plus, les requérants se montrèrent pusillanimes, ne contestant pas le principe de la décharge de l'État de l'une de ses obligations régaliennes (v. la saisine en date du 6 avr. 2005, *JO* du 21, p. 6975 & 6982).

(39) C. const., 14 avr. 2005, décision n° 2005-513 DC, *Loi relative aux aéroports*, § 5.

(40) C. const., n° 2005-513 DC, *préc.*, § 7.

(41) *Mieux assurer la sécurité des commerces et des services*, rapport de la Chambre de commerce et d'industrie de Paris, 23 avril 1998 ; v. spéc. p. 3, 5 et 7.

(42) Ce qui justifie la création d'une force publique dont l'entretien est mis à la charge de la collectivité. Ainsi, l'article 12 de la déclaration des droits de l'Homme et du Citoyen (c) dispose que « *la garantie des droits de l'Homme et du Citoyen nécessite une force publique* », tandis qu'en vertu de l'art. 13 « *pour l'entretien de la force publique, et pour les dépenses d'administration, une contribution commune est indispensable : elle doit être également répartie entre tous les citoyens, en raison de leurs facultés* ».

semble plus que curieux que ceux-ci contribuent une première fois à l'entretien de la force publique, puis se voient contraints de rétribuer une seconde fois la sécurité publique par le financement de la réalisation de dispositifs de sécurité sans lesquels ils ne peuvent mettre en œuvre les activités liées à leur objet social<sup>43</sup>. S'inscrit encore dans ce mouvement la levée de doute instituée par le législateur en 2001<sup>44</sup> ; en vertu de cette procédure, les agents de sécurité ont l'obligation de vérifier le bien-fondé du déclenchement d'une alarme préalablement à tout appel aux forces publiques<sup>45</sup>. La levée de doute oblige des entreprises à vérifier la nature des éléments ayant conduit au déclenchement des signaux d'alarme avant de recourir aux forces de l'ordre ; cela « *impose donc à la société de surveillance le recueil d'informations sur place*<sup>46</sup> » et met une fois de plus à sa charge des frais liés directement à l'exercice de fonctions associées à la sécurité publique.

L'ampleur de ce mouvement oblige à s'interroger ; le maintien de l'ordre public, la prévention des risques, la mission de sécurité appartiennent-ils fondamentalement et exclusivement à la puissance publique ? La compétence monopolistique de l'État en matière de sécurité et de police relève-t-elle d'une nature structurelle ou au contraire, d'un simple phénomène conjoncturel ? La réponse à cette question, qui semblait hier évidente, n'est plus aussi certaine aujourd'hui. Il y aurait, pour certains, une « *relativité fondamentale du régalién* » et par voie de conséquence, la notion de police « *n'aurait pas d'essence définitivement figée, serait malléable et évolutive, parce qu'essentiellement contextuelle et historique*<sup>47</sup> ». Ainsi la charge de la prévention des risques pourrait-elle être sans difficulté conférée à des acteurs privés.

Pour autant et parce que trop empreinte de subjectivité, une telle approche nous semble devoir être écartée pour une analyse plus globale. Alors, si l'on peut évoquer une coproduction de la sécurité, cela doit être fait sans négliger le fait que l'État n'est pas absent d'un mouvement qu'il contrôle toujours. La puissance publique restant seule à posséder la capacité de mettre en cause les normes applicables en matière de sécurité et sous cet angle, le postulat weberien du monopole de la contrainte physique légitime n'est pas contesté. Dès lors, les modalités de l'intervention publique mériteraient d'être relues sous l'angle du diptyque : mise en cause/mise en œuvre. À l'État la mise en cause des règles et modalités d'intervention en matière de sécurité, aux opérateurs privés<sup>48</sup> la mise en œuvre des règles déterminées par l'État et sous son contrôle actif. Une telle clé permettrait une meilleure lecture de la répartition des rôles et des compétences en matière de sécurité ; elle faciliterait encore une meilleure lecture des conditions dans lesquelles des obligations positives de sécurité peuvent se voir mises à la charge des personnes privées en général et des entreprises en particulier ■

(43) Il y a alors violation du principe *non bis in idem* puisque ces entreprises sont assujetties deux fois au paiement de l'impôt, l'un direct, l'autre indirect lié aux charges supplémentaires que la réglementation fait peser sur ces entreprises. Il semble alors *a minima* possible de demander que l'ensemble des charges résultant pour les entreprises de la réalisation de leurs obligations de sécurité soient défiscalisées (réduction ou crédits d'impôts).

(44) Art. L. 613-6 CSI issu de la loi n° 2001-1062 préc.

(45) V. not. Pauvert (B.), 2013, « L'intervention de la sécurité privée sur la voie publique », *Quel avenir pour la sécurité privée ?*, Vallar (C.), Latour (X.) (dir.), PU Aix-Marseille, p. 75-89 et spéc. p. 80.

(46) Michel Richard, obs. sous TA Strasbourg, 16 mai 2002, S<sup>6</sup> *Euro protection surveillance*, AJDA, 2012, p. 1963.

(47) Lemaire (E.), 2009, « Actualité du principe de prohibition de la privatisation de la police », RFDA, p. 774-775.

(48) Mais aussi aux polices municipales et cela sans que les forces nationales en soient exclues.

# L'entreprise collaboratrice du service public de la sécurité : l'exemple des aéroports

Florence NICOUD

La sécurité aéroportuaire a profondément évolué depuis une vingtaine d'années et l'entreprise y joue désormais un rôle de tout premier ordre. La sécurité des plateformes aéroportuaires, relève largement de la responsabilité des entreprises gestionnaires, qui assurent cette mission au moyen de l'intervention massive d'entreprises de sécurité privée, lesquelles tendent à apparaître comme de nouveaux dépositaires de la sécurité publique au sein de ces espaces sensibles. Si ce spectaculaire mouvement de croissance de la sécurité privée dans la zone aéroportuaire semble irréversible, il n'en continue pas moins de soulever un certain nombre d'interrogations sur ce que doivent être aujourd'hui les services publics régaliens et plus fondamentalement, le rôle de l'État.

**S'**il est un domaine dans lequel la coproduction de sécurité s'est développée de manière particulièrement novatrice, c'est bien celui des aéroports, le mouvement qui s'y dessine étant peut-être archétypal de la construction des futures réponses de sécurité publique. En effet, en matière de sûreté<sup>1</sup> aéroportuaire, l'entreprise est, depuis une trentaine d'années, un allié incontournable du secteur public et de l'action d'État. C'est dans ce cadre, tout particulièrement concerné par l'impératif de sécurité et de

lutte contre les risques, que la conjugaison de l'action du service public et des entreprises privées s'est pleinement vérifiée. De l'avis de tous, « *le transport aérien est un moyen de transport sûr et rapide, qui permet de raccourcir les distances, donc le temps, grâce à l'innovation technique et les réalisations modernes de plus en plus sophistiquées*<sup>2</sup> ». Ce lieu emblématique de la modernité est dans le même temps, et bien avant le tournant dramatique des événements du 11 septembre 2001, une cible privilégiée par les attaques terroristes ou les détournements d'avions, spécialement depuis le seuil des années 1970.

En effet, « *l'avion peut ainsi constituer un moyen terrible pour perpétrer la terreur, compte tenu de la*

Florence NICOUD



Maître de Conférences (H.D.R.) à l'Université de Haute-Alsace.

Membre de l'Association Française de Droit de la Sécurité et de la Défense, elle enseigne notamment le droit administratif et le droit des services publics. Elle a publié de nombreux articles notamment sur l'importance du rôle croissant des entreprises de sécurité privée dans la sécurité publique et sur le droit de la sécurité aéroportuaire.

(1) Le langage commun tend à assimiler sécurité et sûreté, pourtant dans le langage aéronautique les deux termes ne sont pas synonymes. Ainsi, le premier terme désigne « les règles de construction et d'utilisation des avions » tandis que le second « vise à la prévention de tout acte illégal volontaire » ; v. Rembauville-Nicolle (P.), 2005, « L'effectivité du droit de la sécurité aérienne », *La sécurité et la sûreté des transports aériens*, Latour (X.) (dir.), Paris, L'Harmattan, p. 33. Toutefois, et pour une commodité de langage, les termes de « sécurité » et de « sûreté » seront bien ici utilisés de manière synonyme, au sens d'une volonté d'assurer la protection de l'équipage, du personnel au sol et des voyageurs contre les actes illicites (au sol et en vol).

(2) Carter (R. H. A.), 2008, *La sûreté des transports*, Paris, PUF, p. 77.



*densité de plus en plus importante de la circulation aérienne<sup>3</sup> ». Alors, « des premiers détournements d'avions à l'attentat de Lockerbie survenu en 1988, jusqu'aux événements tragiques du 11 septembre 2001, les transports aériens sont devenus une cible privilégiée du terrorisme. Dès lors, la question de la sûreté aéroportuaire est devenue récurrente<sup>4</sup> ». Les détournements d'avions ou les attentats au sein d'enceintes aéroportuaires<sup>5</sup> ont ainsi été les catalyseurs d'une coproduction de la sécurité associant, dans un modèle peut-être précurseur, l'action des forces de l'ordre à celle d'entités privées. En effet, si l'État, notamment par le rôle essentiel dévolu au préfet<sup>6</sup>, demeure le premier responsable du maintien de l'ordre et de la prévention des infractions dans la zone aéroportuaire, c'est sans compter la participation croissante de l'entreprise à la mise en œuvre de cet impératif public.*

Il s'agit donc de dresser un état des lieux de ce rôle somme toute assez novateur et aujourd'hui incontournable dévolu

aux entreprises, au cœur d'une mission régalienne, celle relative à la sûreté des aéroports. Il y a encore trente ans, l'État et ses services y étaient les principaux responsables de la mise en œuvre de la sûreté<sup>7</sup> ; depuis, les années 1990 auront vu l'avènement de nouvelles entités – notamment privées – chargées d'assurer cette mission, en coordination avec les services d'État et parfois en lieu et place de ces derniers. La zone aéroportuaire constitue alors l'exemple d'un modèle réussi de coproduction de la sûreté associant le secteur public au privé. La preuve de l'efficacité de ce modèle réside d'ailleurs dans le nombre désormais dérisoire d'attentats au sein même des aéroports ou de détournement d'avions aboutissant effectivement<sup>8</sup>.

Pour autant, l'ampleur de ce phénomène de coproduction qui tend à s'étendre à l'ensemble des lieux exigeant la sécurité n'en suscite pas moins l'interrogation. Peut-on dupliquer ce modèle de coproduction à l'ensemble des

(3) *Ibid.*, p. 11.

(4) Nicoud (F.), 2015, « La sécurité des transports aériens : un exemple pour l'Europe de la sécurité ? », *Le droit de la sécurité et de la défense en 2014*, Gohin (O.) et Pauvert (B.) (dir.), PU Aix-Marseille, p. 305.

(5) Bien qu'ils soient en réalité et en France tout du moins quantitativement assez peu nombreux.

(6) Aux termes de l'art. L. 6332-2 du Code des transports, « la police des aérodromes et des installations aéronautiques régis par les dispositions du présent chapitre est assurée, sous réserve des pouvoirs de l'autorité militaire à l'égard des aérodromes et installations dépendant de la défense nationale, par le représentant de l'État dans le département qui exerce, à cet effet, dans leur emprise, les pouvoirs impartis au maire aux articles L. 2212-2 et L. 2213-33 CGCT ».

(7) Loi n° 73-10 du 4 janv. 1973 relative à la police des aérodromes, modifiant et complétant le Code de l'aviation civile, JO du 5, p. 230.

(8) Mis à part deux attaques perpétrées à l'aéroport d'Orly en janvier 1975 par des groupes palestiniens et ayant fait uniquement des blessés, le seul attentat meurtrier commis en France dans un aéroport remonte au 15 juillet 1983 au cours duquel une bombe explose à l'aéroport d'Orly, placée par l'Armée secrète arménienne de libération de l'Arménie (ASALA), faisant huit morts et plus d'une cinquantaine de blessés.

domaines de la sécurité ? Également, la multiplication des lois octroyant aux entreprises de sécurité privée toujours plus de prérogatives, tant dans le domaine spécifique des aéroports que celui de la sécurité en général, ne marque-t-elle pas l'abandon d'une mission régaliennne parmi les plus emblématiques de l'État ? Cette coproduction de la sécurité, plus de trente années après son instauration dans les zones aéroportuaires, reste encore discutable.

## Une coproduction réussie

Ensemble complexe, l'aéroport est à la fois lieu de passage de millions de voyageurs et le centre d'importants enjeux économiques ; il fait, à ce titre, intervenir une multitude d'acteurs y exerçant des rôles divers et connexes. Sous l'angle de la sécurité, la notion d'entreprise intervient à un double niveau. Il existe d'abord une compétence de principe du gestionnaire privé de l'aéroport, à laquelle est associée l'action complémentaire et indissociable des entreprises de sécurité privée.

## La compétence de principe du gestionnaire privé

Que l'exploitant de la zone aéroportuaire soit une chambre de commerce et d'industrie liée à la puissance publique, une société ou, plus rarement de nos jours, un établissement public, les textes lui confèrent la délicate mission de mettre en œuvre les mesures nécessaires afin de prévenir tout acte illicite pouvant porter atteinte à la sûreté des vols et des personnes en général. Ainsi, en vertu de l'article L. 6341-2 du Code des transports<sup>9</sup>, les

exploitants d'aéroports sont tenus d'assurer la sûreté de la zone aéroportuaire, alors qu'autrefois la mission était largement et principalement assurée par la police aux frontières et les services des douanes.

Les exigences de sécurité couplées à l'inévitable pression budgétaire toujours plus présente pour l'État ont fait que « *le lourd poids financier de la sûreté aérienne a ainsi été transféré par l'État aux gestionnaires d'aérodromes*<sup>10</sup> ». Ces derniers se sont vu confier une mission de police administrative, car l'intervention de la société exploitante, loin de n'être qu'un complément à celle de l'État, vise bien à « *assurer les services publics liés aux aérodromes qu'elle exploite et exécuter les missions de police administrative qui lui incombent*<sup>11</sup> ». La mission de l'exploitant, loin d'ailleurs de n'être dévolue que par des textes nationaux est également issue de directives européennes<sup>12</sup>, comme le rappelle le Code des transports : « *les mesures de sûreté résultent de l'application du règlement (CE) n° 300/2008 du Parlement européen et du Conseil du 11 mars 2008 relatif à l'instauration de règles communes dans le domaine de la sûreté de l'aviation civile*<sup>13</sup> ».

Du point de vue de la mise en œuvre pratique des opérations techniques visant à assurer la sécurité, un cahier des clauses administratives générales et divers arrêtés fixent les impératifs devant être respectés et assurés sous la responsabilité de l'exploitant de l'aéroport. Notamment et en vertu d'un cahier des charges type, issu directement des dispositions de l'article L. 6332-3 du Code des transports, « *les exploitants d'aérodromes civils et les gestionnaires des zones civiles des aérodromes ouverts au trafic aérien commercial [...] sont tenus d'assurer, sous l'autorité du titulaire des pouvoirs de police [...], le sauvetage et la lutte contre les incendies d'aéronefs ainsi que la prévention du péril animalier* ». Enfin, après 2003 et à la suite des événements du 11 septembre 2001, de plus

SOUS L'ANGLE DE LA SÉCURITÉ, LA NOTION D'ENTREPRISE INTERVIENT À UN DOUBLE NIVEAU. IL EXISTE D'ABORD UNE COMPÉTENCE DE PRINCIPLE DU GESTIONNAIRE PRIVÉ DE L'AÉROPORT, À LAQUELLE EST ASSOCIÉE L'ACTION COMPLÉMENTAIRE ET INDISSOCIABLE DES ENTREPRISES DE SÉCURITÉ PRIVÉE.

(9) « Sauf dans les cas où leur mise en œuvre est assurée par les services de l'État, les mesures de sûreté destinées à protéger l'aviation civile contre les actes d'intervention illicite sont mises en œuvre par : les exploitants d'aérodromes ; les entreprises de transport aérien [...]. Les mesures de sûreté sont mises en œuvre sous l'autorité du titulaire des pouvoirs de police mentionné à l'article L. 6332-2 ».

(10) Carter (R.H.A.), *La sûreté des transports*, op. cit., p. 45.

(11) CC, 14 avr. 2005, n° 2005-513 DC, *loi relative aux aéroports*, § 5.

(12) Ainsi, peut-on parler d'une véritable communautarisation dans ce domaine particulier de la sûreté, se vérifiant à un double niveau ; d'abord en matière de fixation des règles de sûreté puis au regard du contrôle de la mise en œuvre des mesures de sûreté. Pour une étude complète sur cette tendance, v. Nicoud (F.), « La sécurité des transports aériens : un exemple pour l'Europe de la sécurité ? », op. cit., p. 307.

(13) Art. L. 6341-2 III du Code des transports.

en plus de missions relatives à la sûreté aérienne se sont vues dévolues aux gestionnaires d'aéroport<sup>14</sup>. Or, du fait de l'ampleur des charges transférées de délégation en délégation, l'exploitant privé de l'aéroport rencontre également des difficultés financières, lesquelles sont loin d'être couvertes par l'acquittement par les passagers de la taxe aéroportuaire. Ces gestionnaires ont ainsi dû tout naturellement faire appel à des forces supplétives afin d'assurer à bien cette mission particulière de service public.

L'action complémentaire des entreprises de sécurité privée devenait alors indissociable de celle du gestionnaire privé. Aussi, le secteur aéroportuaire constitue-t-il, en termes de sûreté, une zone atypique, associant l'action conjuguée des forces publiques traditionnelles mais aussi des forces privées.

### L'action complémentaire des entreprises de sécurité privée

S'il est aujourd'hui courant de relever qu'en matière de sécurité le secteur privé est devenu l'allié incontournable des forces de l'ordre<sup>15</sup> – à tel point que certains ont pu relever que la sécurité paraissait n'être plus l'apanage de l'État<sup>16</sup>, on peut sans crainte énoncer que c'est en matière de sûreté aéroportuaire que ce mouvement d'externalisation et de coproduction de la sécurité a véritablement pris son essor<sup>17</sup>. Les chiffres témoignent de cette mutation désormais incontestée de la sécurité publique.

Ainsi, la sécurité privée représente-t-elle en France 150 000 agents en 2013, pour un chiffre d'affaires d'environ cinq milliards d'euros par an<sup>18</sup>. Et, comme le remarque le Professeur Latour : « une plate-forme comme Roissy ne pourrait pas fonctionner sans cet apport crucial en personnel, sauf à mobiliser plusieurs milliers de policiers et de gendarmes<sup>19</sup> ». Ainsi, « le désengagement de l'État dans la mission de sûreté laisse place à de nombreuses entreprises privées de sécurité, parmi lesquelles les plus importantes restent Brink's, Securitas et ICTS, qui se partagent les marchés distribués par les gestionnaires d'aéroports<sup>20</sup> ». C'est ainsi que les aéroports de Roissy et Orly accueillent 88 millions de passagers commerciaux (54 % du trafic en France). Sur ces deux sites franciliens et ceux du Bourget et de Lognes, la sûreté aérienne et aéroportuaire emploie 6 750 salariés, et réalise 72 % de son chiffre d'affaires national<sup>21</sup>.

Sans retracer l'historique de cette participation *crescendo* de la sécurité privée à cette mission régaliennne au sein des aéroports, on ne peut passer sous silence les étapes de ce glissement progressif du public vers le privé. Au seuil des années 1970, la menace terroriste grandissante conduisit certaines des compagnies aériennes à faire appel à des agents privés pour assurer des missions de sûreté sur leurs vols. Puis, la menace perdurant, le recours systématique à ces agents privés pour participer à la sécurité aéroportuaire résultera de la loi du 10 juillet 1989<sup>22</sup>, alors même que le statut de la sécurité privée commençait à peine à prendre corps<sup>23</sup>. Ces agents privés sont peu à peu devenus des acteurs à part entière de la sûreté aéroportuaire, pouvant « procéder à la visite des bagages, du fret, des colis postaux, des aéronefs et des véhicules<sup>24</sup> ». Néanmoins, « l'ouverture réalisée ne constituait qu'une première étape et somme toute assez minime, bien que fortement symbolique, puisque cette loi ne permettait l'intervention des agents privés que dans le seul domaine du contrôle des biens et non dans celui des personnes. Il est donc significatif que

(14) À la suite de divers arrêtés intervenus à l'automne 2003, l'exploitant doit assurer l'aménagement des zones destinées au contrôle des passagers, la mise en œuvre de ces contrôles par l'inspection-filtrage des passagers (et de leurs bagages), mais encore le contrôle du fret, et de l'ensemble des accès en zone réservée. Aussi, afin d'assurer cette mission, l'exploitant doit veiller à se procurer les équipements nécessaires aux procédures d'inspection, à leur mise en œuvre et à leur maintenance.

(15) Comme l'énonce la loi n° 95-73 du 21 janv. 1995 d'orientation et de programmation relative à la sécurité (JO du 24, p. 1429), la sécurité privée concourt à la sécurité générale, v. Rapport sur les orientations de la politique de sécurité, point I-3 : « Les activités privées de sécurité » : « Les entreprises de gardiennage, de surveillance et de transports de fonds, d'une part, les agences privées de recherche, d'autre part, exercent des activités de sécurité de nature privée. Elles concourent ainsi à la sécurité générale ».

(16) Chevallier (J.), 2014, « La police est-elle encore une activité régaliennne », *La police administrative*, Paris, PUF, p. 10.

(17) On peut sans erreur relever que la sécurité aéroportuaire fut le domaine expérimental du recours au privé ; pour une vue d'ensemble, v., Nicoud (F.), 2006, « La participation des personnes privées à la sécurité publique : actualité et perspectives », *RDP*, spéc. p. 1255-1258.

(18) Observatoire des métiers de la prévention et de la sécurité, *Enquête de branche - Prévention et sécurité - 2012, 2013*, resp. p. 28 et 11.

(19) Latour (X.), 2010, « La place du secteur privé dans la politique moderne de sécurité », *AJDA*, p. 658.

(20) Carter (R.H.A.), *La sûreté des transports*, op. cit., p. 45.

(21) [www.defi-metiers.fr/panoramas/les-metiers-de-la-securite-privee](http://www.defi-metiers.fr/panoramas/les-metiers-de-la-securite-privee)

(22) Loi n° 89-467 du 10 juil. 1989 tendant à renforcer la sécurité des aérodromes et du transport aérien et modifiant diverses dispositions du Code de l'aviation civile (JO du 11, p. 8673).

(23) Loi n° 83-629 du 12 juil. 1983 réglementant les activités privées de surveillance, gardiennage et transports de fonds (JO du 13, p. 2155).

(24) Art. L. 282-8 du Code de l'aviation civile désormais intégré au Code des transports dans l'art. L. 6342-4.

la possibilité d'intervention des agents privés se soit vue élargie en 1996<sup>25</sup> ». À cette date<sup>26</sup>, les agents privés purent procéder à la visite des personnes, leur contrôle restant limité à la mise en œuvre des dispositifs automatiques de contrôle, à l'exclusion des fouilles à corps et de la visite manuelle des bagages à main.

Il faudra attendre la triste et emblématique année 2001 pour que cette alliance du privé avec le public en matière de sûreté aéroportuaire soit parachevée. C'est la loi sur la sécurité quotidienne de janvier 2001<sup>27</sup> qui renforcera les prérogatives des agents de sécurité privée au cours du contrôle de l'inspection filtrage<sup>28</sup> : ils peuvent procéder aux palpations de sécurité sur les personnes et à la fouille des bagages (avec l'accord préalable du passager).

L'entreprise privée est ainsi devenue le pivot de la sûreté aéroportuaire, c'est autour d'elle que se cristallise désormais toute cette activité. Si l'État demeure l'autorité principale chargée d'assurer la mission de sécurité au sein des aéroports, il n'en demeure pas moins qu'aujourd'hui, « plus qu'une mise en œuvre d'échanges de personnel public-privé, l'organisation de la sûreté dans les aéroports parisiens montre qu'il existe une complémentarité et une coopération réelle entre les services publics, ADP et les entreprises privées de sécurité<sup>29</sup> ». Ceci pour le plus grand bien de la sécurité de tout un chacun.

Si les aéroports constituent le domaine topique et emblématique de la manifestation de l'association des acteurs privés à la sécurité publique, l'ampleur du phénomène constaté depuis une trentaine d'années continue de susciter d'importantes interrogations,

tant d'un point de vue juridique que conceptuel. Cette coproduction vérifiée et encouragée par les pouvoirs publics n'en reste pas moins discutable.

## Une coproduction discutable

L'interrogation suscitée par le déploiement de la sécurité privée dans les zones aéroportuaires françaises peut être envisagée en deux directions. Tout d'abord, chacun

constatera que ce transfert progressif – et aujourd'hui bien établi – de compétences s'est imposé quasiment sans discussion des autorités publiques dépositaires du pouvoir, ni aucun débat public. Aussi, peut-on évoquer l'idée d'un modèle adopté mais peu débattu. Par ailleurs peut être encore relevé qu'eu égard à la nature des pouvoirs conférés au secteur privé, ce modèle de coproduction de la sécurité demeure controversé, tant il participe à la relecture et la recomposition du rôle de l'État, dans un secteur jusqu'alors considéré comme régalien.

### Un modèle peu débattu

Le constat semble implacable. Alors même que le phénomène de coproduction de la sûreté aéroportuaire est en marche depuis une bonne trentaine d'années, conférant de larges pouvoirs de police

aux agents privés, l'instauration de ce modèle a quasiment été passée sous silence par les pouvoirs publics. Alors même que le Conseil constitutionnel, saisi de la seule loi de 2005 relative à la privatisation d'ADP<sup>30</sup> rappela que cette société,

ALORS MÊME QUE  
LE PHÉNOMÈNE DE  
COPRODUCTION DE LA  
SÛRETÉ AÉROPORTUAIRE  
EST EN MARCHÉ DEPUIS  
UNE BONNE TRENTAINE  
D'ANNÉES, CONFÉRANT  
DE LARGES POUVOIRS  
DE POLICE AUX AGENTS  
PRIVÉS, L'INSTAURATION  
DE CE MODÈLE A  
QUASIMENT ÉTÉ PASSÉE  
SOUS SILENCE PAR LES  
POUVOIRS PUBLICS.

(25) Nicoud (F.), « La participation des personnes privées à la sécurité publique : actualité et perspectives », op. cit., p. 1256.

(26) Loi n° 96-151 du 26 fév. 1996 relative aux transports (JO du 27, p. 3094).

(27) Loi n° 2001-1062 du 15 nov. 2001 relative à la sécurité quotidienne (JO du 16, p. 18215).

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

Ces agents doivent avoir été préalablement agréés par le représentant de l'État dans le département et le procureur de la République. Ils ne procèdent à la fouille des bagages à main et des autres objets transportés qu'avec le consentement de leur propriétaire et à des palpations de sûreté qu'avec le consentement de la personne. La palpation de sûreté est faite par une personne du même sexe que la personne qui en fait l'objet ».

(29) Mothes (F.) et alii, 2005, « Besoins et modalités d'échanges entre acteurs publics et privés de la sécurité », Les Cahiers de la sécurité, INHES, Paris, la documentation française, n° 57, p.27.

(30) Loi n° 2005-357 du 20 avr. 2005 relative aux aéroports (JO du 21, p. 6969) et CC, n° 2005-513 DC préc. § 5.

aux termes de son cahier des charges, était directement chargée d'une mission de police administrative, il est remarquable de noter que ce mouvement de privatisation partielle s'est fait sans que les parlementaires ne saisissent le Conseil d'une quelconque irrégularité des lois de 1989 et 1996<sup>31</sup> opérant un transfert direct de compétences... Un commentateur avisé notera d'ailleurs que cette participation du secteur privé « *qui constitue pourtant une remise en cause d'un principe essentiel du droit français voulant que la sécurité soit une prérogative régaliennne a été largement étendue depuis quelques années, sans qu'elle ne soulève beaucoup de bruit*<sup>32</sup> ». Ces diverses lois n'ont encore guère plus fait l'objet d'une question prioritaire de constitutionnalité, ceci permettant de supputer *a contrario* de la qualité du modèle législatif instauré et surtout de son efficacité.

C'est de la part des chambres de commerce et d'industrie qu'un bruit discordant se fit un tant soit peu entendre. De fait, et eu égard à l'importance des responsabilités en termes de sécurité mises à la charge des gestionnaires d'aéroport, il était légitime que ceux-ci aient fait entendre leur voix dans cet assourdissant silence. Elles introduisirent un recours en excès de pouvoir devant le Conseil d'État contre les arrêtés de septembre 2003 – relatifs aux infrastructures, équipements et formations en matière de sûreté du transport aérien – et de novembre 2003 – relatif aux mesures de sûreté du transport aérien<sup>33</sup>. Pourtant et en dépit de l'important transfert de compétences et des coûts inhérents à cette charge, le Conseil en reconnaissait la légalité, dans la mesure où « *le rôle consultatif des services de l'État mentionné par ce même arrêté, ne saurait ainsi être analysé comme un dessaisissement par l'État de la responsabilité de police lui incombant mais se rattache au contraire à la mise en œuvre de cette mission*<sup>34</sup> ». Les chambres de commerce seraient-elles les seules à s'inquiéter de ce glissement progressif vers le privé de charges relevant ordinairement de l'État<sup>35</sup> ?

Enfin, ce qui demeure sans doute le plus préoccupant dans cette absence de débat ou de réaction des édiles politiques c'est que, les rares fois où le Conseil constitutionnel fut saisi de ce problème, il sembla trouver plus à redire lorsqu'il s'est agi de déléguer des pouvoirs de police administrative aux agents privés pour surveiller la voie publique, que lorsqu'il s'est agi de la sûreté au sein des aéroports. En effet, si le Conseil interdit en 2011 la délégation de la gestion de la vidéosurveillance sur la voie publique à des sociétés privées<sup>36</sup>, c'est après avoir néanmoins reconnu en 2005 la constitutionnalité de la délégation d'une mission de police administrative à une société privée, dans le cadre de la sécurité aéroportuaire. La contradiction peut paraître des plus troublantes... Dès lors que cette délégation n'est pas contestée pour les aéroports, pourquoi les juges constitutionnels et administratifs présentent-ils une jurisprudence relativement chaotique sur la délimitation des possibilités d'action de ces agents sur la voie publique et dans le cadre de la vidéosurveillance<sup>37</sup> ?

C'est dire qu'au-delà de ces attermoissements jurisprudentiels la délégation des missions de police au secteur privé et la création d'un nouveau modèle de coproduction de la sécurité en France demeurent un sujet controversé, qui en dépit de son efficacité avérée, continuera certainement à nourrir d'importants débats doctrinaux.

### Un modèle pourtant controversé

Dans ce nouveau paradigme de la sécurité, celle-ci tend à devenir une valeur marchande, « *une sécurité "commerce"*<sup>38</sup> », relevant d'un partenariat toujours plus évident entre protagonistes divers, issus du secteur public et de l'entreprise. S'appuyant sur le postulat contemporain « *présumant le mode de gestion privé a priori plus efficace que le*

(31) La loi de 1983 réglementant les activités privées de sécurité n'aura pas plus fait l'objet d'une saisine du Conseil.

(32) Pauvert (B.), « La difficile conciliation de la sûreté aérienne et du respect des libertés individuelles », *La sécurité et la sûreté des transports aériens*, op. cit., p. 84. Il convient de remarquer que lorsqu'une loi concernant la sécurité privée comme celle de mars 2003 fit l'objet d'un contrôle par le Conseil constitutionnel, celui-ci ne se prononça que sur la question des conséquences de l'essor des pouvoirs des agents vis-à-vis des atteintes possibles aux libertés individuelles et non sur celle de la délégation des pouvoirs de police à une entité privée et donc de la perte potentielle d'une compétence essentielle de l'État : v. CC, n° 2003-467 DC, 13 mars 2003, loi pour la sécurité intérieure, « *Considérant que les auteurs des deux saisines font grief à ces dispositions de porter atteinte à la liberté individuelle et d'être formulées de façon trop imprécise* ».

(33) « *En vertu de ces textes, l'exploitant doit assurer l'aménagement des zones destinées au contrôle des passagers, la mise en œuvre de ces contrôles par l'inspection-filtrage des passagers (et de leurs bagages), mais encore le contrôle du fret, et de l'ensemble des accès en zone réservée. Pour mener à bien cette mission, l'exploitant doit donc veiller à se procurer les équipements nécessaires aux procédures d'inspection, veiller à leur mise en œuvre et à leur maintenance* », Nicoud (F.), 2006, « La répartition des compétences entre l'État et les opérateurs privés en matière de sûreté aéroportuaire », *AJDA*, p. 2109.

(34) CE, 9 mars 2005, *Union des chambres de commerce et établissements gestionnaires d'aéroports*, req. n° 264.689.

(35) Outre le recours précédent, v. le rapport de la Chambre de commerce et d'industrie de Paris, « Mieux assurer la sécurité des commerces et des services », 23 avril 1998, inédit, spéc. p. 7 et 8.

(36) CC, n° 2011-625 DC, 10 mars 2011, LOPPSI 2 (JO du 15, p. 4630).

(37) V. pour un résumé de ces jurisprudences, Nicoud (F.), « Les maires et la sécurité privée », *Les Politiques publiques locales de sécurité intérieure*, Dantonel-Cor (N.) (dir.), Paris, L'Harmattan, 2015, spéc. p. 296 à 299.

(38) Galland (J.-P.), 1906, « Éléments pour une prospective de la sécurité », *Les Cahiers de la sécurité intérieure*, IHESI, Paris, la documentation française n° 24, p. 87.

*mode de gestion public*, [et ayant pour conséquence directe] *le recours aux personnes privées comme un gage de performance dans l'exécution de certaines missions publiques*<sup>39</sup> », le constat se vérifie que, « *si l'État est le producteur naturel de la sécurité, il n'est plus le producteur exclusif*<sup>40</sup> ». La sécurité – particulièrement dans les aéroports – serait alors devenue une mission de service public parmi d'autres, pouvant faire l'objet d'une délégation partielle ou totale au privé, au même titre qu'électricité, gaz ou téléphonie en leur temps. Or, si l'instauration de ces pratiques s'est faite sans véritable débat, elle a aussi fait l'impasse sur l'interrogation quant à la forme et au rôle que doit avoir l'État aujourd'hui ! Cette évolution aurait à tout le moins dû permettre de se demander si la sécurité constitue ou non une prérogative régaliennne, ne pouvant être déléguée, car indissociable de la souveraineté de l'État.

Aussi, au regard du constat établi en termes de participation à la mission de service public dans les aéroports, on peut se demander si la sécurité appartient encore à l'État ? Même s'il reste vrai que « *le problème de l'identification des "vraies marques de la souveraineté" – telles que les désignait Jean Bodin – [...] est probablement insoluble*<sup>41</sup> », une telle mutation du rôle de l'État ne devrait pas faire l'économie d'un tel questionnement. Des réponses positives auraient pu être trouvées dans le discours des classiques tels que Jean Bodin<sup>42</sup> ou de plus modernes comme Max Weber, voire dans le courant essentialiste<sup>43</sup> ou chez les juristes<sup>44</sup> ; en sens opposé, les libertariens, mettant au centre de leur

raisonnement l'économie libérale et le marché, y apportent une réponse franchement négative<sup>45</sup>.

Il n'en demeure pas moins qu'en ne prenant pas position sur cette question pourtant fondamentale de la définition et de la délimitation des missions premières de l'État, les gouvernants successifs ont implicitement et favorablement validé un modèle de la sûreté aéroportuaire faisant « *intervenir une pluralité d'acteurs, privés comme publics, dans un enchevêtrement de compétences et de missions, rendant le rôle des uns et des autres difficilement déterminable*<sup>46</sup> » et aboutissant de fait à l'externalisation d'une part importante de la sécurité en France. En outre, il serait illusoire de penser que le recours au privé soit exempt de risque. D'abord, le poids financier résultant de ce transfert de charges vers le gestionnaire privé a pu avoir pour effet le recours à des sous-traitants pas toujours fiables<sup>47</sup>. Par ailleurs, les agents recrutés sont loin de tous présenter les garanties nécessaires à ces missions, ce dont témoignent les retraits de cartes professionnelles nécessaires à l'exercice de leur activité<sup>48</sup> ou d'agrèments à l'accès aux zones réservées des aéroports<sup>49</sup>, pour cause d'accointance avec certains milieux religieux radicaux. Néanmoins, avec le contrôle accru de la profession par l'instauration du Conseil national des activités privées de sécurité<sup>50</sup>, de tels débordements sont rares ou traités dès leur identification ; comme la sécurité privée est devenue « *un binôme de la sécurité publique, cet état de fait [a impliqué] une professionnalisation accrue des acteurs privés*<sup>51</sup> ».

(39) Fonouni-Farde (G.), 2011, « La délégation du service public de la sécurité : *Asinus equum spectat* ? », *La Revue administrative*, n° 384, p. 592.

(40) Latour (X.), 2012, « Sécurité publique et sécurité privée, de l'ignorance à la coproduction », *Sécurité publique-sécurité privée... partenariat ou conflit* ?, Les Cahiers de la sécurité, INHES, Paris, La documentation française, n° 19, p. 9.

(41) Lemaire (E.), 2009, « Actualité du principe de prohibition de la privatisation de la police », *RFDA*, p. 776.

(42) Bodin relève que s'il existe une obligation mutuelle entre le Prince et son sujet, dans la mesure où si le second doit « *obéissance aide et connaissance à son Seigneur* », celui-ci doit en retour « *justice, garde et protection* », *Les six livres de la République*, 1576, Livre 4, ch. 6.

(43) La théorie essentialiste postule l'existence de distinctions ontologiques entre organisations publiques et privées. Dès lors, la sécurité par sa nature et sa liaison avec la souveraineté de l'État, ne devrait connaître comme seul mode de gestion que la régie. Sur la contradiction entre théorie essentialiste et délégation du service public régalienn, v. Danet (D.), 2009, « Guerre d'Irak et partenariats public-privé : des partenariats public-privé controversés », *RFAP*, 2, n° 130, p. 249.

(44) « *Les compétences de police étant par nature inaliénables, il est fait interdiction à l'autorité de police d'utiliser une technique d'ordre contractuel* », relevait Jacques Moreau, 1965, « De l'interdiction faite à l'autorité de police d'utiliser une technique d'ordre contractuel », *AJDA*, p. 3.

(45) V. Nicoud (F.), « La participation des personnes privées à la sécurité publique », *op. cit.*, p. 1270 à 1272.

(46) V. sur ce point, Nicoud (F.), « La répartition des compétences entre l'État et les opérateurs privés en matière de sûreté aéroportuaire », *op. cit.*, p. 2107 à 2111.

(47) Selon Guillaume Fonouni-Farde, « *certaines sociétés de sécurité privée contournent les obligations nées de la loi n° 83-629 du 12 juillet 1983, notamment en matière de formation. Elles ont alors recours à des sous-traitants – le plus généralement des auto-entrepreneurs – en feignant parfois d'ignorer que ces derniers ne disposent pas des qualifications requises, ce qui leur permet non seulement de compresser les coûts d'emploi de ces personnels sous-traités, mais surtout de diluer leur propre responsabilité en cas de contrôle* », *op. cit.*, p. 596.

(48) V. CAA Lyon, 12 mars 2015, req. n° 14LY03742 (refus de carte fondé sur l'art. L. 612-20 CSI) ; v. encore pour relation de l'intéressé avec la mouvance wahabite tchétchène et son adhésion à l'islam traditionaliste ; CAA Nantes, 25 mars 2010, *Alabaev*, req. n° 09NT01345.

(49) TA Strasbourg, 11 avr. 2003, *M. Ahmed C. c/ Préfet du Bas-Rhin*, req. n° 02-02131 (refus d'agrèment d'un agent chargé du contrôle à l'aéroport, en raison de son passé de militant musulman actif).

(50) La mission du Conseil national des activités privées de sécurité (CNAPS) fait l'objet d'une définition par l'art. L. 632-1 CSI.

(51) Rainaud (A.), 2013, « La déontologie de la sécurité privée », *Quel avenir pour la sécurité privée* ?, Vallar (C.), Latour (X.) (dir.), PU Aix-Marseille, p. 107. Si on peut se féliciter de l'instauration d'un tel organe de contrôle, des insuffisances demeurent : « *les textes ne précisent pas qui peut saisir le CNAPS aux fins de contrôle. Cela n'empêche pas le processus de fonctionner certes, mais une précision serait la bienvenue* », Vallar (C.), « *Les contrôle : une procédure à parfaire* », *Quel avenir pour la sécurité privée* ?, p. 100.

Au terme de cette étude, une double remarque peut être effectuée. S'il est acquis que l'entreprise a investi avec succès le champ de la sûreté aéroportuaire, l'État n'a pas pour autant abandonné le terrain, car « *la sécurité privée n'a pas vocation à se substituer à la force publique mais à l'accompagner dans le respect des prérogatives qui sont les siennes*<sup>52</sup> ». Dès lors, c'est à une recomposition du rôle de l'État en matière de sécurité que l'on assiste et non à son retrait. Bien que la logique d'entreprise ne cesse de gagner du terrain, « *cette évolution ne veut pas dire pour autant qu'il [l'État] soit devenu un acteur comme un autre : la démonopolisation n'est pas synonyme de banalisation ; la dimension régaliennne se traduit par le fait que l'État reste la clef de voûte de ces secteurs, dont il fixe l'architecture d'ensemble et qu'il continue de superviser*<sup>53</sup> ». C'est ainsi un autre modèle d'État, intervenant dans ce service public particulier, avec lequel il faudra se familiariser et compter.

En outre, si l'État endosse désormais – spécialement dans les aéroports – les habits neufs d'un coordinateur de la mission de sécurité, il n'agit plus seul. Ce modèle de coproduction de la sécurité aéroportuaire s'inscrit dans un cadre désormais européen : car l'Europe, par

sa réglementation et la mise en place d'organismes de contrôle dédiés<sup>54</sup>, est « *partout, en arrière-plan de toutes les problématiques : elle semble devenue l'alpha et l'oméga des remèdes à l'insécurité et à "l'insûreté"*<sup>55</sup> ». On observe, au-delà de la mutation du rôle de l'État en matière de sécurité, une communautarisation de la sécurité aérienne, tant au niveau de la fixation des règles de sûreté qu'à celui du contrôle de leur mise en œuvre<sup>56</sup>.

Pour que la sûreté aérienne assure toujours mieux son rôle de service public incontournable et que l'avion reste le mode de déplacement le plus sûr de la planète, il faut sans doute qu'acteurs privés et publics continuent de conjuguer leurs actions sous le regard attentif de la puissance publique et de l'Europe. L'entreprise disposera assurément d'une place de premier ordre au sein de cet édifice renouvelé de la sécurité ■

(52) Gohin (O.), 2012, « La constitution, ultime obstacle à la privatisation de la sécurité ? », *Les cahiers de la sécurité*, INHES, Paris, La documentation française, n° 19, p. 18.

(53) Chevallier (J.), « La police est-elle encore une activité régaliennne », *op. cit.*, p. 15.

(54) Ainsi de la création de l'Agence européenne de la sécurité aérienne en 2002.

(55) Grard (L.), « Sécurité et sûreté du transport aérien », *La sécurité et la sûreté des transports aériens*, *op. cit.*, p. 206.

(56) Nicoud (F.), « La sécurité des transports aériens : un exemple pour l'Europe de la sécurité ? », *op. cit.*, p. 307.

# Les entreprises et la sûreté...

## Entre rêve et réalités

Jean-Philippe BÉRILLON

du Bloomberg prédisaient en janvier 2015 une quinzaine de nouveaux conflits dans le monde (*A pessimist's guide to the world in 2015*).

**D**e nombreuses enquêtes montrent que la gouvernance des entreprises a bien pris conscience des menaces qui se sont fait jour ces dernières années (cyber, fraudes, extrémisme, instabilité politique...) et qui s'amplifient aujourd'hui dans le domaine de la sûreté.

Or, les directions de la sûreté peinent encore à trouver une place légitime dans l'organisation de nos entreprises, comme celle d'un partenaire naturel de leur développement. C'est un paradoxe difficile à comprendre alors que les risques qui pèsent sur elles ne cessent de croître.

Les problématiques de sûreté ne sont pas nouvelles, mais force est de constater que nous n'avons pas connu autant de tensions géopolitiques depuis bien longtemps. Regardons rapidement le monde aujourd'hui, la liste est longue : la zone sahélienne, l'Algérie, la Libye, le Mali, Le Nigeria, l'Égypte, la Syrie, l'Irak, le Yémen, les tensions en mer de Chine, l'Ukraine...

Qu'elles soient dues à des tensions aux frontières, à l'instabilité gouvernementale, ou des phénomènes transnationaux, les entreprises évoluent dans un contexte sécuritaire marqué aujourd'hui par une extrême volatilité. Les experts américains

Je n'oublie pas les menaces criminelles et mafieuses qui s'expriment autant physiquement (corruption, blanchiment...) que dans le digital. Les problématiques telles que les vols de données, les tentatives de détournements de flux financiers ou les compromissions sont devenues quotidiennes.

En janvier 2015, alors que le Forum international de la Cybersécurité (FIC) tenait ses assises à Lille en présence des ministres de l'Intérieur français et allemand, la France faisait face à une vague de cyberattaques sans précédent. Une étude de PWC estime d'ailleurs à 177 300 le nombre d'attaques quotidiennes, au niveau mondial, soit une augmentation de 48 % entre 2013 et 2014.

Côté entreprises, les dirigeants semblent, globalement, parfaitement conscients des menaces et des risques qui pèsent sur leurs entreprises. Tous ont pratiquement été confrontés à des incidents lors de déplacements professionnels de leurs salariés ou de leurs expatriés. Ils ont pour la plupart déjà eu à gérer des crises dues à des événements internes ou externes perturbant le fonctionnement de leur activité. Aujourd'hui les incidents de sécurité concernant leur sécurité informatique (SI), cyberattaques,

Jean-Philippe BÉRILLON



Directeur Santé-Sécurité et Sûreté d'ENGIE Global Gaz & GNL de 2009 à 2016, Il a aussi eu

en charge la sûreté maritime, la cybermenace, et le devoir de protection de l'entreprise vis-à-vis de ses collaborateurs. Ancien officier de gendarmerie, breveté de l'École de Guerre et titulaire d'un DEA « politiques de défense et de sécurité » de l'IEP d'Aix-en-Provence, Il est aussi diplômé du Centre des Hautes Etudes de l'Environnement et du Développement Durable (CHEE & DD). Il vient de prendre le poste de Chief Security Officer d'ENGIE Middle-East, South & Central Asia and Turkey, à Dubai.



ingénierie sociale ou détournement d'informations, sont quasi quotidiens.

L'extrait du *Global CEO Survey 2013* de PWC repris ci-dessous l'illustre parfaitement. Il apparaît clairement que sur les huit scénarios identifiés par les Chief Executive Officer (CEO) interrogés sur ce qui pourrait avoir un impact majeur sur leur organisation, trois encadrés de rouge concernent des problématiques de sûreté : troubles sociaux majeurs, risques cyber, tensions politico-sociales et conflits.

Dans le même temps, alors que nous nous accordons tous aujourd'hui sur le constat que la prise de conscience du « risque sûreté » est bien entrée dans l'entreprise, nous pouvons légitimement nous interroger sur ce qu'il en est véritablement de la culture de sécurité et de sa traduction dans l'organisation et les missions des directions de la sûreté lorsqu'elles existent.

Pourquoi cette interrogation ? L'écart entre la prise de conscience du risque (et donc de l'exposition de l'entreprise) et l'organisation mise en place en son sein pour y faire face est assez surprenant. Il nous conduit légitimement à nous interroger sur la réalité souvent problématique des organigrammes, des budgets, des missions et du positionnement de la fonction dans l'entreprise.

À titre d'exemple, j'avais récemment une petite trentaine d'organigrammes sous les yeux, et sur seulement trois d'entre eux apparaissaient la fonction sûreté, rattachée à une autre direction fonctionnelle ou opérationnelle, et sur un seul, la direction sûreté apparaissait en tant que direction parfaitement identifiée.

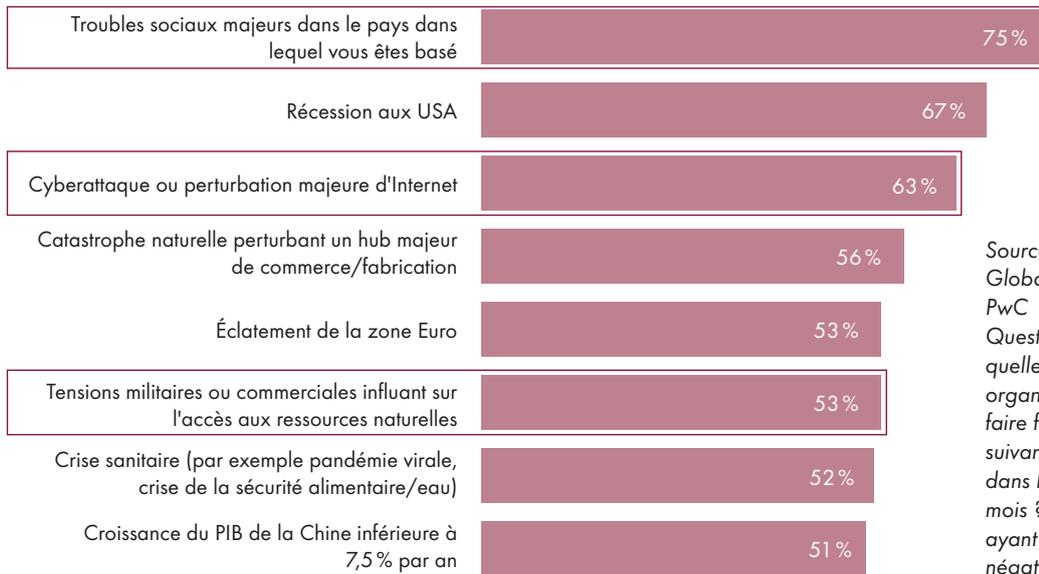
Lorsqu'elle apparaît sur l'organigramme, la direction sûreté est généralement rattachée au secrétariat général, ce qui est assez légitime. Sans secrétariat général, le sujet devient plus complexe, doit-on la rattacher aux opérations ? Aux ressources humaines ? Au juridique ? Aux risques ? Au HSE (santé, sécurité industrielle et environnement) ? Tout existe... C'est pourtant une fonction régaliennne. Faut-il alors la rattacher directement au directeur général ou CEO, éventuellement à son adjoint ? Il existe une forte probabilité pour que l'on vous réponde que ce n'est pas assez important pour cela. COO, CFO, CISO<sup>1</sup>, oui mais pas CSO<sup>2</sup>.

En 2013 déjà, le Club des directeurs de sécurité des entreprises (CDSE) publiait un livre sur la fonction sûreté dans l'entreprise : « *Il s'agit de convaincre tant les industriels que les pouvoirs publics que le directeur de la sécurité/sûreté a le savoir-faire, l'expérience et les connaissances requis pour déjouer la plupart des risques encourus par celle-ci* », expliquait Alain Juillet, président du CDSE.

(1) Chief operations officer, chief financial officer, Chief Information security officer.

(2) Chief security officer.

Scénarios qui, selon les CEO, auront les impacts les plus importants sur leur organisation



Source : 16th Annual Global Survey, 2013, PwC  
 Question : dans quelle mesure votre organisation pourrait faire face aux scénarios suivants, s'ils survenaient dans les 12 prochains mois ? (répondants ayant répondu "impact négatif").

## La direction de la sûreté fait-elle face à un blocage psychologique ?

Il semble, en effet, que les directions de la sûreté n'arrivent pas à trouver une place naturelle au sein des états-majors, au même titre qu'une direction juridique, financière, des ressources humaines ou de la stratégie...

Les directions de la sûreté souffrent peut-être, encore injustement, d'une réputation héritée d'un passé ambigu, de relations fantasmagoriques ou avérées avec des officines douteuses, de modes d'actions manquant de transparence et relevant de barbouzeries dépassées ou encore du comportement mytho-maniaque de certains individus qui habillent la fonction d'un halo de mystère qui n'a pas lieu d'être.

Il faut aussi se demander si nos dirigeants ont une connaissance suffisante de cette fonction pour pouvoir parfaitement l'intégrer dans la gouvernance de leur entreprise, comme un véritable « business partner ».

Savent-ils l'utiliser autrement que comme un extincteur en la sollicitant dans l'urgence pour régler un problème qui se fait jour ? Ne pourrait-on pas mettre, en amont, à la disposition des métiers de l'entreprise, les capacités et l'expertise qui sont les siennes ?

La problématique n'est pas tant liée à la fonction qu'à la culture. En effet, nos amis anglo-saxons ont une approche plus pragmatique et détendue de l'existence de cette fonction. Là, l'existence d'un security department ne pose pas de problème, bien au contraire.

Nous devrions reposer la question fondamentale de : « Qu'est-ce qu'exister dans une organisation ? ». Étymologiquement, du latin *ex stare* ou *ex sistere*, c'est être debout et stable, et donc de pouvoir agir. Agir, dans une organisation, c'est avoir un chef reconnu, une mission claire, des moyens adaptés, donc, être une réalité.

Or, combien de directeurs de la sûreté n'ont pas véritablement de budget « ou un budget inadapté » à la mission qui leur est confiée. Je ne voudrais pas dresser un tableau trop pessimiste du sujet, mais nous sommes bien ici dans la réalité du plus grand nombre, et si, pour la plupart, les grands groupes ont apporté des réponses adaptées et mures, au sein même de ce cercle plutôt privilégié, ce constat est d'actualité.

J'en veux pour preuve un article assez récent<sup>3</sup>, dont le rédacteur, directeur général du CDSE, est au cœur du sujet et parfaitement au fait des réalités actuelles. Il titrait « *La fonction sûreté en entreprise, une fonction encore méconnue* », s'étonnant tout particulièrement que certaines entreprises aient pu faire le choix, dans la conjoncture que nous

(3) Oliver Hassid (directeur général du Club des directeurs de sécurité des entreprises), *Le journal des directeurs sécurité d'entreprise*, Paris, avril 2015.

connaissons aujourd'hui, de supprimer tout simplement leur direction de la sûreté.

## Sommes-nous en train de vivre un paradoxe ?

Il s'agit bien en effet d'un paradoxe que vivent au quotidien nombre d'entreprises, puisque leur maturité en matière de sûreté peine à améliorer ses performances alors que les menaces sont constantes, qu'il s'en développe de nouvelles et que l'exposition aux risques devient aujourd'hui plus forte.

Il s'agit encore d'un paradoxe lorsque, dans le contexte sécuritaire que l'on connaît, l'expertise et les compétences des directeurs de la sûreté ne sont pas exploitées autant qu'elles pourraient l'être.

Alors que le devoir de protection de l'employeur vis-à-vis de ses salariés fait peser sur l'entreprise et ses dirigeants des risques importants<sup>4</sup> devant une juridiction civile ou pénale, qui mieux que cet expert en sécurité est à même d'identifier la menace et d'évaluer les risques, conseiller ses dirigeants et proposer les postures les plus adaptées ?

Il s'agit toujours d'un paradoxe quand aujourd'hui l'entreprise découvre les enjeux liés à son acceptabilité sur les territoires où elle doit s'installer et se développer, principe consacré au sein du concept éminemment transverse de responsabilité sociétale (RSE). Comment alors imaginer que la problématique de sûreté n'y serait pas intégrée ?

En effet, la complexité des territoires sur lesquels se développent les entreprises demande des diligences de

plus en plus fines, des analyses de plus en plus poussées pour leur permettre de s'installer en sécurité tout en respectant les cultures des populations qui les entourent, mais aussi en identifiant celles qui peuvent être de possibles ou probables prédateurs, ceci dans une logique de profitabilité partagée.

Contrefaçon, contrebande, travail clandestin, blanchiment de capitaux, opacité financière, fraude<sup>5</sup>, corruption, troubles sociaux et instabilité politique, terrorisme, piraterie, pénétration des mafias dans l'économie légale, toutes ces menaces pèsent sur l'entreprise et relèvent éminemment du champ d'action des directeurs de la sûreté.

Il n'y a pas de développement sans sécurité, sans sûreté.

Le coût pour les entreprises est significatif. Pour la fraude en France : alors qu'en 2009, 29 % des entreprises déclaraient avoir été victimes d'une fraude contre 30 % dans le reste du monde, en 2014 elles sont 55 % contre 37 % dans le reste du monde. Ces fraudes représentent moins de 90 000 € dans 65 % des cas, entre 90 000 € et 4,5 millions d'euros dans 28 % des cas et entre 5 et 90 millions d'euros pour 3 % d'entre elles<sup>6</sup>.

L'exemple du risque de sûreté maritime nous interpelle aussi chez ENGIE, puisque nous sommes armateurs et affrétons des méthaniers pour transporter le gaz naturel liquéfié (GNL). Pour ce qui concerne la piraterie en général, elle représente entre 2008 et 2014, quelque 2 386 navires attaqués, 50 morts et 3 741 otages dont 70 % ont démissionné. C'est une perte évaluée entre 7 et 12 milliards de dollars par an pour l'ensemble du commerce mondial, ce sont encore 75 millions de dollars de rançons versés chaque année. En 2014 la France a jugé urgent de légiférer sur la problématique de sûreté maritime<sup>7</sup>.

(4) Peuvent être engagées, d'une part, sa responsabilité civile : (faute inexcusable de l'employeur), « ... lorsque l'employeur avait ou aurait dû avoir conscience du danger auquel il exposait la victime et qu'il n'a pas pris les mesures nécessaires pour l'en préserver » ; et, d'autre part, sa responsabilité pénale (faute d'imprudance caractérisée - art.121-3 du Code pénal) : relevant de la responsabilité de « la personne qui a exposé autrui à un risque d'une particulière gravité qu'elle ne pouvait ignorer et qui s'est abstenue de prendre des mesures appropriées, mesures de prévention que la nature de ses missions ou de ses fonctions, le pouvoir et les moyens dont il disposait lui permettaient de concevoir ou de mettre en œuvre », réprimé par l'article 222-19 du Code pénal de 2 ans d'emprisonnement et de 30 000€ d'amende et par l'article 221-6 du même code de 3 ans d'emprisonnement et 45 000€ d'amende en cas de violation manifestement délibérée d'une obligation particulière de prudence ou de sécurité.

(5) La fraude continue à être une vraie menace pour les entreprises. 55 % des entreprises françaises ont été victimes d'une fraude au cours des 24 derniers mois ; 43 % des fraudes reportées par les entreprises françaises ont été détectées grâce à l'analyse informatique des données ; 44 % des entreprises françaises craignent à l'avenir un acte de cybercriminalité : [www.pwc.fr/enquetefraude2014](http://www.pwc.fr/enquetefraude2014)

(6) PWC, *Global Economic Crime Survey 2014*.

(7) Loi n° 2014-742 du 1<sup>er</sup> juillet 2014 relative aux activités privées de protection des navires. Communiqué de presse du conseil des ministres du 3 janvier 2014 : « Le ministre délégué auprès du ministre de l'Écologie, du Développement durable et de l'Énergie, chargé des transports, de la mer et de la pêche, a présenté un projet de loi relatif aux activités privées de protection des navires. Ce projet de loi, qui avait été annoncé par le Premier ministre lors du comité interministériel de la mer du 2 décembre dernier, vise à garantir la sécurité des navires confrontés au risque d'attaques de pirates sur certaines mers du globe. Il s'inscrit également dans la volonté de renforcement de la compétitivité du pavillon français et du transport maritime. En effet, la France était l'un des derniers pays européens à ne pas avoir autorisé la protection de navires par des entreprises privées. Outre les conséquences physiques ou psychologiques sur les marins, la piraterie a des conséquences économiques lourdes pour les armateurs, évaluées entre 7 et 12 milliards de dollars chaque année au niveau mondial ».

En septembre 2015, 211 kilogrammes de cocaïne ont été découverts par les forces de police et les douanes péruviennes à bord d'un méthanier. Il a été affrété par le passé par les plus grandes compagnies du secteur gazier. Auditions de l'équipage, coûts financiers de l'immobilisation, à cinquante mille dollars la journée de navigation d'un méthanier, le calcul se fait rapidement.

L'introduction de ce type de cargaison à bord n'est pas neutre, d'abord en termes d'image. Il souligne ensuite l'importance de la maîtrise des procédures de sûreté, en l'espèce du Code international pour la sûreté des navires et des installations portuaires (ISPS pour *International Ship and Port Security*), dans un contexte de menace de terrorisme maritime constante aujourd'hui et qu'il ne faut pas oublier. Il montre aussi qu'il existe un vrai sujet sur ce que nos amis anglo-saxons appellent « insiders threats » pour l'ensemble des entreprises, traité conjointement entre RH et sûreté.

## Alors quelle place pour la sûreté au sein de l'entreprise ?

C'est effectivement la véritable question. Comment les dirigeants doivent-ils utiliser leur direction de la sûreté pour qu'elle participe pleinement à la création de valeur au sein de leur entreprise ? Dépasser le stade de la poule à qui on aurait donné un couteau...

Le sujet de la sûreté est bien celui de la détection et de la prévention d'un certain nombre de risques qui drainent avec eux une capacité à perturber ou stopper le fonctionnement normal de l'activité, nuire à l'image, déstabiliser les dirigeants. C'est aussi celui de mettre en place les conditions de la continuité d'activité pour faire face aux situations de crise prévisibles ou non, et d'être résilient.

Ce qui est certain, c'est qu'une direction de la sûreté, un CSO, ne doit pas être utilisé comme un extincteur, accroché inerte à un mur et activé lorsqu'un incident survient.

La fonction sûreté, éminemment transverse au sein d'une direction générale, se caractérise par essence par des mots comme « anticiper », « aider à la décision », « donner une respiration en situation de crise ou d'urgence ». Sa fonction de conseil est naturelle comme toute direction fonctionnelle, mais en ce qui la concerne elle comprend aussi une dimension opérationnelle.

Dans le domaine d'expertise qui est le sien, relevant des menaces externes ou internes malveillantes, le directeur de la sûreté prévient des risques dont nous avons parlé plus haut, limite l'exposition physique des salariés, l'exposition juridique (on l'oublie trop souvent) de l'entreprise et de ses dirigeants. Il accompagne les collaborateurs pour qu'ils puissent, partout où ils sont amenés à se déplacer, exercer leur activité dans les meilleures conditions de sécurité. La direction de la sûreté concourt ainsi à la création des conditions de la réussite. S'inscrivant dans la démarche responsable de l'entreprise, l'attachement à la qualité de l'environnement de travail des salariés, même et surtout dans les zones à risque, permet à l'entreprise d'attirer et de retenir les talents, d'être plus compétitive, d'améliorer son image.

Les grands groupes souhaitent aujourd'hui intégrer les indices extra-financiers les plus reconnus, comme le Dow Jones Sustainability Index (DJSI) World et Europe<sup>8</sup>.

L'attention portée à la sûreté des collaborateurs et donc au développement du capital humain permet aussi à l'entreprise de se démarquer de ses concurrents, apportant un avantage déterminant en incitant ses clients à lui donner la préférence en raison de son engagement et de sa maturité en matière de sûreté et de sécurité.

Le débat fondateur sur la place de la sûreté dans l'entreprise reste donc à construire avec ses principaux acteurs : les dirigeants des entreprises et les directeurs de la sûreté. Alors pourquoi ne pas initier ce débat, porté par le Mouvement des entreprises de France (MEDEF), le CDSE ou encore l'AGORA des directeurs de la sécurité ? ■

*Les directions de la sûreté souffrent peut-être, encore injustement, d'une réputation héritée d'un passé ambigu, de relations fantasmagoriques ou avérées avec des officines douteuses, de modes d'actions manquants de transparence et relevant de barbouzeries dépassées ou encore du comportement mytho-maniaque de certains individus qui n'a pas lieu d'être.*

(8) Établis par l'agence de notation extra-financière RobecoSAM.



## L'entreprise au cœur de la coproduction de sécurité – quels enjeux, quels leviers ?

Thierry COUDERT

Considérer l'entreprise sous l'angle de la sécurité n'était pas, il y a quelques années encore, un mode habituel d'approche. Mais l'inflation des normes, l'émergence du principe de précaution, la judiciarisation de la société, la montée des préoccupations environnementales auxquelles s'ajoutent la fin des trente glorieuses, puis la sortie de la guerre froide et la fin d'un monde sécurisé sous l'hyper-puissance américaine, enfin et surtout la multiplication des phénomènes de radicalisation, ont pourtant progressivement fait entrer la notion de risque au cœur des préoccupations de l'entreprise. Celle-ci est devenue, sans qu'elle le veuille véritablement, un acteur de la sécurité.

Comme tout acteur économique, l'entreprise se doit d'assurer sa sécurité et de maîtriser les risques qu'elle peut engendrer pour la société comme ceux qu'elle peut rencontrer dans l'exercice de son activité. Elle peut assumer elle-même cette fonction ou recourir à des prestataires de sécurité privée ou plutôt de sécurités privées si l'on considère la diversité des risques. Dès lors, l'entreprise est à la fois sujet et objet de la sécurité. Il importe donc de la considérer sous ce double aspect.

Dans ce contexte, comment les entreprises font-elles face aux risques ? Comment la fonction sûreté/sécurité est-elle intégrée à la structure de l'entreprise ? De quelle manière les pouvoirs publics peuvent-ils aider les entreprises ? Les réponses données à ces questions sont lourdes de conséquences pour le devenir des entreprises, mais aussi de la société dans son ensemble.

Thierry COUDERT



Délégué aux coopérations de sécurité au Ministère de l'Intérieur.

## Devant la multiplicité des risques, comment les entreprises font-elles face ?

Afin de se démarquer des approches habituelles, nous regarderons d'abord l'entreprise en tant que bénéficiaire de sécurité avant de s'intéresser aux prestataires de sécurité.

### *L'entreprise en demande de sécurité*

Aujourd'hui, la couverture du facteur « risques » figure souvent au bilan des entreprises. La sécurité au sens large est ainsi devenue comptablement un centre de coût. Au-delà de l'aspect purement financier, les entreprises ont aussi appris, peu à peu, à prendre physiquement en compte les risques, à y répondre soit personnellement, soit par prestataires interposés en complément des actions menées par les acteurs publics. Toutefois la fonction sécurité occupe une place variable au sein des sociétés. Dès lors, l'entreprise doit considérer à la fois la fonction sécurité, c'est-à-dire le risque accidentel, et la fonction sûreté, c'est-à-dire la lutte contre la malveillance. Ces fonctions peuvent, le cas échéant, être confiées à deux ou plusieurs structures différentes de l'entreprise ou regroupées au sein d'une même entité.

Si l'appellation de directeur de la sécurité ou de la sûreté s'est banalisée, cette fonction concerne essentiellement les grandes entreprises. De plus, son positionnement n'est pas forcément très haut au sein de la hiérarchie des cadres dirigeants. La fonction n'est, en effet, pas toujours considérée comme stratégique, à tort semble-t-il, et recouvre des catégories de risques différents selon les entreprises. Lorsque la fonction n'est pas une entité autonome elle fait alors l'objet d'un cumul avec une autre fonction. C'est le plus souvent le cas au sein des entreprises de taille moyenne, et dans les petites et moyennes entreprises c'est souvent le dirigeant lui-même qui l'assume.

La fonction sécurité ne se traduit pas forcément par l'existence d'un service interne de sécurité. L'arbitrage vers une sous-traitance totale ou partielle de la couverture des risques est lié à la capacité financière des entreprises à assumer la charge à temps plein de personnels dédiés aux risques identifiés à comparer à une sous-traitance plus facile à dimensionner en termes d'effectifs et de temps de travail.

Voici donc pour la fonction, mais à quels risques s'applique-t-elle ? Ceux-ci se sont en effet diversifiés : malveillance, risque sanitaire, risque social, risque économique, risque de perte d'image, cybersécurité, et bien sûr le risque terroriste qui monte en puissance. Dans tous les cas, force est de constater que l'entreprise ne peut pas répondre seule à l'ensemble de ces risques.

De plus, les entreprises ne sont pas homogènes dans leur comportement en raison même de la variabilité de leur capacité à mobiliser les ressources humaines nécessaires, de la nature de leur « production », de leur localisation géographique.

C'est pourquoi, au risque d'être abrupts, posons nous alors la question : est-il rentable pour l'entreprise d'assumer le coût de la sûreté et de la sécurité ? La réponse est évidemment oui, mais l'entreprise doit-elle et peut-elle prendre en charge le coût de tous les risques ? La réponse sera ici plus nuancée.

À travers la fonction sécurité, l'important pour l'entreprise est de sécuriser son processus de production en évitant les risques accidentels. Plus ce processus sera dangereux, plus l'entreprise sera amenée à investir dans la sécurité. Ainsi, une raffinerie du type de celles de l'étang de Berre, c'est-à-dire proche d'une grande agglomération, ou les industries du couloir de la chimie au sud de Lyon, auront un coût sécurité par agent élevé comparativement à des entreprises d'autres secteurs de production. C'est également le cas d'une centrale nucléaire qui doit assumer la prévention de risques physiques importants comme le crash d'un avion tout en mettant en place des équipes nombreuses de sécurité associant des agents EDF, des agents de prestataires de sécurité et des pelotons spécialisés de gendarmerie dont elle assume le coût financier. De même les grandes entreprises implantées dans des zones géographiques à risques naturels importants, y compris et surtout à l'étranger, doivent nécessairement en assumer la charge, notamment en termes d'assurance. Ce coût de production est inhérent à l'entreprise et doit être pris en compte en cas de transmission ou de rachat des actifs par une autre entité.

Bien que ces risques soient le plus souvent objectifs, force est de constater que l'entreprise est plus dans la réaction que la prévention. C'est une attitude qui va devoir évoluer, notamment sous la pression des assurances et des médias. On constate que plus une entreprise est importante, mieux les risques sont évalués et couverts. Pour les grandes entreprises, leur surface financière est suffisante pour une prise en charge des risques accidentels. Dans les entreprises de taille intermédiaire cette capacité

est moindre et plus encore dans les PME. Dans ces derniers cas, un arbitrage coût-avantage s'opère sous la responsabilité du dirigeant.

La fonction sûreté est elle aussi diversement prise en compte. Or, la protection de l'entreprise contre les malveillances apparaît plus nécessaire que jamais en raison de la croissance et de la diversification de la délinquance. Les risques sont bien connus : intrusions malveillantes, cyberattaques, agressions physiques du personnel, escroqueries, chantages... L'entreprise peut répondre à ces risques soit en se dotant des capacités de réaction propres à éradiquer chacun d'entre eux par la création de services internes spécialisés, soit en recourant à des prestataires spécialisés (agents de surveillance et de gardiennage, sociétés de vidéoprotection, informaticiens spécialisés...).

Il n'existe pas un ratio de référence pour les deux centres de coût (sécurité et sûreté). Il revient aux titulaires des fonctions, lorsqu'ils existent, de convaincre les états-majors ou le dirigeant du bien-fondé des taux de couverture proposés en face de chaque risque.

Toutefois, une catégorie d'entreprises est contrainte d'investir spécifiquement dans la sécurité : les opérateurs d'importance vitale dont la continuité de l'activité est indispensable à la vie de la population. Douze secteurs d'importance vitale ont été répertoriés. Plus de 200 entreprises sont concernées, notamment dans les secteurs des transports, de l'énergie, de la santé et de l'eau. Il revient à chaque opérateur d'identifier, dans son système de production, les points névralgiques et de les proposer comme points d'importance vitale devant faire l'objet d'une protection particulière. L'opérateur doit former spécifiquement ses responsables de la sécurité et mettre en place un double système de sécurité : un plan de sécurité pour l'ensemble de ses activités et des plans particuliers de protection pour chacun de ses points d'importance vitale.

Pour la plupart des entreprises c'est la sous-traitance qui est privilégiée au détriment de services propres. On trouve également des structures intermédiaires dans lesquelles une partie du personnel appartient à l'entreprise et accueille également du personnel appartenant à des prestataires. Lorsqu'une entreprise est implantée sur

plusieurs sites, les choix peuvent être différents de l'un à l'autre.

L'actualité se charge régulièrement d'illustrer le bien-fondé d'une prise en compte des risques. Ainsi, lorsqu'une PME est victime d'une grave escroquerie de comptabilité mettant à bas sa trésorerie, c'est la survie de l'entreprise qui est en jeu avec à la clé la disparition potentielle de quelques emplois locaux. Lorsque le système informatique d'une entreprise est attaqué, c'est au mieux un savoir-faire pillé, au pire la disparition de l'ensemble des données concernant la société, entraînant un préjudice important pouvant toucher les processus industriels, les données individuelles relatives au personnel, voire la fuite de secrets de fabrication liés à des brevets déposés par l'entreprise. Lorsqu'un personnel est enlevé à l'étranger, c'est la confiance interne en l'entreprise qui peut être ébranlée. Lorsqu'un risque naturel a été mal évalué, c'est le cycle de production qui peut être affecté. Lorsque qu'une entreprise fait l'objet de vols, de malveillances physiques ou pire encore de sabotage, le préjudice financier peut être élevé ou la vie de l'entreprise gravement perturbée.

*Même improbable, un préjudice altère l'image de l'entreprise qui apparaît en défaut de prévision. Le principe de précaution, il faut le rappeler, est très vite invoqué, notamment dans le domaine environnemental. La responsabilité personnelle des dirigeants peut être mise en cause et fait dans tous les cas l'objet d'une médiatisation immédiate via les médias ou les réseaux sociaux.*

Même improbable, un préjudice altère l'image de l'entreprise qui apparaît en défaut de prévision. Le principe de précaution, il faut le rappeler, est très vite invoqué, notamment dans le domaine environnemental. La responsabilité personnelle des dirigeants peut être mise en cause et fait dans tous les cas

l'objet d'une médiatisation immédiate via les médias ou les réseaux sociaux.

Toutefois, ainsi qu'il a déjà été dit, il ne serait pas légitime que celui-ci ne soit pas partagé.

## **Les entreprises prestataires de sécurité**

Nous venons d'envisager la sécurité du point de vue de l'entreprise qui couvre les risques auxquels elle est confrontée. Il faut maintenant considérer les entreprises qui ont pour vocation d'assurer la sécurité de personnes et de biens dans leur sphère privée et dans un cadre contractuel, au premier rang desquelles figurent les entreprises de sécurité privée régies par le livre VI du Code

de la sécurité intérieure (CSI). Celles-ci sont, par nature, productrices de sécurité. La sécurité est ainsi devenue un marché important et de plus en plus pointu.

En ne considérant que la seule « prévention-sécurité », le rapport de la branche pour l'année 2014 nous rappelle que 9 870 entreprises œuvrent directement pour la sécurité des entreprises et des citoyens. Ces entreprises comptent près de 152 000 salariés. Parmi celles-ci, 29 ont plus de 500 salariés et 10 plus de 2 000. Ce secteur comprend donc des acteurs économiques importants. Le chiffre d'affaires global est de 5,7 milliards d'euros. Ces chiffres peuvent paraître élevés, mais il faut considérer qu'ils concernent conjointement les activités de surveillance et de gardiennage, de transports de fonds, de vidéosurveillance et de protection rapprochée.

La sécurité privée a pour rôle d'assurer la sécurité du domaine privé des personnes physiques ou morales, les forces de sécurité de l'État et les polices municipales ayant, en simplifiant, en charge la sécurité des espaces publics. Sa place au sein des acteurs de la sécurité est désormais pleinement reconnue en raison de la politique de professionnalisation et de moralisation qui a été menée conjointement par la branche et les pouvoirs publics depuis plusieurs années. Cette évolution était indispensable pour crédibiliser les entreprises. Elle était aussi nécessaire pour faire évoluer le secteur vers une plus grande efficacité économique à travers des modifications d'une législation qui datait pour l'essentiel de 1983, époque de forte défiance à l'égard de la sécurité privée.

En effet, le livre VI avait certes évolué depuis 1983, mais sans remise en cause de l'esprit de fond et la formation restait notamment un maillon faible, étant absente du champ du livre VI. Il fallait donc aller plus loin.

La création en 2011 du poste de Délégué interministériel à la sécurité privée, devenu en 2014 Délégué aux coopérations de sécurité, a entendu manifester la volonté gouvernementale de réformer le secteur. Celle, en 2012, du Conseil national des activités privées de sécurité (CNAPS), avait précédé cette évolution avec pour objectif de mieux réguler et contrôler ce secteur réglementé, en plein accord d'ailleurs avec les organisations professionnelles. La sécurité privée offre ainsi le visage singulier d'un secteur à accès réglementé, soumis à un organisme de contrôle voulu par les organisations professionnelles représentatives et financé par les entreprises.

Beaucoup reste à faire toutefois pour moderniser les textes, nous y reviendrons, mais le secteur bénéficie néanmoins d'une bonne image.

Ainsi, selon un sondage IPSOS en 2013, 69 % des Français reconnaissent positive la contribution des entreprises de sécurité privée et 59 % estiment qu'elles constituent un atout pour la sécurité. En outre, 70 % des Français pensent que la présence des agents de prévention-sécurité améliore leur sentiment de sécurité. Cette bonne image est liée au fait que la sécurité privée répond à une demande sociétale multiple :

- une demande des entreprises en liaison avec la nécessité de protéger leur patrimoine matériel et immatériel, notamment en période de crise économique et de concurrence forte. Il s'agit même d'un intérêt de défense économique sur lequel l'État a un droit de regard pour certains domaines sensibles. En période de crise économique, les entreprises font de plus face à des vols basiques ;
- une demande de la sphère publique qui, à cet égard, se comporte comme une entreprise privée. L'État tend à faire surveiller de plus en plus ses emprises et ses bâtiments par des sociétés privées afin de consacrer ses forces de l'ordre à un spectre plus haut de délinquance. Les collectivités territoriales font de même et les campus hospitaliers ou universitaires suivent la même tendance ;
- une demande sociale liée au vieillissement de la société entraînant un souhait plus fort de tranquillité, notamment dans les nouvelles formes d'urbanisme et d'habitat, ce qui pousse au développement de la vidéosurveillance.

## Quel appui des pouvoirs publics ?

Les pouvoirs publics ont en charge la sécurité générale de la nation et prennent en compte les entreprises à ce titre.

L'État a ainsi en charge la coordination de la lutte contre les calamités naturelles et la politique générale de prévention contre les risques naturels ou technologiques. Les entreprises peuvent ainsi compter sur des moyens de grande ampleur. Cela vient compléter leurs efforts propres consentis pour sécuriser les cycles de production (prévention incendie, prévention santé, formation du personnel, exercices communs avec les pouvoirs publics). L'État dispose aussi des forces nationales de sécurité chargées de la sécurité générale. Le constat peut être fait que l'existence de capacités extérieures d'intervention n'a pas dispensé les entreprises, y compris les entreprises de services pour lesquelles les risques sont moindres, de réfléchir par elles-mêmes à leur propre sécurité.

L'État, en tant que gardien du droit de la sécurité privée, souhaite faire évoluer la législation en la matière afin

de mieux répondre à l'évolution de la société. C'est la vocation de la délégation aux coopérations de sécurité, directement placée auprès du ministre de l'Intérieur, qui veille en outre à maintenir un dialogue permanent avec tous les acteurs afin de promouvoir leur coopération avec les autres forces de sécurité, nationales ou municipales, sur le terrain.

Le ministre de l'Intérieur a ainsi présenté le 8 décembre 2014, devant les 3<sup>e</sup> Assises de la sécurité privée, un plan de plus de trente mesures qui s'articule autour de deux axes : améliorer la formation, condition essentielle de la professionnalisation et donner plus de liberté à la profession. Ce plan a d'ores et déjà été concrétisé par l'entrée de la formation au sein du livre VI du Code de la sécurité intérieure par l'article 40 de la loi relative au dialogue social et à l'emploi, la clarification par circulaire de la procédure de levée de doute relative aux alarmes déclenchées par les systèmes de surveillance électronique et l'assouplissement, également par circulaire, des règles d'emploi des agents doublement qualifiés sécurité incendie (SSIAP) et sécurité privée.

Le ministre entend également répondre aux nouveaux besoins de sécurité. À ce titre, le chantier le plus important est celui de la mise en place de véritables coopérations opérationnelles sur le terrain, la coproduction de sécurité étant une solution susceptible de contribuer à garantir une meilleure sécurité globale en France. De telles coopérations reposent sur un système gagnant-gagnant : le secteur privé montre son savoir-faire et gagne en crédibilité grâce à la reconnaissance des pouvoirs publics, tandis que les services de l'État peuvent se recentrer sur leurs missions de police administrative et judiciaire, gagnant ainsi en efficacité opérationnelle. Nous devons donc approfondir ces coopérations de sécurité, en nous inspirant, le cas échéant, des bonnes pratiques en vigueur à l'étranger. Une réflexion est ainsi en cours pour que des conventions de coopérations puissent émerger dans des zones où coexistent différents acteurs et où par ailleurs une délinquance répétitive est avérée. Elle devrait aboutir prochainement à la signature d'une circulaire par le ministre de l'Intérieur. La convention type entre l'État et les centres commerciaux avait déjà montré l'utilité de faire travailler en commun les acteurs.

La notion de coopération est en effet essentielle au moment où l'État ne peut pas tout faire. Elle se fait évidemment dans le respect scrupuleux des compétences de chaque acteur. Les grands événements culturels ou sportifs, au même titre que les événements locaux organisés par les collectivités locales, qui sollicitent plus qu'auparavant la sécurité privée, en sont une bonne illustration.

L'Euro 2016 sera à cet égard particulièrement emblématique puisque ce sera le plus grand événement français en termes de sécurité privée. 51 matchs dans dix villes hôtes devront être sécurisés sur un mois, plus des « fan zones », en nombre aujourd'hui non déterminé, qui accueilleront un public nombreux. Tous ces événements vont nécessiter la présence de plusieurs milliers de professionnels de la sécurité privée. Les forces de sécurité de l'État seront aussi mobilisées pour la sécurité des espaces publics. Il sera utile pour l'avenir de tirer le bilan de l'Euro 2016 afin d'affiner les modes d'action et de collaboration et en tirer une doctrine d'emploi. On mesure bien à cette occasion le rôle décisif de la sécurité privée sans laquelle l'État ne pourrait pas assumer seul la sécurité des grands événements et la notion de coproduction de sécurité devient ici concrète.

*Il sera utile pour l'avenir de tirer le bilan de l'Euro 2016 afin d'affiner les modes d'action et de collaboration et en tirer une doctrine d'emploi. On mesure bien à cette occasion le rôle décisif de la sécurité privée sans laquelle l'État ne pourrait pas assumer seul la sécurité des grands événements et la notion de coproduction de sécurité devient ici concrète.*

La réussite de l'euro 2016 est indispensable pour démontrer la capacité de la France à organiser des grands rassemblements notamment dans le cadre de la présentation de la candidature de Paris aux jeux olympiques d'été de 2024 et l'exposition universelle. Les grands événements de ce type sont de plus en plus nombreux, c'est pourquoi les fédérations sportives sont très mobilisées sur ce thème. L'existence de la Délégation aux grands événements sportifs montre d'ailleurs la volonté de l'État de coopérer avec les professionnels. De même les responsables des foires et salons sont attentifs à ce que la France reste attractive en étant très vigilante sur les règles de sécurité.

Enfin, dans le même esprit, a été mis en place dans le quartier d'affaires de La Défense, depuis juin 2015, un dispositif « Vigie » qui associe les agents de sécurité des différentes entreprises et les forces de sécurité de l'État. L'objectif est d'acquiescer un langage et des réflexes communs par rapport aux risques spécifiques du quartier

qui compte de nombreux sièges sociaux de grandes entreprises et voit passer chaque jour un flux important de population. De plus, une information régulière sur l'évolution des risques est réalisée. Si ce dispositif s'avère efficace, il sera appelé à être implanté sur d'autres sites.

Mais l'État ne s'occupe pas seulement de sécurité par la présence de forces de l'ordre sur le terrain. Il est aussi à l'écoute directe des entreprises. C'est notamment dans cet esprit que la délégation aux coopérations de sécurité et le Club des directeurs de sécurité/sûreté en entreprises ont signé une convention de partenariat en 2014, faisant de la délégation le point unique d'entrée pour toutes les questions posées au ministère de l'Intérieur par les directeurs de sécurité des entreprises, pour une plus grande réactivité aux questionnements.

Les entreprises peuvent également compter sur les services de police judiciaire pour la recherche des auteurs d'infraction, de crimes et de délits. Les entreprises peuvent à cet effet adresser leurs plaintes aux services locaux de police judiciaire ou aux différents services spécialisés dans les litiges relatifs à un secteur particulier : Office central de lutte contre la délinquance itinérante en cas de vol de métaux par exemple, Office de lutte contre le crime organisé, Office central de répression de la grande délinquance financière, Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Les entreprises peuvent en sens inverse aider les offices en les alimentant en informations leur permettant d'affiner leurs recherches et s'engager ainsi avec eux dans une coproduction de sécurité à plus long terme.

Deux autres services, qui ne sont pas directement en contact avec le public, sont également actifs et peuvent à l'occasion aider les sociétés :

- la direction générale de la Sécurité intérieure qui relève directement du ministre de l'Intérieur ; elle est, tout à la fois, un service de renseignement et un service de police judiciaire spécialisé. Elle agit notamment en matière de contre-terrorisme et de lutte contre la cybercriminalité ;
- la Délégation à la coopération internationale dont le rôle est la coopération technique et opérationnelle.

Il faut rappeler également que le ministère de l'Intérieur a créé un poste de préfet en charge de la coordination de la lutte contre les cybermenaces au début de l'année 2015.

Le Secrétariat de la défense et de la sécurité nationale aide quant à lui les entreprises des douze secteurs d'importance vitale qui ont été définis par un arrêté du 2 juin 2006,

modifié le 3 juillet 2008, en mettant à leur disposition un guide méthodologique pour les aider à élaborer leur dispositif spécifique de sécurité.

## Quelles perspectives pour demain ?

Après ces quelques réflexions, on mesure mieux combien les entreprises sont, sous différentes façons et très concrètement, des producteurs de sécurité. Des réglementations sont certes en place, des services coopèrent, mais il faut continuer à évoluer en commun. Le monde est en effet en plein bouleversement et pour paraphraser et contredire le propos de Francis Fukuyama, on peut être sûr que ce n'est pas la fin de l'histoire. La menace continue à évoluer et le terrorisme non plus étatique mais individuel devient une vraie menace. Parallèlement, la résilience de la nation tend à diminuer.

Or, la sécurité est une condition du bien-être de chacun et un atout pour le développement économique. Les acteurs économiques demandent toujours plus de sécurité : ils souhaitent pouvoir vivre, travailler et se déplacer en tous lieux de notre territoire en toute tranquillité. La demande de sécurité de proximité est réelle. De même, les entreprises visent à réaliser leurs activités hors de tout acte de malveillance et ont des besoins de sécurité de plus en plus divers. On demande de plus en plus à l'État et parallèlement la sécurité privée se développe.

Plus que jamais, face à ces demandes, la sécurité ne peut être que le fruit des efforts de tous, État, collectivités locales, entreprises, citoyens. Les entreprises doivent plus encore être des partenaires de confiance, c'est la volonté du ministre de l'Intérieur et c'est le rôle de la Délégation aux coopérations de sécurité d'y parvenir. Les entreprises dans leur ensemble ne doivent pas être passives face aux problèmes de sécurité, mais il convient aussi d'être à leur écoute pour mieux les aider.

En sens inverse, les entreprises ne doivent pas avoir peur de collaborer avec les services de police afin de les aider à percevoir le plus rapidement possible les évolutions de la délinquance et élaborer des ripostes efficaces.

Plus généralement, la diffusion d'une culture de la sécurité passe par la capacité des acteurs à anticiper les risques, c'est pourquoi la diffusion de l'information est une vertu essentielle : connaissance de la situation d'un pays en cas de déplacement ou d'installation d'un collaborateur à l'étranger, connaissance des dernières méthodes d'agressions informatiques, information en temps réel sur

la délinquance de proximité dans les lieux d'implantation des entreprises, etc.

*In fine* il conviendra de réfléchir à moyen terme, par exemple 2020, à l'évolution des menaces, notamment dans les secteurs d'importance vitale, mais aussi des métiers de la sécurité en entreprise afin de définir précisément les profils des futurs responsables.

Cela concerne au premier chef les directeurs de la sécurité, mais aussi les responsables informatiques, les responsables du personnel pour détecter les agents pouvant être une menace potentielle en cas de radicalisation au travail. Cela concerne aussi les responsables de la formation pour sensibiliser tous les agents aux risques et mettre en place une culture d'entreprise spécifique. Cela concerne enfin et surtout les managers eux-mêmes dont la responsabilité personnelle peut être mise en cause. Afin de donner aux dirigeants d'entreprises les moyens d'être des décideurs efficaces en matière de risques, la mise en place d'une norme, ou d'un référentiel, en management de la sécurité/sûreté pourrait, en outre, leur donner des outils objectifs de décision.

Parallèlement des analyses devront être faites pour apprécier le bon niveau d'équilibre entre compétences internes et recours à des prestataires.

Enfin, l'amélioration de la prise en charge des risques ne devra pas se faire au détriment des libertés, au risque sinon de ne pas rencontrer l'adhésion sociale nécessaire et faire considérer certaines mesures de sécurité comme inacceptables. Cette condition est déterminante pour que les entreprises, déjà largement coproducteurs de sécurité, participent mieux à la résilience de la nation.

Il est évident que tout ne passe pas par des réglementations et il importe que le dialogue entre les acteurs se poursuive, c'est là la tâche exaltante de la délégation aux coopérations de sécurité ■



# Construire un nouveau contrat de confiance public-privé en matière de sécurité

Groupe de veille et d'analyse Richelieu. 18<sup>e</sup> session nationale spécialisée « Protection des entreprises et Intelligence économique » des auditeurs de l'INHESJ<sup>1</sup>

*Contributeurs membres du GVA Richelieu*

*Président du GVA : Jean-Louis BRUNIN*

*Pascal BITOT PANELLI, Xavier CARRE, Bruno DOMINGO, Raphaël FAGIANI,*

*Michel GUILLOT, Angélique GUZMAN, Loïc LE GALL*

*Encadrement INHESJ : Delphine SEGUIER*

**A**u sein de notre société, fondée sur une culture politique étatiste et centralisatrice, la sécurité est appréhendée comme une matière régaliennne. L'État, transcendant les intérêts particuliers et défenseur de l'ordre public dans le cadre national, est conçu comme l'ultime garant de l'intérêt général et de la protection de la population. Dès lors, concevoir une sécurité qui soit « privée » peut apparaître « hors de propos », voire peut

susciter une certaine méfiance chez des citoyens attachés aux valeurs d'égalité. Cette sécurité, « privée » et « marchande », a ainsi longtemps eu mauvaise presse. Il est vrai que les opérateurs privés de sécurité ont souvent évolué dans un espace marginal et obscur, au service d'intérêts particuliers, qu'ils soient industriels, commerciaux, ou politiques. Un processus de réforme, visant à réglementer et moraliser leurs activités, a été entamé au début des années 1980. Il a permis une forte extension de ce secteur, dont l'évolution vient aujourd'hui questionner le périmètre des modalités d'intervention de l'État.

(1) Cet article a été écrit à partir d'un rapport élaboré par un Groupe de Veille et d'Analyse (GVA) de la 18<sup>e</sup> session nationale spécialisée (2015) animée par le Département Intelligence et sécurité économique de l'INHESJ.

De nombreuses influences travaillent le modèle français de sécurité publique qui tente de se réinventer dans le cadre de la mondialisation et de certains modèles libéraux qui défendent un « moins d'État » et/ou un « mieux d'État ». De même, le contexte de menace terroriste enregistré en France à la suite des attentats du 11 janvier et du 13 novembre 2015 implique de repenser la mobilisation des forces et des ressources de sécurité. Ces paramètres conduisent à examiner la position de la sécurité privée marchandisée par rapport à la sécurité publique et au monopole traditionnel revendiqué par l'État en la matière. Quel est désormais l'avenir de ce secteur privé de la sécurité ? La logique de relatif *statu quo* qui semble aujourd'hui prédominer est-elle satisfaisante pour l'État et pour les acteurs du marché ? Quel modèle de « coproduction de sécurité » entre l'État et le marché est-il possible de proposer qui soit à la fois défendable du point de vue tant politique et sociétal qu'économique et professionnel ? Répondre à ces questions implique de débattre sous un angle stratégique du monopole régalién de l'État et de ses services en matière de sécurité, d'une part, et de la place du marché et des acteurs privés, d'autre part. En effet, dans le cadre français, les deux enjeux sont indissociablement liés. Un modèle d'ensemble, articulant dimensions publiques et privées, n'existe pas aujourd'hui ou, tout du moins, n'a pas été véritablement explicité. Il implique de s'accorder sur les normes juridiques et professionnelles à établir, sur les instances de régulation à mettre en place et sur les modalités de financement à définir. Il est néanmoins possible de mettre l'accent sur plusieurs constats et enjeux centraux devant être pris en considération pour faire évoluer le modèle de coproduction de la sécurité entre acteurs publics et privés :

- une croissance régulière des besoins de sécurité, devenue une exigence sociétale dans un monde multipolaire, ouvert à toutes les innovations, comme à tous les dangers ;
- un État qui doit répondre impérativement à cet appel sociétal, tout en tenant compte, simultanément, de son efficience au regard de la limitation de ses moyens ;
- un État qui se positionne davantage en tant que régulateur et contrôleur de la fonction de sécurité, sans néanmoins jamais abandonner certaines de ses missions « cœur de métier » (renseignement, police judiciaire, ordre public) ;
- un secteur privé et marchand qui doit accepter de coproduire avec l'État cette fonction de sécurité, en déterminant avec lui une répartition des missions qui réponde au mieux, tant qualitativement que quantitativement, à une demande sociétale de plus en plus étendue et diversifiée.

En conclusion, il s'agit désormais de construire les fondements d'un nouveau contrat de confiance entre le secteur public (État et collectivités locales) et celui de la sécurité privée. Comme le souligne le président du CDSE, Alain Juillet, les propositions d'évolution du secteur de la sécurité privée doivent se fonder sur un esprit de consensus : « *Il faut réfléchir ensemble. Je défends en France le partenariat public privé, car je pense qu'il est indispensable. Je ne crois pas que l'État puisse s'en sortir tout seul en imposant la vision de son administration. On le voit tous les jours. Et je ne crois pas non plus que les entreprises puissent s'en sortir toutes seules. Je pense qu'il faut qu'il y ait un ensemble* » [Juillet, 2014]. Il s'agit, en effet, de définir de nouvelles modalités de gouvernance pour les années à venir, articulées autour de plusieurs principes structurants : formation, moralisation, coproduction et viabilité économique.

## La formation et la qualification comme leviers de la professionnalisation

Cet enjeu a été récemment abordé dans le cadre du rapport des Inspections générales de l'administration (IGA), de l'Éducation nationale (IGEN) et des Affaires sanitaires et sociales (IGASS) sur la formation aux métiers de la sécurité privée, rédigé par Gilles Sanson, Brigitte Le Brethon et Catherine Hesse en juillet 2012. Ce document souligne que les « *métiers de la sécurité privée sont pour l'essentiel des métiers de main-d'œuvre tenus par des personnels encore souvent formés trop hâtivement, de bas niveau de qualification et aux faibles perspectives de carrières* » [Sanson *et al.*, 2012, p. 3]. Plutôt consacré au secteur de la surveillance humaine, il relève plusieurs faiblesses du dispositif actuel de formation : un nombre de bénéficiaires trop restreint, une offre de formation incomplète et pas assez structurée, des contenus et une durée des formations faisant débat, une formation continue pas assez développée et faisant l'objet d'efforts décroissants de la part du secteur, un contrôle insuffisant de la qualité des formations dispensées et une fiabilité des examens régulièrement suspectée, une ambition bridée en matière de formation. Il propose une amélioration du pilotage du dispositif de formation, l'adaptation de sa gestion opérationnelle et la promotion de politiques de fond.

C'est finalement une image très mitigée qui se dégage de la mobilisation des entreprises de sécurité privée pour améliorer la formation professionnelle de leurs agents. Certes, les organismes paritaires ont participé à la définition de référentiels de formation, sont propriétaires des certificats de qualification professionnelle (CQP),

gèrent les examens ainsi que la délivrance des diplômes et assurent également le contrôle des organismes de formation qui les délivrent. Des formations professionnelles et des diplômes ont progressivement émergé, notamment au sein de l'Éducation nationale, permettant une reconnaissance des nouveaux besoins en matière de sûreté qui émergent au sein de la société. Ainsi, des certificats d'aptitude professionnelle (CAP) « agent de sécurité », des mentions complémentaires (MC) « sûreté des espaces ouverts au public », des BAC professionnels « métiers de la sécurité » ont progressivement été proposés à des jeunes à la recherche de formations débouchant sur des métiers. Les GRETA assurent des modules de formation pour les futurs agents. D'autres initiatives ont également vu le jour dans le domaine de la formation du « middle management » et de la formation des cadres et directeurs de sûreté. De même, l'INHESJ a mis en place un cycle spécifique de formation destiné à former les encadrants intermédiaires des sociétés. Ce cycle « middle management en sécurité privée » se fixe pour objectifs « *d'apporter des compétences complémentaires dans les domaines technique, juridique et sociologique aux cadres intermédiaires de la sécurité privée, à l'aide d'outils adaptés, afin de mieux répondre aux exigences de rigueur et de professionnalisme du secteur* ». De même, l'Université de Paris Descartes propose une licence professionnelle « sécurité des biens et des personnes ». Plusieurs Master 2, spécialisés sur les problématiques de sécurité intérieure, tels que ceux de Toulouse ou de Nice, permettent d'ouvrir la voie à une professionnalisation de l'encadrement intermédiaire et à des cadres susceptibles d'intervenir dans le secteur privé de la sécurité.

Néanmoins, en dépit de ces initiatives souvent locales, les acteurs du secteur privé et les pouvoirs publics ne se sont toujours pas accordés sur un modèle cohérent et global d'organisation de la formation professionnelle couvrant l'ensemble des besoins et répondant à des critères de qualité. C'est donc également une insuffisante mobilisation de l'État qui transparait, celui-ci n'ayant pas, jusqu'à aujourd'hui, été en mesure de proposer un cadrage législatif et réglementaire satisfaisant. Lors de son intervention du 8 décembre 2014, le ministre de l'Intérieur s'est montré désireux d'avancer sur l'organisation et la régulation du secteur de la formation professionnelle. Pour le Ministre, « *la priorité absolue du secteur privé, condition essentielle de la professionnalisation, est tout d'abord la formation* ». Il s'est prononcé pour l'intégration de la formation au

sein du Livre VI du Code de la sécurité intérieure (CSI), avec l'ambition de garantir une formation de qualité aux agents de sécurité privée et de maintenir leurs compétences. Par ailleurs, le Ministre entend renforcer la formation continue des agents de sécurité, en application du Code du travail. L'adaptation des salariés aux évolutions des postes qu'ils occupent implique la mise en œuvre de dispositifs de formation professionnelle qui prennent en considération les transformations des demandes exprimées par les donneurs d'ordre. Pour le Ministre, un décret devrait ainsi préciser cette obligation qui « *prend la forme d'un maintien des compétences, dispensé par un organisme agréé, et sous forme de stage. Le renouvellement de la carte professionnelle d'un agent serait subordonné au suivi d'un tel stage. Cette avancée réglementaire permettra de s'assurer d'une adaptation constante des professionnels de la sécurité aux évolutions de leurs missions, en termes de connaissance du cadre juridique, de savoir-faire techniques, mais aussi de savoir être* ».

## C'EST FINALEMENT UNE IMAGE TRÈS MITIGÉE QUI SE DÉGAGE DE LA MOBILISATION DES ENTREPRISES DE SÉCURITÉ PRIVÉE POUR AMÉLIORER LA FORMATION PROFESSIONNELLE DE LEURS AGENTS.

Parallèlement, le Conseil national des activités privées de sécurité (CNAPS) a aujourd'hui établi en son sein une commission « formation », présidée par Michel Mathieu, président de Securitas France. Plusieurs points d'accord ressortent du premier document de travail produit par cette commission :

1. La formation est « *un réel sujet de préoccupation* », mais son organisation ne satisfait ni les professionnels ni les pouvoirs publics, tant en termes de fonctionnement, de qualité, d'efficacité, que d'éthique ;
2. Seuls les pouvoirs publics (en l'occurrence par l'intermédiaire du CNAPS) apparaissent en position d'assurer un rôle de police administrative visant à la régulation de ce secteur ;
3. Néanmoins, les métiers (surveillance humaine, sûreté aéroportuaire, transport de valeurs, etc.) entendent jouer un rôle de contrôle, par exemple via leur représentation au sein du CNAPS.

Dans le domaine de la formation, une co-régulation public-privé semble ainsi se dessiner.

Parmi les points qui pourraient faire l'objet de propositions, il est possible d'exposer les axes de travail suivants visant à améliorer tant le contenu des formations

que les modalités de leur organisation qui demeurent aujourd'hui perfectibles :

- le développement des compétences des agents de sécurité privée pourrait se fonder sur un référentiel de formation (niveaux, contenus, durée, etc.) partagé par le secteur et les autorités publiques (ministères de l'Intérieur, de l'Éducation et de la Formation professionnelle). Il pourrait intégrer des modules de base, mais aussi des modules complémentaires susceptibles de répondre à des besoins très spécifiques de certains donneurs d'ordre. En effet, comme le souligne le dernier *Livre blanc* de la Confédération européenne des services de sécurité, les futurs agents de sécurité devront être plus compétents et dans des domaines requérant plus d'aptitudes, notamment en informatique, compte tenu de l'évolution rapide des innovations technologiques, mais également sur le plan juridique ;
- l'obligation de la formation continue serait rendue obligatoire pour le maintien de la carte professionnelle sur l'exemple d'autres professions réglementées (cf. certificat d'aptitude à la conduite de véhicules). Cette obligation de formation doit être précisément définie, tant sur le plan de son contenu que de sa durée et son organisation. Le suivi des obligations de formation pourrait faire l'objet d'un traitement automatisé sous l'autorité du CNAPS ;
- la mise en place d'un réseau national d'organismes de formation agréés aux métiers de la sécurité privée maillant le territoire national. À défaut de l'installation d'une école nationale pour les métiers de la sécurité privée, un système coordonné et harmonisé de formation doit être structuré. Il pourrait être administré et financé de manière paritaire (le CNAPS ou un autre organisme dédié), sans pour autant avoir la responsabilité de l'organisation des examens, ni de la délivrance des diplômes ;
- l'administration de l'organisation des examens et la délivrance des diplômes par l'Éducation nationale et/ou le ministère du Travail et de la Formation professionnelle ;
- le développement des formations pour les cadres amenés à exercer des fonctions de direction et de « middle management » et assurer une certaine perméabilité avec les différentes formations des cadres de la sécurité intérieure (police nationale, gendarmerie nationale, polices municipales).

## La moralisation comme condition de développement du secteur

Depuis la loi de 1983, de très nombreux efforts ont été réalisés en matière de moralisation du secteur, tant au niveau des dirigeants des sociétés de sécurité privée que des personnels qui les emploient. Des instruments de régulation ont également participé à cette moralisation : charte des achats, charte des contrôles CNAPS, accords visant à lutter contre le travail illégal, etc. Une convention régionale de lutte contre le travail illégal dans le secteur de la sécurité privée en Ile-de-France a, par exemple, été récemment signée, le 21 septembre 2015, entre l'État et les organisations représentatives du secteur de la sécurité privée.

Néanmoins, il apparaît que ce travail de moralisation nécessite encore d'être renforcé sur un certain nombre de points. Plusieurs enjeux s'imposent aujourd'hui pour permettre de progresser en matière de moralisation du marché et des professionnels, qui ont été mis en exergue par le ministre de l'Intérieur lors des Assises de la sécurité privée du 8 décembre 2014 :

1. La lutte contre le travail illégal qui demeure une problématique particulièrement prégnante et porteuse de distorsions de concurrence et de pratiques déloyales. Une meilleure coordination entre l'URSSAF<sup>2</sup>, les agents des services fiscaux, de la DGCCRF<sup>3</sup> et les agents du CNAPS, doit être recherchée pour une application pleine et entière de la réglementation ;
2. La généralisation de la signature de la Charte de bonnes pratiques d'achats de prestations de sécurité privée (déjà signée par plus de 290 organismes, tels que la Fédération française de football, le Stade de France ou le Service des achats de l'État) ;
3. Un meilleur filtrage du recrutement des personnels par une simplification des enquêtes administratives. Cela suppose de permettre aux agents des préfectures et du CNAPS d'interroger directement le fichier de Traitement des antécédents judiciaires (TAJ) avec l'accord du ministère de la Justice. Comme nous le verrons ultérieurement, des avancées récentes ont pu être enregistrées sur ce point.

La Mission d'information sur la lutte contre l'insécurité sur tout le territoire de l'Assemblée nationale, dite « mission Blazy », organisée en 2014, s'était en outre

(2) URSSAF : Union de recouvrement des cotisations de sécurité sociale et d'allocations familiales.

(3) DGCCRF: Direction générale de la concurrence, de la consommation et de la répression des fraudes.

déclarée favorable à l'instauration d'une garantie financière pour les entreprises de sécurité privée. Comme le notait le rapporteur, « *la mise en place de cette obligation de garantie financière pourrait permettre le paiement de pénalités en cas de manquement professionnel, en même temps qu'elle rendrait plus difficile la disparition de ces entreprises, qui nuisent indiscutablement à la réputation du secteur tout entier* ». Celle-ci avait d'ailleurs également proposé de mettre en place un système de qualification des entreprises qui « *pourrait prendre la forme d'une certification de leur niveau de compétence, favoriserait cette bonne information, de même qu'elle permettrait aux entreprises en question de se positionner sur certains types de prestations, le tout dans la perspective de la mise en place d'un marché plus transparent* ». La moralisation du secteur de la formation professionnelle est, elle-même, devenue un enjeu central du processus de professionnalisation. Certes, le CNAPS s'est vu reconnaître le droit de délivrer les autorisations d'accès à la formation professionnelle (118 744 autorisations d'entrée en formation délivrées lors du mandat 2012-2014). Il s'agissait de vérifier la moralité des prétendants à la formation, donc d'anticiper les éventuels refus ultérieurs de cartes professionnelles. Cependant, la moralisation des prestataires de formation se posait par elle-même. La finalité de ces différentes démarches est de procéder à un assainissement du secteur de la formation en sécurité. Comme le souligne le document de la commission formation du CNAPS : « *l'étude met brutalement en exergue un dysfonctionnement majeur. En dehors des CQP qui sont sous contrôle et délivrés par 360 organismes de formation, il existe au moins 400 autres organismes qui délivrent des "titres", tout à fait officiels, déposés au RNCP<sup>4</sup>, mais qui sont sans aucun contrôle réel. C'est dans cet environnement que nous rencontrons le pire de ce que l'on peut imaginer. Un titre délivré sans aucune formation, moyennant rémunération et/ou sur les deniers publics, suffit à la délivrance de la carte professionnelle en toute impunité. Cela constitue un réel point de faiblesse sur lequel il convient d'agir. En effet, si le CNAPS et la profession veulent une action utile, efficace et rapide, elle doit se concentrer dans ce domaine* ». Le ministre de l'Intérieur partageait le même constat lors des 3<sup>e</sup> Assises nationales de la sécurité privée, en notant que « *les organismes peu scrupuleux sont parfois constitués aux seules fins de mettre en place un système de fraude aux diplômes. Par leurs actions malhonnêtes, ils viennent ternir cette activité, alors même que la qualité des agents – et donc le service rendu aux clients – dépend de la qualité de la formation initiale des personnels* ». Dans sa proposition n° 41, la commission parlementaire Blazy envisage ainsi de « *subordonner l'activité de formation dispensée aux agents de sécurité privée à l'agrément préalable du prestataire et (de) créer une obligation de certification des organismes de formation* ».

Ces débats démontrent que l'ambition de moraliser le secteur doit prendre en considération de multiples aspects particulièrement complexes qui ne pourront être surmontés qu'au terme d'un travail de fond et de longue haleine. Quelques préconisations peuvent être avancées pour travailler dans cette voie :

- la moralisation des entreprises pourrait être améliorée par la mise en place d'une garantie financière sur une base à définir, comme le propose la commission parlementaire Blazy. Son montant doit cependant être apprécié au regard de différentes circonstances et conditions pour éviter tout barrage prohibitif à l'entrée sur le marché et aboutissant à une concentration de ce dernier ;
- la moralisation de nouveaux champs d'activités, tels que l'audit et le conseil en sûreté et leur inscription éventuelle au livre VI du CSI. Pour certaines activités particulièrement sensibles (exemple : protection des expatriés, assistance internationale, veille sécuritaire, etc.), des habilitations particulières pourront être exigées en lien avec les ministères concernés (ministère de la Défense, ministère des Affaires étrangères, ministère de l'Écologie, du Travail, de la Santé, etc.) ;
- la moralisation de la formation professionnelle : les centres de formation, publics ou privés devraient faire l'objet d'une délivrance d'agrément du CNAPS à la fois pour les organismes de formation, leurs dirigeants et les formateurs qui interviennent en leur sein. C'est sur la base de ces agréments et du programme de formation proposé que ces organismes pourront prétendre adhérer au réseau national de formation précité. En matière d'organisation des examens, les jurys devront être totalement indépendants des centres de formation et placés sous l'autorité du CNAPS (cf. modalités similaires à l'arrêté du 2 mai 2005 relatif aux qualifications des personnels des services de sécurité incendie et d'assistance à personnes). La loi du 17 août 2015 relative au dialogue social et à l'emploi, dite « loi Rebsamen », vient cependant apporter un début de réponse à ces enjeux en prévoyant l'intégration des organismes de formation en sécurité privée dans le champ de compétences du CNAPS. Elle ajoute un titre II bis « Formation aux activités privées de sécurité » au livre VI du CSI. Les prestataires de formation devront désormais satisfaire à une série de conditions (déclaration d'activité auprès d'une direction régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi (DIRECCTE), moralité des dirigeants,

(4) RNCP : Répertoire national des certifications professionnelles.

L'AMBITION DE MORALISER LE SECTEUR DOIT PRENDRE EN CONSIDÉRATION DE MULTIPLES ASPECTS PARTICULIÈREMENT COMPLEXES QUI NE POURRONT ÊTRE SURMONTÉS QU'AU TERME D'UN TRAVAIL DE FOND ET DE LONGUE HALEINE.

certification) pour obtenir une autorisation d'exercice. Ces prestataires de formation professionnelle et leurs activités (formation, délivrance des diplômes) sont ainsi désormais soumis aux différents contrôles disciplinaires du CNAPS. Un régime de sanctions pénales est également prévu (nouveaux articles L625-6 L625-7 du Code de la sécurité intérieure). En outre, la loi rend obligatoire la formation continue avant tout renouvellement de la carte professionnelle. Le CNAPS indique cependant

sur son site internet que des décrets d'application seront « *nécessaires pour préciser les modalités de délivrance des autorisations aux organismes de formation et permettre au CNAPS de mettre en œuvre les dispositions de cette loi* », de même que pour préciser les modalités concrètes de la formation continue.

- la moralisation des agents de sécurité, en autorisant le CNAPS et les préfetures à accéder au Traitement d'antécédents judiciaires (TAJ), procédure à encadrer étroitement. Sur ce point, le décret n° 2015-648 du 10 juin 2015 relatif à l'accès au TAJ et au fichier des personnes recherchées (FPR) permet, depuis peu, aux agents du CNAPS et des préfetures, d'avoir un accès plus large aux informations. Si la consultation de ce fichier TAJ conduit à formuler un avis défavorable pour le demandeur (relatif à son statut de « mis en cause » dans une affaire judiciaire par exemple), toute décision définitive devra cependant se fonder sur un complément d'information auprès des services de police et de gendarmerie nationales et sur une demande de la vérification des suites judiciaires auprès des procureurs de la République compétents. Le même décret ajoute également à l'article 5 du décret n° 2010-569 du 28 mai 2010 relatif au FPR un nouvel alinéa, permettant désormais aux agents du CNAPS d'avoir accès à ce traitement. Au-delà de ces mesures, la moralisation des agents ne pourra, en outre, intervenir que sur la base d'une harmonisation et d'une sécurisation du titre professionnel (cf. du type carte professionnelle du ministère de l'Intérieur), dont la délivrance serait officiellement organisée en préfecture, après lecture et signature du Code de déontologie. Cette carte professionnelle devrait rester la propriété du CNAPS. Elle serait délivrée à titre temporaire et révoquée en

lien avec les impératifs de moralité et d'obligation de formation continue. Elle devrait comporter un numéro de matricule national propre à l'agent et être portée de manière visible à tout moment lors de la réalisation des missions pour permettre une identification immédiate de la qualité de l'intervenant en évitant la confusion avec les forces publiques. Une incrimination pénale pourrait être votée par le Parlement en cas d'utilisation abusive ou frauduleuse de ce document ;

- la moralisation des donneurs d'ordre peut également donner lieu à plusieurs mesures : d'une part, en fonction de la qualification de l'établissement (OIV, ERP, IGH, SEVESO etc.) et de son niveau de classification, des obligations minimales de dimensionnement et de définition fonctionnelles du dispositif de sûreté pourraient être exigées ; d'autre part, l'adhésion à la charte de bonnes pratiques en matière d'achats devrait être rendue obligatoire au-delà d'un certain montant de prestations. Les entreprises signataires pourraient enfin se prévaloir d'un label reconnaissant le respect des engagements de ladite charte.

## La clarification des modalités de coproduction public/privé

Les relations entre l'État et le secteur privé de la sécurité ont progressé au cours des trente dernières années, passant d'un modèle quasi uniquement régalien à un modèle de coproduction. Comme le souligne Claude Tarlet, président de l'Union des entreprises de sécurité privées (USP) : « *Nous ne sommes pas dans une logique de compétition avec la puissance publique, mais dans celle d'une coproduction de sécurité* ». C'est également la position retenue par le président du CDSE qui indique que « *le partenariat public-privé implique un consensus de toutes les parties prenantes. [...] L'exigence d'une relation public-privé en sécurité doit impérativement intégrer tous les acteurs constitutifs de la filière public-privé. C'est cela le secret de la réussite* » [Juillet, 2014]. Du côté de l'État, le Préfet Thierry Coudert, délégué aux coopérations de sécurité, indique également que « *la coproduction de sécurité ne veut pas dire la mise sous tutelle des uns par les autres* ». Aujourd'hui, les fondations d'une collaboration entre pouvoirs publics et acteurs privés semblent donc bien exister, permettant d'envisager d'entrer dans une nouvelle ère de coproduction dédiée, cette fois, aux aspects plus opérationnels.

Le rapport Blazy préconisait ainsi une meilleure coopération entre les forces de sécurité publique et les entreprises de sécurité privée, et une augmentation des échanges d'informations dans le but de renforcer la protection des personnes et des biens dont ces dernières

ont la charge. Pour cela, il proposait que « *les forces de sécurité publique soient informées des contrats de prestation faisant intervenir des entreprises de sécurité privée, dès lors qu'une durée déterminée ou qu'un seuil de personnes engagées dans le cadre de ces contrats serait atteint, afin que les premières soient, d'une part, averties de la présence des secondes sur la voie publique, et, d'autre part, que les interactions entre les deux parties soient facilitées* ».

Il n'existe, en effet, aujourd'hui, aucune disposition préconisant ou obligeant les donneurs d'ordre ou les prestataires à informer les services de l'État de la nature et du volume des moyens privés implantés sur des sites gardiennés. Cela apparaît comme une faiblesse au niveau des capacités de coordination opérationnelle entre autorités publiques et privées, de même qu'en termes d'optimisation des moyens déployés. Les risques d'une absence de coordination sont également multiples : défauts d'identification par les citoyens et les agents de la force publique, manque de cohérence dans les modalités d'intervention, etc. Ces risques s'accroissent aujourd'hui au regard du développement toujours plus important des activités de sécurité confiées aux entreprises privées. Au plan local, ces défauts de coordination entre services de sécurité, au sens large, sont encore aggravés par le développement important des forces de police municipale sous l'autorité des maires.

Dans son allocution du 8 décembre 2014, le ministre de l'Intérieur a proposé plusieurs instruments pour répondre à ces enjeux. Il s'agit, d'une part, de la signature d'une circulaire sur la levée de doute pour les télésurveilleurs qui a été effectivement adoptée le 26 mars 2015, afin de limiter la mobilisation injustifiée des forces de police et de gendarmerie sur des crimes ou délits flagrants concernant la protection des biens et, d'autre part, de la nécessité pour les acteurs privés de la sécurité de signaler tous les faits de violence de nature délictuelle (et pas seulement criminelle) dont ils ont connaissance. Le Ministre entend ainsi systématiser le signalement aux forces de l'ordre, lorsqu'est commis un délit de violences volontaires ou bien un délit commis avec la circonstance aggravante de violences. Ces deux projets visent à l'amélioration et à la systématisation des échanges d'information entre les acteurs publics et privés. Mais le Ministre entend alors aller plus loin dans le renforcement de leur coordination en proposant le principe d'une « convention nationale de coopérations de sécurité », associant les différents acteurs de la sécurité privée, les municipalités ainsi que les autorités publiques. Cette convention aurait ainsi pour vocation à servir de cadre à la mise en œuvre de « programmes de coopération de sécurité » établis en fonction des besoins locaux sur l'ensemble du territoire. Ces programmes devraient être soutenus par les préfets pour faciliter l'implantation et l'adaptation locale de ces nouveaux instruments de coordination opérationnelle.

Cette volonté de renforcer l'échange d'informations et la coopération entre autorités publiques et entreprises privées peut également être identifiée en matière d'évaluation de « risque pays » et de sûreté à l'international, comme le démontre la création du Centre interentreprises de l'expatriation (CINDEX).

Les différents projets visant à renforcer l'échange d'informations réciproques entre forces publiques et privées ainsi que la volonté d'une plus grande coordination opérationnelle démontrent une hybridation progressive des moyens mis au service de la nation. Cette dynamique est appréhendée de façon globale, le Préfet Thierry Coudert soulignant que « *la sécurité passe par une coproduction entre les acteurs régaliens – la gendarmerie et la police nationales –, les polices municipales et la sécurité privée* » (revue *Protection et sécurité magazine* de sept/oct 2014). Cette coordination opérationnelle pourrait d'ailleurs également comprendre l'intégration et la participation des différentes réserves citoyennes (réserve civile de la PN et de la GN, citoyens volontaires, dispositifs de participation citoyenne, etc.) que l'État cherche à développer. Certaines sociétés semblent d'ailleurs s'inscrire dans cette perspective. Securitas propose aujourd'hui à ses clients des « City Patrols » ; comme l'indique le site internet de la société : « *Notre personnel de sécurité qualifié patrouille pour assurer la protection d'un ou de plusieurs sites. Des rondes répétées – en complément ou remplacement d'une surveillance continue sur place – garantissent un maximum de sécurité. Effectuées à pied ou avec des véhicules distinctifs, la présence des Patrouilles Protectas dissuade ou limite les dommages de perte de propriété du mandataire. La Patrouille Protectas est en liaison permanente avec la centrale d'appels d'urgence et de services Protectas* ».

L'instrument de cadrage et de contractualisation de ces coopérations opérationnelles pourrait être constitué par une « convention de coordination tripartite » établie entre les forces publiques nationales, publiques locales et privées de sécurité. Les conventions de coordination devenues obligatoires entre les forces d'État et les polices municipales (sur la base des prescriptions de l'article L512-4 du CSI) et expérimentées depuis plusieurs années, pourraient servir de base à la mise en œuvre de ces coopérations opérationnelles étendues. Le rapport de la mission Blazy évoque d'ailleurs que : « *afin de créer les conditions d'une meilleure coopération entre les forces régaliennes et les entreprises de sécurité privée, il pourrait utilement être recouru à la signature de conventions de coopération – auxquelles seraient parties l'entreprise de sécurité privée, le préfet et le maire – dont l'objet serait de renforcer la sécurité dans les emprises privées et sur la voie publique à proximité immédiate. Ces conventions préciseraient notamment la nature et les lieux d'exécution des missions des agents privés de sécurité et détermineraient les modalités selon lesquelles ces mêmes agents pourraient être conduits à échanger des informations, à*

*signaler des infractions ou à solliciter l'intervention de la police et de la gendarmerie nationales* ». Le rapport Blazy introduit donc une variable nouvelle : la possibilité pour des agents privés d'intervenir sur la voie publique « à proximité immédiate » des emprises privées dont ils ont la garde. Aujourd'hui, l'article L613-1 du CSI prévoit que les gardiens affectés à la surveillance d'emprises privées ne peuvent exercer leurs fonctions qu'à l'intérieur des bâtiments ou dans la limite des lieux dont ils ont la garde. L'exercice de leurs missions sur la voie publique leur est donc interdit, même si, « à titre exceptionnel », ils peuvent être autorisés par le préfet « à exercer sur la voie publique des missions, même itinérantes, de surveillance contre les vols, dégradations et effractions visant les biens dont ils ont la garde ».

Si la proposition du rapport Blazy ne vise pas à généraliser la compétence des agents privés sur la voie publique, cette dernière tendance est cependant apparue et s'est développée dans certains pays étrangers, comme dans les pays anglo-saxons, où les Business Improvement Districts (BID) – structures à but non lucratif qui cherchent à assurer la promotion de quartiers d'affaires ou de zones commerciales en complément des municipalités – recrutent leurs propres agents de sécurité qui assurent des patrouilles sur la voie publique selon une logique de coproduction de sécurité locale. En France, ce type d'approche n'est pas entré dans notre droit, mis à part les autorisations exceptionnelles qui peuvent être délivrées par les préfets et qui font l'objet d'une attention étroite des pouvoirs publics. Cependant, des évolutions apparaissent possibles en la matière, surtout si l'on considère les transformations récentes du cadre légal appliqué à la vidéoprotection sur la voie publique. En effet, la loi n° 2014-626 du 18 juin 2014, relative à l'artisanat, au commerce et aux très petites entreprises, permet d'assurer un visionnage des abords immédiats de ces établissements. Le décret organisant la mise en place plus concrète de ce dispositif a été adopté le 29 avril 2015 (décret n°2015-489), révélant la volonté des pouvoirs publics d'aménager la réglementation afin d'offrir un cadre légal à une extension maîtrisée de l'activité de sécurité privée.

Ces éléments démontrent que la place reconnue aux acteurs privés évolue en France pour se rapprocher des modèles étrangers qui autorisent l'émergence de partenariats opérationnels public-privé plus ambitieux (exemple : dans le Lincolnshire, en février 2012, un certain nombre de services – gardes de personnes arrêtées, enquêtes de voisinages, salles de commande, etc. – a été confié à la société anglo-danoise G4S, mais également des patrouilles mixtes, la gestion de la relation avec le public, le soutien aux victimes, etc.). Ils initient de nouvelles modalités de coopération, donnant lieu à divers

systèmes hybrides, en réponse aux contraintes budgétaires et à la demande sociétale de réassurance. Ces partenariats opérationnels ont connu des succès divers et parfois controversés à l'étranger, devant surmonter de multiples difficultés, notamment en termes de politisation des enjeux liés à la privatisation du secteur de la sécurité. Par-delà ces freins et des questions idéologiques et politiques que soulève le choix des modèles policiers, la viabilité et la performance de ces dispositifs dépendent aussi en grande partie des méthodes de mises en œuvre. L'exemple de l'échec de l'expérimentation de la privatisation dans les West Midlands (via la mise en place du *Business Partnering for Police*) démontre d'ailleurs, qu'en dépit de l'intérêt suscité par la privatisation de certains secteurs policiers, les pouvoirs publics ont été conduits à abandonner leur initiative et à revenir à des modes traditionnels de gouvernance de la sécurité [De Maillard, 2013].

Quelques propositions peuvent être avancées afin d'approfondir la tendance en cours à structurer des partenariats locaux de sécurité impliquant le secteur privé, sans pour autant abandonner les ressorts de la régulation étatique :

- la création d'une base de données nationale recensant, en temps réel, l'ensemble des dispositifs de sécurité privée mis en place par les donneurs d'ordre publics et privés, permettrait aux préfets et aux forces publiques de connaître l'ensemble des moyens privés de sécurité déployés dans une zone territoriale donnée. Cette base intégrerait les coordonnées des responsables « sûreté » des donneurs d'ordre, ainsi que des sociétés privées prestataires, de manière à ce que les pouvoirs publics puissent disposer d'une connaissance du potentiel mobilisable en cas d'incident, de crise ou de grands événements (exemple : Euro 2016, Vigipirate). Il incomberait aux donneurs d'ordre de tenir à jour ce traitement automatisé de données sur le mode déclaratif, ce qui leur permettrait de renforcer les liens de coopération opérationnelle avec la police et gendarmerie nationales, ainsi qu'avec les polices municipales ;
- l'élargissement des périmètres d'intervention des agents de sécurité privée, en leur permettant d'intervenir sur la voie publique aux « abords immédiats » des biens dont ils ont la garde. Cette disposition pourrait s'inspirer sur le plan législatif et réglementaire des initiatives récentes prises en matière de vidéoprotection ;
- l'établissement d'un droit à l'expérimentation d'initiatives de coproduction de sécurité sur le modèle des BID. Ces expérimentations pourraient être impulsées et évaluées par le Délégué aux coopérations de sécurité et mises en œuvre sous l'autorité des préfets. Ces expérimentations

devraient prendre en compte la gestion de types d'espaces diversifiés (exemple : zones commerciales, espaces de loisirs, établissements de santé, campus d'éducation, zones sportives, etc.) ;

- la clarification du positionnement des agents du Service de sécurité incendie et d'assistance aux personnes (SSIAP) en matière de sûreté dans un cadre de poly-activité. Ces éléments mériteraient de figurer au sein du livre VI du CSI, sans pour autant soumettre les métiers de la sécurité civile aux dispositions législatives et réglementaires de la sécurité privée. La circulaire NOR INTK1517236J du 12 août 2015 est en ce sens venue assouplir les règles d'emploi d'agents doublement qualifiés, sécurité incendie (SSIAP) et sécurité privée, dans les établissements recevant du public et les immeubles de grande hauteur.

## La viabilité économique du marché

La situation financière des entreprises de surveillance s'est beaucoup dégradée au cours des cinq dernières années. La baisse des prix entraîne la disparition de l'encadrement intermédiaire et la réduction des efforts de formation, avec pour effet une perte de compétences, puis consécutivement, une perte de revenu et de valeur ajoutée. Elle affecte tout à la fois la qualité de service et le modèle économique. Il n'existe aujourd'hui qu'un nombre très faible d'entreprises aux activités humaines de sécurité qui possèdent une situation saine et se développent sur des fondamentaux solides. Ce contexte d'hyper-concurrence et de concentration entraîne une course au volume au détriment, le plus souvent, du niveau de rentabilité. Il engendre une spirale à la baisse du secteur dont le taux de croissance se situe au plus bas (+1,8 % en 2013), en dessous de la moyenne des dix dernières années (+ 3,3%) et à un niveau deux fois moindre par rapport au score de la décennie précédente (+6,7 %), ce qui met en évidence une tendance à la décroissance.

Le marché des activités humaines de sécurité privée est un marché de demande, très réglementé et standardisé sur le plan social, sur lequel le client donneur d'ordres est le plus souvent en mesure d'imposer à son prestataire privé les conditions opérationnelles et commerciales de la prestation. Le vocable « donneurs d'ordre » est en lui-même, comme le rappelle Michel Matthieu (Securitas France) lors de son allocution aux 3<sup>e</sup> Assises de la sécurité privée, « porteur de tous les gènes tueurs de la valeur ajoutée ». Le prestataire de sécurité privée, réduit au simple rôle de « fournisseur de kilo de vigile », confronté à un contexte

d'austérité économique, doit faire face à des baisses de marge, à une dégradation des politiques sociales, à des risques de contentieux prud'homaux, à une baisse de qualité des prestations et consécutivement de satisfaction des clients. Les entreprises de sécurité privée se trouvent ainsi enlisées dans une spirale destructrice.

Parallèlement, la professionnalisation du secteur et son encadrement par des textes législatifs et réglementaires toujours plus nombreux, induisent des coûts associés au respect de ces prescriptions. Par exemple, l'amélioration de la condition sociale des agents peut entraîner une plus grande complexité de gestion humaine et des personnels, pouvant obérer des taux de marge déjà faibles. L'arrêté du 9 avril 2015, portant extension d'un accord conclu dans le cadre de la convention collective nationale des entreprises de prévention et de sécurité (JORF n° 0091 du 18 avril 2015), rend ainsi obligatoires, pour tous les employeurs et tous les salariés compris dans le champ d'application professionnel de la convention collective nationale des entreprises de prévention et de sécurité du 15 février 1985, les dispositions de l'accord du 15 juillet 2014, visant à favoriser l'équilibre vie privée/vie professionnelle des agents de sûreté. De même, le principe d'exclusivité applicable aux entreprises prestataires de sécurité privée depuis l'adoption de la loi du 12 juillet 1983 est perçu comme une contrainte structurelle privant les entreprises d'accéder à certaines économies d'échelle et de mutualisation de moyens. Dans son allocution du 8 décembre 2014, le ministre de l'Intérieur a annoncé un assouplissement des règles d'emploi d'agents doublement qualifiés « sécurité incendie (SSIAP) et sécurité privée » dans les établissements recevant du public (ERP) et les immeubles de grande hauteur (IGH). Il vient d'ailleurs de signer une circulaire (NOR INTK1517236J) du 12 août 2015, rappelant l'état du droit et définissant les modalités d'assouplissement de l'application de la réglementation. Cette recherche d'assouplissements pragmatiques trouve un autre exemple concret dans la publication du décret n°2015-1289 du 14 octobre 2015 portant création d'une carte professionnelle de surveillance dans le cadre de manifestations sportives, récréatives, culturelles et économiques rassemblant plus de 1 500 personnes. Cette mesure est destinée à aider la filière de la sécurité privée à faire face à la hausse temporaire d'activité liée à l'Euro 2016. Elle cherche à faciliter l'emploi de personnels pour réaliser le filtrage et le contrôle d'accès, la surveillance des bagages à main, la palpation de sécurité, la gestion des situations conflictuelles et l'alerte. En revanche, ces agents ne seront pas autorisés à exercer les activités classiques de gestion des alarmes, de réalisation de rondes de surveillance, de tenue d'un poste de sécurité ou la surveillance par des moyens électroniques.

Néanmoins, au regard de l'ensemble d'exigences et de contraintes qui affectent le secteur, le retour à la croissance ne viendra pas seulement de simples aménagements réglementaires, mais d'une réflexion plus globale. La croissance sur le marché des activités humaines de sécurité ne peut donc s'envisager que dans la perspective d'un nouveau modèle fondé sur :

- la revalorisation des métiers (exemple : révision des définitions de postes, des qualifications et des grilles salariales associées, amélioration du cadre social, etc.), permettant aux entreprises de sécurité privée de défendre une nouvelle politique de prix plus adaptée aux réalités de marché. Une campagne de communication en vue de valoriser le secteur et ses métiers pourrait être déployée à l'endroit du public et des donneurs d'ordre ;

- la rationalisation des moyens opérationnels (exemple : mutualisation de moyens inter-entreprises, formation continue, polyvalence des profils, poly-activité, etc.) ;

- l'offre de nouveaux produits et services (exemple : service « agent en une heure », proposé par Securitas France au regard de la demande de réactivité face à l'émergence d'un événement) ;

- l'innovation technologique. Les avancées technologiques (dans les domaines de la communication, de la dématérialisation des « workflows », des alarmes, de la surveillance vidéo, de la géolocalisation, etc.) permettent d'envisager un nouveau champ du possible sur le plan fonctionnel, en vue d'améliorer le niveau de sécurité des prestations et révéler de nouveaux champs d'activité (exemple : PC de sécurité mobile avec image embarquée en Finlande, lecture automatisée des plaques d'immatriculation des véhicules en stationnement et gestion de la redevance d'occupation de l'espace public en Grande-Bretagne, utilisation des drones et robots pour la surveillance des infrastructures et rondes mobiles, etc.) ;

- l'ouverture de nouveaux marchés : l'émergence de nouveaux besoins de sécurité, le plus souvent sur des environnements sensibles, tels que l'hôtellerie de luxe,

la bijouterie/joaillerie, la pharmacie, les événementiels, etc., constitue le terreau de nouvelles prestations. C'est le cas par exemple de l'expérimentation de coopération avec les forces de police nationale pour une chaîne de sécurité plus efficace autour de la place Vendôme, à Paris ;

- l'aménagement du cadre légal permettant de sécuriser juridiquement et de viabiliser les éventuelles nouvelles activités et pratiques du secteur (exemple : permettre l'escorte de transports sensibles et de véhicules exceptionnels sur la voie publique, etc.).

## Conclusion : une nouvelle coproduction à instituer ?

Aujourd'hui, les pouvoirs publics et les acteurs privés s'inscrivent donc dans une logique de coproduction.

Leurs volontés stratégiques semblent dorénavant converger après une période marquée par la méfiance mutuelle. L'avenir de la sécurité privée s'inscrit incontestablement dans cette dynamique de réciprocité avec l'État, mais ce secteur devra préalablement répondre à un certain nombre d'évolutions, condition de réussite d'un nouveau modèle à construire.

Pour cela, l'ensemble des acteurs concernés devra s'engager dans un véritable partenariat, résolument opérationnel : l'État, tête de ce réseau, vigilant dans son rôle de régulateur et de contrôleur ; le secteur de la sécurité privée, volontariste dans l'assainissement de son fonctionnement et l'accroissement de la qualité de ses prestations ; les donneurs d'ordre, comme acteurs clés de l'émergence d'un modèle économique viabilisé ; les collectivités locales, comme étroitement associées aux trois autres acteurs. Les échéances prochaines, tant en termes d'événementiel

(exemple : Euro 2016) que de mise en place de dispositifs nouveaux (exemple : lutte contre le terrorisme) seront l'occasion de la démonstration de cette dynamique nouvelle ■

IL N'EXISTE AUJOURD'HUI QU'UN NOMBRE TRÈS FAIBLE D'ENTREPRISES AUX ACTIVITÉS HUMAINES DE SÉCURITÉ QUI POSSÈDENT UNE SITUATION SAINNE ET SE DÉVELOPPENT SUR DES FONDAMENTAUX SOLIDES. CE CONTEXTE D'HYPER-CONCURRENCE ET DE CONCENTRATION ENTRAÎNE UNE COURSE AU VOLUME AU DÉTRIMENT, LE PLUS SOUVENT, DU NIVEAU DE RENTABILITÉ.

## Bibliographie

---

ANAPS, 2014, *Propositions de l'ANAPS pour la révision du livre VI du Code de sécurité intérieure*, Paris.

BLAZY (J.P.) (dir.), 2014, *Mission d'information sur la lutte contre l'insécurité sur tout le territoire*, Assemblée nationale, Paris.

BRAJEUX (P.), DELBECQUE (E.), MATHIEU (M.) (dir.), 2013, *Sécurité privée, enjeu public*, Armand Colin, Recherches.

CDSE, 2011, *Livre Blanc. La fonction sûreté dans l'entreprise*. Paris.

CNAPS, 2015, *Rapport de mandat 2012-2014*, Paris.

CNAPS, 2014, *Rapport d'activité*, Paris.

CoESS et INHES, 2008, *La participation de la sécurité privée à la sécurité générale en Europe*, Paris.

CoESS, 2015, *The new security company: integration of services and technology responding to changes in customer demand, demography and technology*, Bruxelles.

HASSID (O.), 2010, « Les dynamiques actuelles du marché de la sécurité en France », *Champ pénal/Penal field* [En ligne], Vol. VII, | mis en ligne le 23 janvier 2010, consulté le 18 juin 2014.

JUILLET (A.), 2014, *Entretien avec Alain Juillet par Michel Ferrero*, Les grands entretiens du SNES, [www.e-snes.org](http://www.e-snes.org), janvier.

LOUBET DEL BAYLE (J.-L.), 2012, « Une approche socio-politique de la sécurité privée », *Cahiers de la sécurité*, INHESJ, Paris, La documentation Française, n° 19.

MAILLARD (J.), 2013, « Les dynamiques récentes de la police et de la sécurité privée en Grande-Bretagne », *Sécurité et stratégie*, CDSE, juin-septembre.

MULONE (M.), DUPONT (B.), 2008, « Saisir la sécurité privée : quand l'État, l'industrie et la police négocient un nouveau cadre de régulation », *Criminologie*, 41, 1, 103-132.

OCQUETEAU (F.), 2004, *Polices entre État et marché*, Paris, Presses de Sciences Po.

Rapport des inspections générales de l'administration (IGA), de l'Éducation nationale (IGEN) et des Affaires sanitaires et sociales (IGASS) sur la formation aux métiers de la sécurité privée, rédigé par Gilles Sanson, Brigitte Le Brethon et Catherine Hesse, juillet 2012.

VINDEVOGEL (F.), 2004. « Les municipalités américaines favorisent-elles l'émergence de polices privées ? », *Déviance et Société*, 4, Vol. 28, p. 507-532.

WARFMAN (D.), OCQUETEAU (F.), 2011, *La sécurité privée en France*, Paris, Presses Universitaires de France, coll. Que sais-je ?



© JENS - Fotolia.com

# La souveraineté économique de la nation

## *Une question centrale*

Entretien avec Jean-Baptiste CARPENTIER<sup>1</sup>

“

*Quel bilan faites-vous aujourd'hui des politiques publiques d'intelligence économique menées en France depuis une dizaine d'années ? Quel a été le rôle de la Délégation interministérielle à l'intelligence économique (D2IE) ?*

Le premier constat que nous pouvons dresser est positif : la politique publique d'intelligence économique, relativement récente en France, commence à s'inscrire durablement dans le paysage institutionnel et industriel. Elle participe non seulement à l'élaboration des stratégies de développement

des grands groupes industriels, mais aussi à celle des entreprises de taille plus modeste. Et c'est cette dynamique que nous souhaitons soutenir.

Toutefois, les changements successifs de la structure chargée de la conduire ainsi que l'instabilité de l'ancrage institutionnel de celle-ci n'ont pas contribué à sa pérennité, ni à une définition claire de son contenu et de ses objectifs.

Il convient cependant de souligner le travail de réflexion et de définition des notions d'« intelligence et de sécurité économiques » conduit par la D2IE depuis sa création, en 2009, qui a constitué une étape essentielle

Jean-Baptiste CARPENTIER



Commissaire  
à l'information  
stratégique et  
à la sécurité  
économiques.

(1) Cet entretien a été réalisé par le Département « Intelligence et sécurité économiques » de l'INHESJ. Il figure sur la publication électronique du département, « Défis », n° 6, en ligne sur le site de l'Institut : <http://www.inhesj.fr/fr/qui-sommes-nous/les-publications/defis>

du dispositif. Après l'effort de conceptualisation, vient le temps de l'action, de la concrétisation des concepts. L'objectif est donc de conduire une stratégie à visée plus opérationnelle, plus proche de la préoccupation des entreprises.

*Le rattachement du « Service de l'information stratégique et de la sécurité économiques (SISSE) » auprès du ministère de l'Économie ne traduit-il pas de facto une réorientation de stratégie ? D'aucuns s'interrogent sur ce nouveau positionnement et la perte potentiellement induite du caractère interministériel. Le rattachement aux Services du Premier ministre n'offrirait-il pas, au moins symboliquement, le rang que se doit d'occuper une structure pilotant la politique publique d'intelligence économique par nature transversale ? N'en est-il pas de même concernant sa marge de manœuvre ? Ce changement ne pourrait-il pas être vécu comme un retour en arrière ? Peut-on y voir un raccrochement à l'héritage de la politique publique telle que définie par Alain Juillet lorsqu'il était haut responsable à l'intelligence économique (HRIE) ?*

Le constat que l'on peut tirer aujourd'hui des dernières années porte sur un excès de verticalité. Le choix en 2009 de créer une structure *ex nihilo* isolée, sans rattachement administratif, a finalement peut-être desservi l'action de la D2IE en contribuant à isoler la D2IE d'un point de vue opérationnel.

Pour autant, la création du nouveau Service de l'information stratégique et de la sécurité économiques, peut-elle être assimilée à un rapprochement avec la structure telle qu'elle existait au temps du HRIE ? Je ne crois pas. Les circonstances de 2015 n'étant pas celles de 2002, un modèle n'est pas transposable à un autre. Il s'agit d'adopter la logique du contexte actuel, tout comme Alain Juillet, à l'époque, qui a eu la sagesse d'installer sa fonction dans une structure déjà ancrée dans l'administration. Au-delà de ses qualités personnelles, je considère pour ma part qu'il est celui qui aura le plus marqué la discipline.

Concernant la perte potentiellement induite du caractère interministériel, cette crainte est, à mon sens, infondée. L'interministérialité ne se décrète pas ! Toutes les structures ministérielles ont vocation à porter les politiques interministérielles. En revanche, il est vrai que, en tant que composante inhérente à toute politique économique, il apparaît légitime que l'intelligence économique soit pilotée par Bercy. Cela n'exclut en rien la dimension interministérielle de l'action de la structure qui est chargée d'animer les politiques publiques ayant trait à

la protection du patrimoine matériel et immatériel français et de décider des orientations stratégiques en matière d'information stratégique et de sécurité économiques. Pour marquer cette dimension interministérielle, il est du reste proposé de conserver un comité directeur, tel qu'imaginé en 2009, composé de représentants des principaux ministres concernés par cette politique.

Mon ambition est de stabiliser la structure et pérenniser ses fondamentaux en se donnant les capacités de l'ancrer durablement, au-delà des personnes.

La réorientation de la stratégie vers une dimension plus opérationnelle est un choix assumé. Après un effort de conceptualisation nécessaire, il s'agit de donner la priorité à une doctrine d'application et d'emploi. Sa mise en œuvre s'appuie sur une équipe dédiée et restreinte. Le caractère léger de la structure de type état-major garantit une prise de décision plus directe, un emploi tactique plus souple et une action plus lisible et recentrée. L'objectif est clair :

la défense et la promotion des intérêts fondamentaux de la nation dans le domaine économique devraient guider les choix et les actions entreprises.

*On peut affirmer sans réserve que la souveraineté et l'expression de la puissance ne reposent pas seulement sur son armée et son industrie d'armement, mais également sur son tissu économique. Le risque de confusion avec une forme de nationalisme ou de patriotisme économique excessif ne doit pas conduire à minimiser cette nécessaire protection des intérêts essentiels de la nation.*

Sans écarter pour autant les autres problématiques générales, notamment celle liée à la préservation des emplois, la question de la souveraineté économique de la nation est, à mon sens, centrale. On peut affirmer sans réserve que la souveraineté et l'expression de la puissance ne reposent pas seulement sur son armée et son industrie d'armement, mais également sur son tissu économique. Le risque de confusion avec une forme de nationalisme ou de patriotisme économique excessif ne doit pas conduire à minimiser cette nécessaire protection des intérêts essentiels de la nation. L'extension du champ de l'espionnage à celui de l'économie, comme ont pu

le rappeler des affaires récentes, a montré que l'action économique n'était pas apatride ou dénationalisée. De façon plus générale, nous assistons, depuis la crise de 2009-2010 à un retour de la régulation et à une implication étatique plus grande dans le domaine économique notamment.

*L'abandon envisagé de la référence au terme « intelligence économique » dans le nom du futur service, traduit-il une restriction quant à votre périmètre d'action ? Quelles en sont les missions ? Est-ce à dire que les autres volets de l'intelligence économique que sont la veille et l'influence ne seront plus traités comme des priorités ?*

La veille et l'influence sont des savoir-faire essentiels dans notre champ de prérogatives, dans la mesure où elles sont conçues comme des outils, et non pas des finalités en soi, au service d'un objectif clair qui est la souveraineté et la sécurité économiques.

L'efficacité de ces modes opératoires tient à leurs champs d'application spécifiques. En effet, c'est moins l'influence de la France en général qui nous préoccupe que sa capacité à faire infléchir les décisions en matière de normalisation européenne, par exemple. De la même manière, le processus de veille stratégique repose sur l'identification et la centralisation des informations sur les pépites stratégiques qui constituent l'économie française. Nous distinguons donc deux volets dans la feuille de route du SISSE, l'un opérationnel, l'autre consistant en l'animation d'une politique interministérielle visant à défendre et promouvoir le patrimoine économique français. Dans ce sens, la nouvelle structure, comme les précédentes, jouera un rôle en matière d'investissements étrangers en France (IEF) en lien avec la direction générale du Trésor. Elle assurera également une coordination entre les différentes administrations de l'État en charge de la défense des intérêts économiques et de la sécurité des entreprises françaises. L'organisation de la structure en deux volets cherche à concilier l'enracinement dans une structure administrative telle que Bercy avec un pilotage interministériel.

Concernant l'absence de référence au terme « intelligence économique », ce choix part d'une volonté de sortir d'un débat, à mon sens stérile, autour de ce concept. Ce terme, intéressant du fait de sa transversalité, souffre des limites inhérentes à son caractère englobant.

Celui de « sécurité économique », même s'il peut paraître un peu réducteur, est davantage lisible, déjà inscrit dans le vocabulaire administratif et juridique français. Ainsi l'article 1142-3 du Code de la défense dit explicitement que le ministre chargé de l'économie « est responsable de la préparation et de l'exécution de la politique de sécurité économique », elle-même relevant de la politique de défense et de sécurité nationales.

*Dans ce cadre, comment concevez-vous le rôle qui sera le vôtre ? Serez-vous l'instigateur d'une nouvelle politique publique ? À quels besoins ou attentes répond ce changement ? Ce repositionnement*

*et votre passage en tant que directeur chez TRACFIN ne vous prédisposent-ils pas à renforcer le partage de l'information stratégique, et cela, à plusieurs niveaux ?*

- avec les entreprises (quels sont les moyens envisagés en dehors des actions pédagogiques et de sensibilisation menées auprès des entreprises ?);
- en formalisant ou officialisant un niveau de collaboration avec les services de l'État, notamment avec le Conseil national du renseignement (CNR) ?
- enfin en renforçant les liens avec l'ANSSI et nos entités de recherche et de formation ministérielles telles que l'INHESJ ?

Si les intérêts ne sont pas les mêmes, il y a des points de convergences entre ces différentes institutions et les entreprises. Concrètement, pour investir dans un pays à risque, les entreprises ont besoin d'avoir le soutien et l'éclairage de structures étatiques sur le contexte local. La décision relève pour autant du seul choix de l'investisseur. Il convient de respecter le champ des prérogatives de chacune des parties prenantes, mais de garder en perspective des intérêts convergents.

Concernant une éventuelle collaboration avec les services de l'État, notamment avec le CNR, il faut d'ores et déjà mettre un terme à certains fantasmes qui n'ont pas lieu d'être. L'intelligence économique n'est pas le renseignement. Chacun de ces organismes poursuit une logique d'action qui lui est propre, inscrite dans un cadre légal, et une finalité très particulière.

Le commissaire est chargé d'élaborer et de mettre en œuvre la politique publique en matière de protection et de promotion des intérêts économiques, industriels et scientifiques de la nation. Il est donc logique et impératif qu'il soit informé par le CNR des éventuelles atteintes à des intérêts de la nation. Dans la même perspective, les échanges avec les entreprises doivent être favorisés, en respectant les limites inhérentes à la confidentialité de certaines informations, en maintenant un dialogue et des zones de compréhension.

Pour autant, il n'est pas question d'opérer un mélange des genres et de transposer un dispositif américain qui a montré récemment ses limites. Mais il faut admettre que les Anglo-Saxons ont mieux compris la nécessité d'un dialogue constant entre la société civile, l'économie et le secteur public.

Le nouveau service participera aussi activement à la réflexion sur la défense de la souveraineté numérique.

La capacité des entreprises à répondre ou à influencer certaines normes est illustrative d'une recherche de convergence d'intérêts entre acteurs. Par ses arbitrages,

L'État doit rester garant de l'intérêt collectif. Le futur service continuera le travail entrepris par la D2IE en matière de définition des stratégies conduites en matière de normalisation.

Il ne faut pas non plus omettre le rôle des structures intermédiaires telles que les instituts que sont l'INHESJ ou l'Institut des hautes études de défense nationale (IHEDN) et les associations professionnelles que sont le Club des directeurs de sécurité des entreprises (CDSE) ou l'AGORA, à mon sens essentielles pour animer le débat, renforcer le dialogue et sensibiliser l'ensemble des acteurs privés comme publics aux enjeux de sécurité économique. La force de la structure tiendra aussi dans sa capacité à s'appuyer sur les compétences reconnues des autres administrations et sur celles émanant de la société civile. Cette intelligence existe déjà, il convient de la cristalliser pour en extraire la meilleure expertise et capacité d'action.

*Les événements de cette année ont montré que les sites industriels n'étaient pas à l'abri des actes de malveillance ni du terrorisme. L'État avait décidé le 30 juillet de renforcer la protection de 2 500 sites industriels. Quels enjeux identifiez-vous ? N'y aurait-il pas une nécessité à renforcer la diffusion de la culture de la sécurité/sûreté dans les industries ?*

Je constate qu'il reste une vraie marge de progression dans le domaine de l'informatique notamment. Il y a encore des failles majeures dans l'administration, mais aussi du côté des entreprises. Un effort de sensibilisation régulier sur les risques liés à la confidentialité, l'intrusion, ou encore à la destruction du patrimoine informationnel est tout à fait indispensable. Cela contribue progressivement à ancrer la sûreté de façon positive dans les esprits et cultures d'entreprises, afin qu'elle soit considérée, au-delà du coût qu'elle peut représenter, comme un réel atout en matière de compétitivité.

Le risque est indissociable de l'activité entrepreneuriale, mais ce risque est partagé par toute la chaîne économique contribuant à une activité donnée. Partant de ce constat, une structure capable d'offrir une chaîne « sûreté » fiable, certifiée et reconnue apporte un avantage compétitif absolument majeur.

La diversité des menaces et leurs conséquences parfois dramatiques obligent les organisations à adopter une approche globale de l'analyse des risques. En effet, au-delà de l'impact strictement financier, les conséquences engagent aussi la réputation de l'entreprise, la stabilité de son organisation, etc. La stabilité économique repose aussi sur un rapport de confiance entre l'entreprise et ses diverses parties prenantes. Elle est peut-être la meilleure garantie aux investissements pérennes.

Je suis convaincu qu'à terme un schéma reconnu de certification permettra de maintenir, voire de restaurer ce climat de confiance.

Une autre marge de progrès, qui me paraît essentielle pour la sécurité des entreprises, réside dans la reconnaissance et donc le positionnement de la fonction au sein de l'entreprise. Dans les grands groupes, le rattachement de la sûreté aux comités directeurs devrait être systématique. Les bases de réflexion du CDSE et des instituts tels que l'INHESJ méritent d'être relancées et mieux exploitées ■



# La mission intelligence économique de la gendarmerie nationale au prisme des entreprises

Catherine de LA ROBERTIE

Norbert LEBRUMENT

Stéphane MORTIER

## Catherine de La ROBERTIE



Rectrice, professeure des universités, PRISM, Paris 1- Panthéon Sorbonne, responsable du Master 2

S2IE - Stratégie internationale & Intelligence économique, et du pôle de recherche SEE - Stratégie & Économie d'entreprise, CREM - UMR CNRS 6211 ; colonel GN r.c., membre du conseil restreint du CSRM, de l'IHEDN et du CHEAR.

## Norbert LEBRUMENT



Maître de conférences, CRCGM - EA 3849, École universitaire de management,

université d'Auvergne, responsable du Master 2 Management de projet et Innovation, CREM - UMR CNRS 6211.

## Stéphane MORTIER



Doctorant, PRISM, Paris 1 - Panthéon Sorbonne.

## Introduction

**D**otée d'un maillage territorial couvrant environ 90 % du territoire métropolitain, la gendarmerie exerce une multitude de missions : police judiciaire, police administrative, renseignement, etc. Le gendarme est présent, connu, identifié. Il se pose ainsi en acteur majeur de la vie de la cité. Dans le cadre de ses missions, et s'inscrivant également dans une démarche territoriale, le gendarme a en charge la sécurité économique.

La gendarmerie nationale participe donc à la politique publique d'intelligence économique et à ce titre intègre le

réseau des acteurs de cette politique. L'organisation de la gendarmerie est pyramidale et intégrée. Les formations opérationnelles et administratives s'imbriquent les unes dans les autres : brigades de proximité, communautés de brigades ou brigades territoriales autonomes, compagnies, groupements départementaux, régions de gendarmerie. Cette organisation est régie par un principe visant non pas la spécialisation, mais la polyvalence des unités de base.

En matière de sécurité économique, conformément à la circulaire ministérielle du 1<sup>er</sup> juin 2010, la gendarmerie nationale, au travers de son réseau territorial, dispose d'une capacité importante de collecte d'informations sur la vie interne et l'environnement des entreprises dans sa zone de compétence. Ce maillage territorial permet d'évaluer les vulnérabilités des entreprises, de les sensibiliser et d'alerter les opérateurs afin de préserver le patrimoine économique et d'améliorer la résilience du tissu industriel

et commercial local. Les objectifs de développement économique territorial d'un bassin d'emploi donné, de mise en réseau des acteurs, des intervenants, tant privés que publics sont les facteurs déterminants de cette politique publique d'intelligence économique.

La proximité avec l'entreprise induite par cette mission d'intelligence économique place la gendarmerie nationale au cœur des territoires, au cœur de leur tissu économique. Après plusieurs années d'implication dans cette mission, quelle est la perception des entreprises quant à l'action de la gendarmerie en matière d'intelligence économique ? Dans une démarche purement qualitative, un échantillon d'entreprises sensibilisées par la gendarmerie amène quelques éclaircissements sur ce que leur a apporté cette mission spécifique de la gendarmerie nationale.

## Gendarmerie nationale et politique publique d'intelligence économique

### La politique publique d'intelligence économique

#### Au niveau national

La mondialisation et le déploiement rapide des technologies de l'information et de la communication ont bouleversé le monde en quelque vingt-cinq années. L'information est devenue, pour le monde de l'entreprise, une matière exploitable à des fins stratégiques, un enjeu de compétitivité. En France, la prise de conscience du rôle stratégique de l'information émerge à partir du rapport « Intelligence économique et stratégie des entreprises » du Commissariat général au plan [de La Robertie, Lebrument, 2008], plus connu sous le nom de « Rapport Martre », publié en février 1994.

Dix ans ont été nécessaires pour que les lignes du « rapport Martre » fassent l'objet d'une politique publique dédiée.

En effet, l'État français a mis en place, en décembre 2003, une politique publique d'intelligence économique, avec la nomination d'un haut responsable à l'intelligence économique, placé auprès du Premier ministre<sup>1</sup> et plus particulièrement du secrétaire général de la défense nationale. Daniel Canepa, alors secrétaire général du ministère de l'Intérieur et de l'Aménagement du territoire soulignait l'importance d'une telle politique : « *Économie fortement concurrentielle, stratégie d'influence, maîtrise de l'information, c'est assez logiquement que la conduite d'une ambitieuse politique publique d'intelligence économique constitue désormais un objectif majeur de l'État, tant dans ses missions régaliennes que dans son rôle de régulateur économique et social* » [Canepa, 2006]. Il faut pourtant attendre 2007 pour que l'intelligence économique entre dans les attributions des hauts fonctionnaires de défense et de sécurité<sup>2</sup> et consacre ainsi un véritable caractère interministériel à cette politique publique. Il sera mis fin à la fonction de haut responsable chargé de l'intelligence économique en mai 2009<sup>3</sup>. Cette politique s'est depuis lors ré-articulée autour d'un Délégué interministériel à l'intelligence économique, nommé par décret en 2009, et se décline, au niveau central, comme suit : une Délégation interministérielle à l'intelligence économique (D2IE) instituée par le décret n°2009-1122 du 17 septembre 2009 relatif au délégué interministériel à l'intelligence économique. Celle-ci exerce une mission générale d'animation et de coordination de l'action de l'État en matière d'intelligence économique. La D2IE pilote également des projets de fond et propose des mesures et des orientations selon un plan d'action arrêté par un comité directeur de l'intelligence économique présidé par le secrétaire général de la présidence de la République. Elle mène donc la politique publique d'intelligence économique. En 2013, la D2IE ne rend plus compte à l'Élysée, mais à nouveau au Premier ministre<sup>4</sup>.

L'année 2015 constitue un nouveau tournant dans cette politique publique. En effet, par décret du 1<sup>er</sup> juillet 2015, un nouveau délégué interministériel est nommé à compter du 3 août de la même année. Cependant, un nouveau décret devrait enterrer la D2IE et instituer un « commissaire à l'information stratégique et à la sécurité économiques » et porter sur la création du service à compétence nationale dénommé « service de l'information stratégique et de la sécurité économiques ». Ce commissaire élaborera

(1) Décret n° 2003-1230 du 22 décembre 2003 instituant un haut responsable chargé de l'intelligence économique, et décret PRMD0350011D du 31 décembre 2003 portant nomination du haut responsable chargé de l'intelligence économique.

(2) Décret n° 2007-207 du 19 février 2007 relatif aux attributions des hauts fonctionnaires de défense et de sécurité.

(3) Décret PR MD 0909733 D du 27 mai 2009 portant cessation de fonctions du haut responsable chargé de l'intelligence économique - Juillet (A.).

(4) Décret n° 2013-759 du 22 août 2013 relatif au délégué interministériel à l'intelligence économique.

et proposera, en lien avec le secrétariat général de la défense et de la sécurité nationale et les autres ministères concernés, la politique publique en matière de protection et de promotion des intérêts économiques, industriels et scientifiques de la Nation. Il sera placé auprès du ministre chargé de l'économie. Quant au « service de l'information stratégique et de la sécurité économiques », il sera rattaché au directeur général des Entreprises du ministère de l'Économie, dirigé par le commissaire susmentionné et sera à compétence nationale. Il faut noter l'abandon du vocable « intelligence économique » et mettre en parallèle ce nouveau service avec le rôle qu'occupent le coordinateur ministériel à l'intelligence économique et le service de coordination à l'intelligence économique mis en place en mars 2007 au sein de ce ministère<sup>5</sup>.

Concernant le ministère de l'Intérieur, ses responsabilités en matière d'intelligence économique reposent sur deux missions fondamentales : d'une part, l'animation du réseau territorial organisé autour du préfet de région et, d'autre part, la protection des entreprises et la contre-ingérence. La mise en place et la gestion de la politique publique d'intelligence économique territoriale sont sous la responsabilité du corps préfectoral, ce qui est rappelé dans la circulaire du 18 novembre 2013 relative à la feuille de route du ministère de l'Intérieur en matière d'intelligence économique. Quant à la gendarmerie nationale, elle est essentiellement positionnée sur le volet « sécurité économique » et contribue ainsi à chaque échelon hiérarchique à la mise en place de celle-ci. La direction générale de la Sécurité intérieure (DGSI), beaucoup plus attachée à ses missions de contre-ingérence est le troisième acteur majeur du ministère de l'Intérieur en matière d'intelligence économique.

### Au niveau territorial

Une déclinaison à l'échelon territorial a été opérée en 2005 au travers d'une circulaire destinée aux préfets de région<sup>6</sup>. L'État a ainsi défini une politique d'intelligence territoriale consistant à établir progressivement dans chaque région des schémas régionaux d'intelligence économique. La gendarmerie nationale y est largement évoquée : « *La gendarmerie nationale bénéficie également d'un maillage exceptionnel*

*du territoire qui fait d'elle une source de renseignements de premier ordre ainsi qu'un vecteur de sensibilisation qu'il conviendra d'impliquer pleinement dans votre politique locale d'intelligence économique* ».

La doctrine intelligence économique de la gendarmerie nationale (voir *infra*) a, d'ailleurs, été publiée la même année<sup>7</sup> et les premiers référents intelligence économique ont été formés dès novembre 2005 [Chardavoine, 2015]. Cette déclinaison territoriale de la politique publique d'intelligence économique institue un correspondant « intelligence économique » directement placé auprès du préfet de région. Ce dernier met en place un comité de pilotage (cf. Schéma 1.) qu'il anime et qui est composé entre autres des représentants de l'État, des collectivités territoriales, des chambres consulaires régionales, de chefs d'entreprise, d'universitaires et de responsables de laboratoires, ainsi que du représentant de la BPI France (Banque publique d'investissement), mais aussi les services de l'État en charge de la sécurité économique [gendarmerie nationale, direction générale de la Sécurité intérieure (DGSI<sup>8</sup>), direction de la Protection et de la Sécurité de la défense (DPSD<sup>9</sup>), Service central du renseignement territorial (SCRT<sup>10</sup>)].

Ce comité régional d'intelligence économique territoriale (CRIET) a pour mission de concevoir le schéma régional d'intelligence économique à mettre en place et comprenant trois volets : la définition d'un plan de sécurité économique visant à identifier et accompagner les entreprises sensibles, la création de portails d'intelligence économique et les actions de formation à destination des responsables de PME-PMI [Clerc, 2012]. La circulaire relative à la feuille de route du ministère de l'Intérieur en matière d'intelligence économique du 18 novembre 2013 rappelle que le préfet de région est l'échelon de référence de pilotage. Les préfetures de région maintiennent et renforcent les partenariats afin de promouvoir des projets de veille stratégique, des coopérations à l'export, des programmes de sensibilisation à la contre-ingérence au profit des acteurs économiques. Le préfet de région confie le pilotage opérationnel à un coordonnateur régional de l'intelligence économique territoriale qui s'appuie sur le CRIET pour mettre en œuvre cette politique territoriale. L'intelligence économique prend alors toute sa place au

(5) Circulaire ECO P 0700249 C du 21 mars 2007 relative au dispositif d'intelligence économique mis en œuvre au sein des services du ministère de l'Économie, des Finances et de l'Industrie.

(6) Circulaire INT A-05-00085-C du 13 septembre 2005 relative à l'intelligence économique appliquée aux territoires.

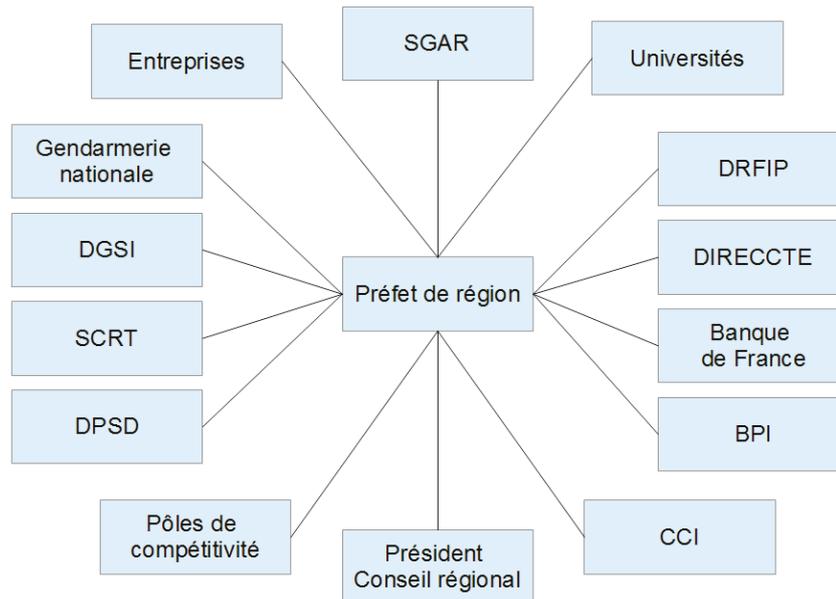
(7) Note d'orientation n° 1.060 DEF/GEND CAB du 8 mars 2005.

(8) Direction de la Surveillance du territoire (DST) de 1944 à 2008, direction centrale du Renseignement intérieur (DCRI) de 2008 à 2014 et direction générale de la Sécurité intérieure depuis le 12 mai 2014.

(9) Un des services de renseignement du ministère de la Défense (avec la direction du Renseignement militaire (DRM)).

(10) Suite à l'intégration d'une part importante des effectifs des Renseignements généraux (RG) à la DCRI en 2008, il a été créé une sous-direction de l'Information générale qui deviendra Service central du renseignement territorial en mai 2014.

Schéma 1 - Composition type d'un CRIET. Noyau du dispositif autour duquel d'autres institutions ou entités, publiques ou privées, entreprises, etc. peuvent venir s'agréger en fonction des spécificités régionales (SGAR : Secrétaire général pour les affaires régionales, DRFIP : direction régionale des Finances publiques, DIRECCTE : direction régionale des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi, BPI : Banque publique d'investissement, CCI : Chambre de commerce et d'industrie).



cœur des actions régionales de développement. Elle a pour ambition de susciter des dynamiques locales favorisant la création d'activités et d'emplois, de gérer stratégiquement la diversité – et donc la richesse – des différentes identités régionales, par la création de réseaux [Delbecq, 2006]. La finalité des CRIET est, par conséquent, la mise en relation, en réseau, des différents acteurs privés comme publics participant à la mise en œuvre de cette politique publique.

Depuis la circulaire du ministère de l'Intérieur du 24 avril 2012<sup>11</sup>, l'échelon départemental est lui aussi impliqué dans la mise en œuvre de cette politique. Il est demandé aux préfets de département de « désigner un correspondant départemental, membre du corps préfectoral, appelé à participer à l'élaboration de la stratégie régionale et à assurer la circulation de l'information et le traitement des dossiers ».

Le vocable « intelligence territoriale », qui n'est, en réalité, que l'application au territoire défini comme espace à trois dimensions – surface, population et tissu économique – de l'intelligence économique [Gilles, 2006], tend à devenir le

concept de référence de la politique publique d'intelligence économique et le rôle des collectivités locales dans le processus est primordial [Février et Raymond, 2010]. Il s'agit non seulement d'une quête de légitimité, mais également d'une prise de conscience forte de la nécessité d'une valorisation des territoires.

La puissance publique a ainsi pris conscience de l'importance de la démarche d'intelligence économique, ce qu'illustre sa déclinaison au niveau des échelons locaux dans le but d'y impliquer tous les acteurs. La circulaire du Premier ministre du 15 septembre 2011<sup>12</sup> joue un rôle prépondérant en ce domaine et définit l'intelligence économique comme consistant à « collecter, analyser, valoriser, diffuser et protéger l'information économique stratégique, afin de renforcer la compétitivité d'un État, d'une entreprise ou d'un établissement de recherche ».

Dans la pratique, les développeurs, les réseaux économiques, sociaux et culturels, les collectivités territoriales, l'État et les administrations, les entreprises sont invités à comprendre les dynamiques de leur

(11) Circulaire IOC K 12 07280 C du 24 avril 2012 relative à l'implication de l'échelon départemental dans la politique publique d'intelligence économique.

(12) Circulaire du Premier ministre n° 5554/SG du 15 septembre 2011, relative à l'action de l'État en matière d'intelligence économique.

environnement, à repérer, analyser les menaces, les risques, les occasions de développement pour piloter des stratégies de différenciation, de puissance et d'influence à des fins d'accroissement de la compétitivité. L'imbrication des sphères publiques et privées permet, et permettra, de conjuguer les connaissances, de faire émerger les potentiels d'innovation, et d'accompagner leur développement par des stratégies claires [Clerc, 2012]. Il s'agit de la mise en place à grande échelle d'une stratégie de réseau.

## La gendarmerie nationale, acteur de la sécurité économique

Dès 2004, la gendarmerie nationale s'est révélée précurseur. Dès le 7 janvier 2004, soit sept jours après la nomination d'Alain Juillet au poste de haut responsable chargé de l'intelligence économique, la direction générale de la Gendarmerie nationale (DGGN) a désigné un officier<sup>13</sup> pour proposer des modes d'action conformes à la doctrine et qui pourraient contribuer à cette politique [Chardavoine, 2015]. Le travail de cet officier débouche, un peu plus d'un an après, sur les premiers éléments de doctrine intelligence économique de la gendarmerie nationale<sup>14</sup>.

La circulaire du ministre de l'Intérieur, en date du 1<sup>er</sup> juin 2010<sup>15</sup> prévoit que la gendarmerie nationale, les services de la DGSI et du SCRT disposent de champs de compétences distincts et complémentaires en matière de veille stratégique et de sécurité économique, c'est-à-dire dans le volet défensif de l'intelligence économique. Protection et contre-ingérence sont du ressort de la DGSI, sécurité générale des personnes et des biens appliquée au monde de l'entreprise, de celui de la gendarmerie nationale et du SCRT. Le maillage de ces deux derniers services permet d'évaluer les vulnérabilités des entreprises, de les sensibiliser et d'alerter les différents opérateurs.

La circulaire Premier ministre du 15 septembre 2011<sup>16</sup> rappelle que l'action opérationnelle de l'État en matière d'intelligence économique s'organise autour de trois axes : assurer la veille stratégique, soutenir la compétitivité économique et garantir la sécurité économique.

Le 18 novembre 2013, la publication de la feuille de route pour l'action du ministère de l'Intérieur relative à l'« IE » va s'inscrire dans la consolidation de la politique publique en la matière. Il s'agira de renforcer le rôle du Ministère dans le dispositif interministériel et d'affermir la dimension locale de cette politique publique sur tous les territoires de la République. En liaison avec la DGSI, la SCRT, et la DPSD, la gendarmerie nationale concourt à la sécurité et à la protection du patrimoine économique<sup>17</sup>.

Au sein du ministère de l'Intérieur, trois services se partagent donc les missions de sécurité économique : la DGSI, la gendarmerie nationale et le SCRT qui sont complémentaires dans l'exercice de la politique publique d'intelligence économique au titre de leur ministère de rattachement. Les missions de la gendarmerie nationale, à l'instar de celles de la DGSI et d'autres acteurs, clairement définies par la circulaire du 1<sup>er</sup> juin 2010, et confirmées ensuite, s'articulent comme suit :

LA PUISSANCE PUBLIQUE  
A AINSI PRIS CONSCIENCE  
DE L'IMPORTANCE  
DE LA DÉMARCHE  
D'INTELLIGENCE  
ÉCONOMIQUE, CE  
QU'ILLUSTRE SA  
DÉCLINAISON AU  
NIVEAU DES ÉCHELONS  
LOCAUX DANS LE BUT  
D'Y IMPLIQUER TOUS LES  
ACTEURS.

Si le suivi des entreprises « sensibles » (secteurs stratégiques, pôles de compétitivité, entreprises d'importance régionale) a été réparti entre les grands services de l'État par les préfets de région (essentiellement DGSI et DPSD), la gendarmerie nationale et le SCRT apportent leurs capacités d'analyse des vulnérabilités à toutes les PME-PMI, le plus souvent partenaires de ces entreprises stratégiques, et donc à l'accompagnement desquelles la gendarmerie nationale collabore de façon indirecte.

L'activité de la gendarmerie nationale porte essentiellement sur la prévention (la surveillance générale, les relations

(13) Lettre n° 0070 DEF/GEND/CAB en date du 07 janvier 2014.

(14) Note d'orientation n° 1.060 DEF/GEND CAB du 8 mars 2005 puis ensuite N.E. n° 124.318 DEF/GEND/OE/SDDOP/CROG du 26 septembre 2006.

(15) Circulaire du ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales du 1<sup>er</sup> juin 2010, portant information sur le dispositif de la politique publique d'intelligence économique après la mise en place du délégué interministériel à l'intelligence économique.

(16) Circulaire du Premier ministre n° 5554/SG du 15 septembre 2011, relative à l'action de l'État en matière d'intelligence économique.

(17) Circulaire n° 109350 du 1<sup>er</sup> juin 2010, portant information sur le dispositif de la politique publique d'intelligence économique.

avec les décideurs économiques, les conférences de sensibilisation, les visites en entreprise), mais également sur le volet répressif si nécessaire (investigations judiciaires), dans le cadre de ses prérogatives judiciaires.

Pour répondre à l'enjeu majeur que constituent la protection de l'économie nationale et la préservation des emplois, la gendarmerie a mis au point une stratégie de maillage des territoires par l'implantation de référents intelligence économique, a créé des structures spécialisées, développé des modes d'action spécifiques et adapté la formation de ses personnels dès 2005 (première session de formation de référents intelligence économique). En terme d'organisation interne, chaque échelon de commandement territorial et central exerce un rôle précis : les brigades territoriales et les compagnies recensent les entreprises les plus sensibles, recueillent le renseignement d'intérêt économique et organisent des opérations de sensibilisation [...]. Les groupements et les régions exploitent les renseignements et effectuent des actions de prévention auprès des acteurs économiques. La direction générale de la Gendarmerie nationale élabore la doctrine, centralise le renseignement et participe aux différentes instances interministérielles du traitement de l'intelligence économique [Leonetti, 2012]. Pour mener à bien cette mission, des personnels sont formés à la discipline intelligence économique. Au sein de chaque région de gendarmerie se trouve un officier de gendarmerie « référent intelligence économique » formé au cours d'un cycle spécialisé à l'Institut national des hautes études de la sécurité et de la justice (INHESJ). Des sous-officiers « référents intelligence économique », répartis sur tout le territoire métropolitain et outre-mer ainsi que dans les formations spécialisées de la gendarmerie (maritime, de l'air, des transports aériens, de l'armement), sont formés en interne via une structure de formation spécialisée, le Centre national de formation au renseignement opérationnel (CNFRO), et généralement placés au sein de cellules renseignement de chaque département. Quant aux personnels en charge de l'intelligence économique à la DGGN, ils disposent tous, *a minima*, de diplômes de Master2 reconnus en la matière (cf. par exemple un sous-officier diplômé de l'École de guerre économique) [Leonetti, 2012]. Ces derniers appartiennent à la section Intelligence économique territoriale (SIET) de la sous-direction de l'Anticipation opérationnelle (SDAO) créée en novembre 2013<sup>18</sup>. Cette dernière a notamment dans ses attributions le traitement du renseignement

de sécurité économique en métropole et en outre-mer (art. 5 de l'arrêté du 6 décembre 2013). Au gré des mutations et réorientations en cours de carrière, ces différents personnels rejoignent de nouvelles affectations où ils peuvent mettre à profit l'expertise ainsi acquise en intelligence économique. Cette expertise, couplée à celle des personnels nouvellement formés, constitue un véritable réseau d'experts qui vient s'imbriquer dans le maillage territorial de la gendarmerie. À ce jour, plus de deux cents officiers et sous-officiers de gendarmerie ont été formés à l'intelligence économique.

## L'action de la gendarmerie en matière d'intelligence économique telle que perçue par les entreprises

La gendarmerie, au travers de ses référents intelligence économique, sensibilise environ huit à dix mille entreprises par an, dans tous les secteurs d'activité, partout sur le territoire soit lors de conférences de sensibilisation soit lors d'une visite en entreprise dédiée à un « diagnostic vulnérabilités<sup>19</sup> ». Comment sont perçues ces interventions de la gendarmerie dans l'entreprise, qu'apportent-elles de concret à l'entreprise ?

Sur l'année 2015, une centaine de chefs d'entreprises situées en Ile-de-France nous ont accordé un entretien, le seuil de saturation a été atteint après douze entretiens de type non directifs. Ces PME, toutes de moins de 500 salariés, sont globalement satisfaites de l'intervention et de l'action de sensibilisation d'un référent intelligence économique. Les responsables insistent sur le fait que cette visite leur a permis de prendre conscience de l'existence de vulnérabilités qui leur échappaient totalement. Essentiellement des vulnérabilités relevant des comportements individuels des employés et dirigeants de l'entreprise (comportements et indiscretions lors des déplacements, utilisation des réseaux sociaux, règles de sécurité trop faibles ou inexistantes, vulnérabilités des supports amovibles, et nomades tels que smartphones, tablettes, etc.). Il s'agit essentiellement d'atteintes dites « risques informatiques » ou « cyber-risques », et, « risques liés aux fragilités humaines » dans le référentiel utilisé par la gendarmerie nationale<sup>20</sup>. Cette prise de conscience

(18) Arrêté du 6 décembre 2013 modifiant l'arrêté du 12 août 2013 portant organisation de la direction générale de la Gendarmerie nationale.

(19) Essentiellement le diagnostic DIESE de la Délégation interministérielle à l'intelligence économique. Le Diagnostic d'intelligence économique et de sécurité des entreprises (DIESE) est un logiciel d'évaluation des vulnérabilités des entreprises. Il a été développé par un ensemble de partenaires publics et privés, dont la gendarmerie nationale. Une version spécifique a été développée pour les laboratoires de recherche. Voir <http://www.intelligence-economique.gouv.fr/methodes-et-outils/logiciels-dauto-evaluation>

a débouché sur la mise en place d'actions correctives et d'une sensibilisation des personnels.

Plusieurs de ces entreprises, ultérieurement victimes de tentatives d'escroquerie de type « faux ordre de virement international » ou « faux président », ont été en mesure de déjouer les arnaques grâce aux conseils prodigués par le référent intelligence économique lors de son intervention. Les « risques financiers » sont un sujet abordé de façon récurrente par les chefs de PME, que ces risques soient liés à de la criminalité (escroquerie, corruption, etc.) ou à des investissements (étrangers, concurrents, etc.). La possibilité pour les entreprises d'avoir un point d'entrée (le référent intelligence économique) identifié et connu à la gendarmerie constitue, pour elles, un atout majeur.

La question des risques liés à la radicalisation des employés dans l'entreprise soulève de nombreuses interrogations chez les chefs d'entreprise. Et plus généralement, les attentats de janvier 2015 (retranchement des terroristes dans des entreprises à Dammartin-en-Goële et à Vincennes), la décapitation d'un chef d'entreprise par un de ses employés à Saint-Quentin-Fallavier, « l'affaire du Thalys » (sécurité lors des déplacements professionnels), les attentats de Paris le 13 novembre 2015 (les salles de spectacle et restaurants sont des entreprises) ont induit un climat d'inquiétude chez certains chefs d'entreprise. La question du suivi des individus en voie de radicalisation et les procédures de signalement sont devenues pour certains chefs d'entreprise une préoccupation majeure. Ont également été évoquées les problématiques liées au phénomène des dérives sectaires de façon plus générale. Il est cependant courant que la perception des risques soit influencée par les titres de l'actualité<sup>21</sup>. À ce sujet, un

chef d'entreprise nous confie que le référent intelligence économique de la gendarmerie lui a proposé de prendre connaissance du guide *Gestion du fait religieux dans l'entreprise privée* publié par l'Observatoire de la laïcité. Il s'agit ici également de « risques liés aux fragilités humaines ».

POUR RÉPONDRE À L'ENJEU MAJEUR QUE CONSTITUENT LA PROTECTION DE L'ÉCONOMIE NATIONALE ET LA PRÉSERVATION DES EMPLOIS, LA GENDARMERIE A MIS AU POINT UNE STRATÉGIE DE MAILLAGE DES TERRITOIRES PAR L'IMPLANTATION DE RÉFÉRENTS INTELLIGENCE ÉCONOMIQUE, A CRÉÉ DES STRUCTURES SPÉCIALISÉES, DÉVELOPPÉ DES MODES D'ACTION SPÉCIFIQUES ET ADAPTÉ LA FORMATION DE SES PERSONNELS DÈS 2005

Les différents risques évoqués lors des entretiens viennent corroborer les chiffres dont dispose la section intelligence économique territoriale de la direction générale de la Gendarmerie nationale, soit une augmentation importante des « cyber-risques », « risques financiers » et « risques liés aux fragilités humaines » qui apparaissent élevés. Ces statistiques nationales ne sont toutefois pas rendues publiques au regard de leur caractère sensible.

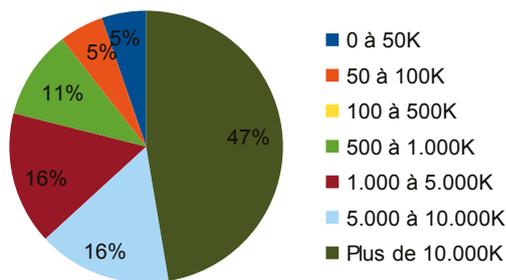
Dans un second temps, cette étude qualitative exploratoire a permis la réalisation d'un questionnaire, envoyé à chaque référent régional intelligence économique de la gendarmerie nationale. Il a été demandé à ces derniers de solliciter les entreprises de leur zone de compétence ayant fait l'objet d'une visite d'un référent intelligence économique de la gendarmerie. Seules dix-neuf entreprises de trois régions (Corse, Rhône-Alpes, Franche-Comté) ont accepté de répondre à ce questionnaire et de faire part de leur expérience avec la gendarmerie nationale en matière d'intelligence économique. Ce nombre très faible

de régions participantes s'explique par le caractère discret et sensible des informations recueillies par les référents dans les entreprises. En effet, la mission « intelligence économique » de la gendarmerie nationale s'articule autour du renseignement de sécurité économique et de nombreuses informations sont couvertes par les règles du « confidentiel défense ». Parmi les entreprises ayant répondu favorablement quant à leur participation à cette enquête, huit secteurs d'activité sont représentés :

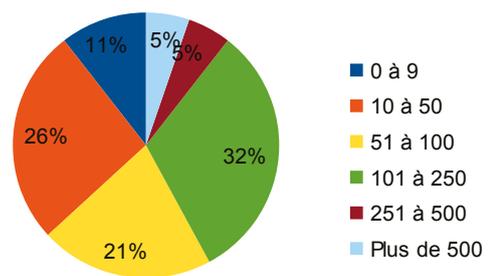
(20) Le référentiel des atteintes utilisé par la gendarmerie nationale comporte huit familles : atteintes au savoir-faire, risques financiers, risques informatiques, désorganisation et fragilisation, atteintes physique sur site, atteintes à la réputation, risques liés aux fragilités humaines et intrusions consenties.

(21) La perception des risques est influencée par l'actualité et les médias : sur la période 2014-2015, la montée de l'État islamique en Syrie et en Irak est considérée par les entreprises comme un risque majeur selon le *Global Risk Management Survey 2015* d'Aon Risk Solution.

Chiffres d'affaires des entreprises participantes



Nombre de salariés par entreprise



agroalimentaire, biens d'équipement, biens intermédiaires, biens de consommation, automobile, commerce, services aux entreprises et services aux particuliers. Le profil des entreprises participantes est le suivant :

Il s'agit donc de PME de moins de 500 salariés, à une exception près, mais aux chiffres d'affaires très variables. Cependant, près d'une entreprise sur deux réalise un chiffre d'affaires supérieur à dix millions d'Euros. Cela est représentatif du tissu des PME situées en zone de compétence gendarmerie où l'on retrouve essentiellement de petites entreprises, souvent sous-traitantes de premier, second, voir troisième rang des grands groupes français ou étrangers.

Les entreprises participantes, soit celles ayant répondu au questionnaire, évaluent l'action de la gendarmerie nationale comme suit :

- en termes de satisfaction générale, 42 % des entreprises sont tout à fait satisfaites de l'intervention du référent intelligence économique de la gendarmerie, 58 % en sont plutôt satisfaites ;
- quant aux qualités professionnelles des référents intelligence économique, elles sont pour 58 % des entreprises tout à fait satisfaisantes et pour les 42 % restantes plutôt satisfaisantes ;
- 73,5 % des entreprises soulignent que le climat de confiance qui s'est installé entre elles et le référent est tout à fait satisfaisant, 26,5 % le considérant comme plutôt satisfaisant ;
- la qualité du diagnostic est plutôt satisfaisante pour 74 % des entreprises, tout à fait satisfaisante pour les 26 % restants. À noter que les diagnostics utilisés ne sont pas systématiquement les mêmes (DIESE de la D2IE, diagnostic région de gendarmerie, etc.) ;

- quant à la question relative à la facilité d'identification des services à contacter par l'entreprise lors de la constatation d'une problématique liée à l'intelligence économique, seules 26 % des entreprises sont tout à fait satisfaites, 26 % plutôt satisfaites et 48 % pas vraiment satisfaites.

- globalement les interventions du référent intelligence économique de la gendarmerie dans l'entreprise sont satisfaisantes (à 86,3 % tout à fait ou plutôt satisfaisantes). Cependant, la difficulté pour l'entreprise d'identifier le bon interlocuteur constitue le point faible (52 % de satisfaction) ;

- 89,5 % des entreprises estiment avoir retiré une plus-value de l'intervention du référent intelligence économique de la gendarmerie ;

- cette intervention était nécessaire pour 42 % des entreprises et intéressante pour 58 % d'entre elles ;

- 95 % des entreprises visitées ont pris des mesures suite au diagnostic réalisé avec le référent intelligence économique. Ces mesures sont les suivantes :

- 3 entreprises ont décidé de prendre en compte la démarche d'intelligence économique dans leur organisation,
- 14 entreprises ont sensibilisé leur personnel à l'intelligence économique et à la sécurité économique,
- 5 entreprises ont mis en place un système de veille,
- 8 ont procédé à des adaptations du système de sécurité physique de leur emprise,
- 12 ont renforcé la sécurité des systèmes d'informations,

- 2 entreprises ont pris en compte les leviers d'influence dans leur stratégie,
  - 2 ont demandé l'intervention d'un référent sûreté de la gendarmerie, spécialisé en sécurité bâtimentaire et en vidéoprotection,
- quant à l'impact général sur l'image de la gendarmerie, l'intervention du référent intelligence économique a un effet positif sur la confiance qu'inspire la gendarmerie dans 84 % des cas ; il en est pratiquement de même quant à l'idée de son efficacité (79 %). La capacité de la gendarmerie à traiter les demandes formulées par les entreprises est considérée comme bonne par 68 % des entreprises. D'une façon générale, la mission d'intelligence économique conférée à la gendarmerie et l'action de ses référents a un impact positif sur l'image de l'institution.
- certaines entreprises ont formulé des attentes envers l'action de la gendarmerie en matière d'intelligence économique :
- apporter un regard extérieur permettant de contrecarrer les routines (diagnostic à intervalle régulier),
  - donner des conseils plus précis et plus techniques,
  - informer sur les solutions de protection innovantes,
  - une demande d'expertise en prévention des cybermenaces.

Globalement, l'action de la gendarmerie nationale en matière d'intelligence économique est appréciée des entreprises. Non seulement l'intervention des référents intelligence économique induit des actions et ajustements dans l'entreprise, mais aussi suscite des attentes nouvelles nées de la prise de conscience des vulnérabilités encourues par celles-ci. L'objectif est ainsi atteint et s'inscrit totalement dans la politique publique d'intelligence économique. De plus, en termes d'image, la gendarmerie nationale bénéficie de l'établissement d'une relation de confiance avec le monde de l'entreprise et met en avant des domaines d'expertise connexes à ses missions régaliennes. Il s'agit par conséquent d'une relation de type « gagnant-gagnant » entre les entreprises, la politique publique d'intelligence économique et la gendarmerie nationale.

## Conclusion

Pleinement inscrite dans la politique publique d'intelligence économique mise en place en 2004, la gendarmerie nationale a su tirer profit de son maillage territorial pour mettre en place un dispositif de sensibilisation du tissu économique à l'intelligence économique sur l'ensemble du territoire. Cette mission, pourtant quelque peu en retrait des missions originelles et régaliennes de l'institution, s'est totalement imbriquée dans ces dernières. Plusieurs dizaines de milliers d'entreprises ont ainsi été sensibilisées aux risques et vulnérabilités auxquels elles sont aujourd'hui confrontées. L'intelligence économique est une démarche que la gendarmerie apporte dans l'entreprise et qui permet à l'entreprise de se prémunir, se préserver de la prédation.

Dans le même temps, cette mission de la gendarmerie nationale lui permet une réappropriation du territoire par le tissu économique et de bénéficier ainsi d'une perception plus favorable et constructive, détachée du modèle répressif communément véhiculé dans l'esprit des populations. De la sorte, l'intelligence économique contribue largement à une image positive de la gendarmerie nationale.

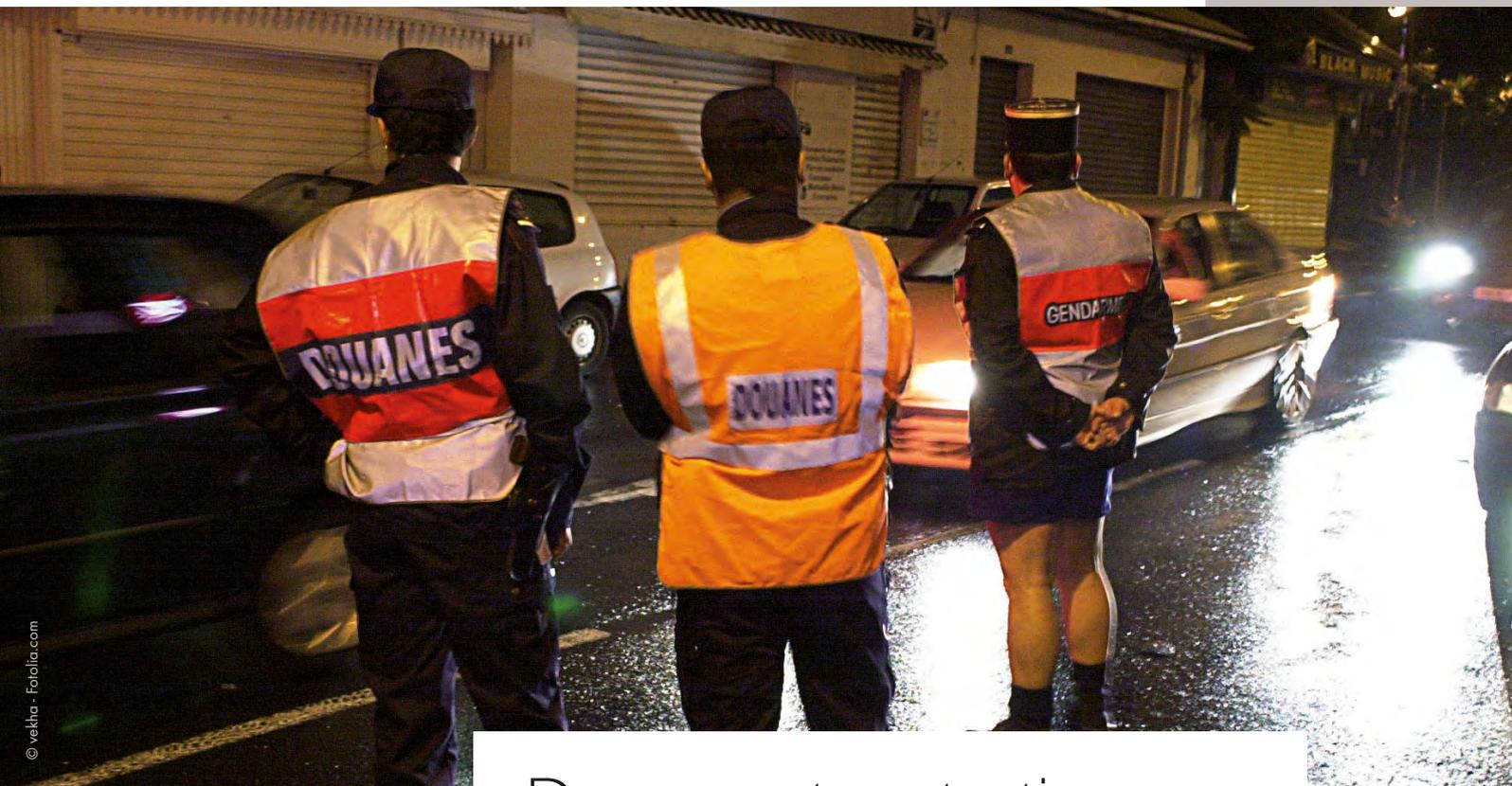
Tant pour les entreprises que pour la gendarmerie, la mission intelligence économique est utile et bien perçue. Les attentes nées au sein des entreprises du fait de l'intervention des référents intelligence économique de la gendarmerie nationale démontrent à quel point les nouvelles menaces sont une préoccupation majeure dans les PME, au premier titre desquelles les cybermenaces et les risques liés à la radicalisation des personnels de l'entreprise. En matière de « cyber-risques », la gendarmerie nationale, la DGSI et la police nationale, sous l'égide des services du ministère de l'Intérieur, ont mis en place un dispositif de sensibilisation à la cybersécurité, des référents intelligence économique, sûreté et prévention de la délinquance. La sécurité économique évolue au rythme de l'apparition de nouvelles menaces et les services en charge de cette sécurité, dont la gendarmerie nationale, adaptent constamment leurs dispositifs pour répondre au mieux non seulement à la politique publique d'intelligence économique, mais surtout aux attentes des entreprises.

Cette action particulière de la gendarmerie nationale, la mise en œuvre de sa mission d'intelligence économique, correspond bien à une attente et un besoin des PME-PMI, attente et besoin qui ne savent pas toujours s'exprimer, mais qui trouvent là à se manifester ■

## Bibliographie

---

- CANEPA (D.), 2006, « L'intelligence territoriale. Une nouvelle politique publique », *Revue de la gendarmerie nationale*, n° 218, mars 2006.
- CHARDAVOINE (O.), 2015, *La politique publique d'intelligence économique*, Paris, L'Harmattan.
- DE LA ROBERTIE (C.), LEBRUMENT (N.), 2008, « Quel paradigme stratégique pour l'intelligence économique ? », *Cahiers de la sécurité*, INHES, Paris, La documentation Française, n° 4, avril, p. 89-101.
- DE LA ROBERTIE (C.), LEBRUMENT (N.), 2009, « Capacités d'absorption et gestion de crise : les pratiques d'intelligence économique des PME », *Cahiers de la sécurité*, INHES, Paris, La documentation Française, N° 10, octobre-décembre, p. 253-261.
- DE LA ROBERTIE (C.), LEBRUMENT (N.), 2011, « Prolégomènes à une compréhension du concept de responsabilité en intelligence économique », in Cattoir-Jonville (V.), Saison (J.) (dir.), *Les différentes facettes du concept juridique de sécurité, mélanges en l'honneur de Pierre-André Lecocq*, Lille2, décembre, p. 363-376.
- DE LA ROBERTIE (C.), LEBRUMENT (N.), 2012, « Les pratiques d'intelligence économique des PME du pôle de compétitivité « Images et Réseaux » : une conceptualisation selon les principes de la théorisation enracinée » in Luckerhoff (J.), Guillemette (F.) (Ed.), *Méthodologie de la théorisation enracinée (grounded theory) : riche diversité*, Québec, Presses de l'Université du Québec, p. 163-190.
- DE LA ROBERTIE (C.), LEBRUMENT (N.), 2012, « L'influence explicative du capital social des dirigeants sur le développement des pratiques d'intelligence économique : le cas des PME du Grand Ouest », in Lecointre (G.) (dir.), *Le Grand Livre de l'économie PME 2012*, Paris, Éditions Gualino, p.245-271.
- DELBECQUE (E.), 2006, *L'intelligence économique*, Paris, Presses Universitaires de France.
- FÉVRIER (R.) ET RAYMOND (P.), 2010, *Intelligence économique et collectivités territoriales. Des stratégies innovantes pour une meilleure valorisation des territoires*, Paris, Ellipses.
- GILLES (R.), 2006, « L'intelligence économique territoriale et la gendarmerie », *Revue de la gendarmerie nationale*, n° 218, 51-58, mars 2006.
- LEBRUMENT (N.), 2012, *Intelligence économique et management stratégique - Le cas des pratiques d'intelligence économique des PME*, préface de Bournois (F.), Paris, L'Harmattan.
- LEBRUMENT (N.), 2014, « L'intelligence économique, créatrice de valeur publique dans les PME », in BOURNOIS (F.), CHANUT (V.), RIVAL (M.) (dir.), *Intelligence économique et lobbying au crible des valeurs publiques*, Paris, ESKA.
- LEONETTI (X.), 2012, « Intelligence économique et contrefaçon », *Revue de la gendarmerie nationale*, n° 243, 49-56, septembre.



## Douanes et protection de l'entreprise

Bruno DOMINGO

La douane constitue-t-elle un instrument pertinent d'une stratégie de défense et de sécurité économiques ? Quelle efficacité conserve-t-elle à l'heure du commerce mondialisé et du libre-échange généralisé ? Comment se positionne-t-elle face aux entreprises nationales qui recherchent à la fois une protection face à la mondialisation mais aussi, dans le même temps, l'ouverture de nouveaux marchés à l'international ? Comment est-elle appréhendée par les grands groupes économiques multinationaux à la recherche de territoires attractifs et

performants pour la maximisation de leurs investissements et la localisation de leurs activités ? Enfin, comment les entreprises privées se positionnent-elles face aux dimensions criminelles de l'économie au niveau transnational et quel rôle la douane joue-t-elle en matière de régulation ?

Cet article revient sur quelques-uns de ces enjeux en les discutant du point de vue socio-politique plutôt que strictement économique. Il met en exergue un constat aujourd'hui largement partagé : si les droits de douane, *stricto sensu*, ont historiquement constitué un instrument de protection économique, leur utilisation s'est désormais considérablement affaiblie dans le cadre de la libéralisation du

**Bruno DOMINGO**



Consultant et formateur. Ancien auditeur de l'INHESJ, il est chercheur associé en Science-

Politique à l'Université Toulouse Capitole, et membre du bureau de l'Association Française de Criminologie.

commerce international depuis la fin de la Seconde Guerre mondiale. Néanmoins, l'action des administrations douanières continue d'être mobilisée. De même, diverses mesures qualifiées de « douanières » (au sens où elles se traduisent par une action de régulation aux frontières opérée par les services des douanes) sont également appliquées dans le cadre d'un système d'instruments de protection économique que les États et les autres ensembles économiques régionaux utilisent pour mener à bien leurs stratégies commerciales « défensives », mais aussi désormais plus « offensives ». Parallèlement, les intérêts des différentes entreprises ne peuvent plus être saisis de façon unidimensionnelle. Selon la conjoncture économique, leur secteur d'activité, leur « nationalité », les demandes de protection formulées par les acteurs économiques vont s'avérer éminemment variables. La protection douanière du territoire, des populations et des acteurs économiques apparaît ainsi particulièrement complexe. Elle implique de prendre en compte de nouveaux compromis entre douanes et entreprises dans un espace mondial toujours plus ouvert économiquement et exposé à de nouveaux risques criminels transnationaux.

Ce sont ces multiples enjeux de la transformation des relations entre douanes et entreprises que l'on tentera de présenter dans les développements suivants. Ils soulignent les modalités particulièrement subtiles selon lesquelles se restructurent les relations des acteurs autour des nouveaux contextes économiques et de sécurité. Cette régulation douanière recouvre à la fois des enjeux et des instruments traditionnels de protection tarifaires, mais aussi le développement de la compétitivité des territoires et des firmes, ainsi que la lutte contre la criminalité organisée et le terrorisme au niveau international. Elle se met en place dans un environnement mondial particulièrement fluide où l'on assiste à un découplage relatif entre populations, acteurs économiques, et pouvoirs politiques territorialisés.

## Le legs de l'État douanier territorial

On tentera, dans un premier temps, de rappeler comment s'est construit un État douanier territorial qui s'est présenté comme le garant de la sécurité économique des entreprises de son territoire. Les droits de douane ont été historiquement structurés aux frontières nationales et ont participé à une forte limitation du libre-échange entre les États. Perçus principalement à l'importation, ils se présentent à la fois comme un outil d'ordre fiscal (ils alimentent le budget de l'État) et économique (ils permettent la protection de certains secteurs de l'économie nationale d'une concurrence extérieure

jugée déstabilisatrice). Ces droits peuvent être « ad valorem », c'est-à-dire calculés sur la base d'un pourcentage de la valeur du bien importé, ou bien « spécifiques », se fondant alors sur le paiement d'une somme fixe par unité de bien importé. Le filtrage des flux commerciaux internationaux aux frontières a également eu pour objectif de protéger les populations des flux de marchandises pouvant affecter leur sécurité.

En France, ce modèle ne s'est progressivement affirmé que lors de la période révolutionnaire. Ce n'est qu'à la suite de la Révolution française que les limites douanières ont réellement épousé les frontières du territoire national. Toutes les marchandises entrant ou sortant de ce même territoire pouvaient dès lors être soumises au même « tarif douanier » (établissant la nomenclature des marchandises sur lesquelles étaient désormais opérées les perceptions fiscales). Cette harmonisation entre les frontières politiques et les frontières douanières est advenue au terme d'un assez lent mouvement d'unification territoriale dont les grands principes avaient déjà été initiés par Colbert au XVII<sup>e</sup> siècle. Ce dernier avait en effet entrepris un énorme effort de simplification de la circulation des marchandises en mettant fin à de très nombreux droits et « traites » qui s'appliquaient – de façon désordonnée – aux frontières des différentes provinces, c'est-à-dire à l'intérieur même du territoire national. La Ferme générale, ancêtre de notre administration des douanes moderne, était alors en charge d'assurer, pour le compte de l'État, la perception des droits. Considérée comme usant abusivement de ses pouvoirs, elle fera l'objet de nombreuses critiques et se verra remplacée par une nouvelle administration publique, l'administration des douanes, à la suite de la Révolution française. La période révolutionnaire marque donc l'affirmation d'un État clairement inscrit dans ses frontières, au sein duquel la liberté de circulation des marchandises est assurée, les anciennes « traites » intérieures ayant été supprimées.

Le modèle légué par l'histoire est donc celui d'un État douanier territorial. L'État est ainsi devenu un espace économique unifié à l'intérieur duquel la circulation des

*Le modèle légué par l'histoire est donc celui d'un État douanier territorial. L'État est ainsi devenu un espace économique unifié à l'intérieur duquel la circulation des marchandises est reconnue et aux frontières duquel le commerce est régulé par l'intermédiaire de l'instrument douanier. La douane est alors devenue un instrument central de la politique commerciale organisant et régulant les échanges avec l'étranger.*

marchandises est reconnue et aux frontières duquel le commerce est régulé par l'intermédiaire de l'instrument douanier. La douane est alors devenue un instrument central de la politique commerciale organisant et régulant les échanges avec l'étranger. Le territoire national devient dès lors l'unité pertinente pour l'organisation des échanges économiques internationaux, les pouvoirs politiques alternant les périodes de libéralisme et de protectionnisme économiques. Ainsi, selon Rainelli, « *l'étude des politiques commerciales depuis le début du XIX<sup>e</sup> siècle révèle qu'il n'y a pas de tendance lourde orientée dans un sens, le protectionnisme laissant par exemple progressivement la place au libre-échange. Bien au contraire, il existe des cycles marqués par l'affaiblissement ou par le renforcement du protectionnisme, qui peuvent être rapprochés des fluctuations générales de l'activité économique. En règle générale, les périodes de récession favorisent la montée du protectionnisme, alors que celles d'expansion sont plus favorables au libre-échange* » [Rainelli, 2002, p. 5].

Les entreprises nationales et les populations pouvaient donc vivre sous l'aile protectrice de cet État douanier territorial définissant une politique commerciale en liaison avec ses objectifs de puissance. Historiquement, les droits de douane perçus aux frontières ont été utilisés pour protéger des secteurs économiques particuliers. L'un des exemples les plus classiques est la mise en place des « Corn Laws » en Angleterre au XVII<sup>e</sup> siècle. Ces lois protectionnistes, destinées à protéger l'industrie céréalière, seront abrogées en 1846 sous la pression de groupes libre-échangistes, mais également des famines touchant l'Irlande. En France, le tarif dit « Méline » (du nom du président de la Chambre des députés qui le fera adopter) augmentera sensiblement les droits perçus sur les marchandises importées avec pour objectif de protéger les agriculteurs contre les produits agricoles étrangers à bas prix. Aux États-Unis, durant la crise de 1929, le gouvernement fera également voter un dispositif douanier protectionniste, le *Smoot-Hawley Tariff Act*, promulgué le 17 juin 1930. Ces mesures, destinées à protéger des secteurs industriels ou agricoles nationaux, ont souvent mauvaise presse. D'une part, leur instauration peut aboutir à renchérir le prix des produits offerts à la population nationale. Protection des industries et optimisation des prix offerts aux citoyens peuvent donc se présenter comme des objectifs opposés pour les gouvernements nationaux. En outre, l'instauration de protections tarifaires généralisées peut engager un cycle de « guerre douanière », avec la mise en œuvre de représailles commerciales ayant pour effet de limiter le volume des échanges et les gains pour chacun des États. Enfin, les mesures douanières trop protectrices pour le tissu économique national peuvent générer une économie de rente au détriment non seulement du consommateur, mais également de la performance économique générale de la nation. En effet,

des acteurs économiques non soumis à la concurrence risquent de ne plus s'adapter au contexte mondial tant en termes d'organisation que d'innovation.

## Vers une fin des barrières douanières ?

Ce modèle stato-centré évoluera fortement à la suite du second conflit mondial avec la libéralisation d'un commerce international porteur d'ambitions en matière de développement économique et humain. Les droits de douane vont ainsi progressivement devenir résiduels suite à un vaste mouvement de désarmement tarifaire, sans pour autant disparaître complètement. Le niveau des droits de douane est ainsi abordé comme un problème à la fin de la Seconde Guerre mondiale. Le *General Agreement on Tariff and Trade* (accords du GATT) de 1947 acte que les droits de douane constituent de « *sérieux obstacles au commerce* » et que des négociations doivent être conduites pour assurer une « *réduction substantielle* » de leur niveau général. La libéralisation du commerce international est alors appréhendée comme un facteur de développement économique profitable à l'ensemble des États. Centrée principalement sur la réduction du niveau des droits de douane, elle constituait une réponse à la phase protectionniste qui s'était développée à la suite de la crise de 1929, et qui était considérée comme portant une responsabilité dans le déclenchement de la guerre.

Le GATT va ainsi promouvoir la « clause de la nation la plus favorisée » (approche multilatérale) et engager une série de négociations (« cycles » ou « rounds ») qui offriront un cadre aux négociations jusqu'à la création de l'Organisation mondiale du commerce (OMC) en 1994. Pour Olivier Pastré, « *le premier round de négociations [...] s'est déroulé en 1947 à Genève en présence de 23 pays fondateurs et a permis de décider rien moins que 45 000 réductions tarifaires concernant la moitié du commerce mondial. Puis il y a eu l'Ancey round en 1949 (5 000 réductions), le Torquay round en 1951 (8700) puis trois autres rounds qui virent les concessions tarifaires se multiplier. Jusqu'au Kennedy round (1963-1967), qui vit le nombre de participants s'élargir à 62 et les questions non tarifaires abordées. Le Tokyo round (1973-1979) permit d'aborder enfin de front les questions qui fâchent dans le domaine agricole, et l'Uruguay round (1986-1994) celles concernant la propriété industrielle en présence de 107 pays* » [Pastré, 2006, p. 87-88]. À partir des années 1970, les négociations vont ainsi progressivement s'étendre à d'autres types d'« obstacles au commerce » ne relevant pas du niveau des droits de douane. Ces « mesures non tarifaires » sont variées. Par exemple, les quotas (ou « contingents ») permettent d'importer des biens dans des limites déterminées à l'avance en fonction

des besoins définis pour le marché interne (on parle aussi de « restrictions quantitatives » aux échanges). Ils peuvent être « quantitatifs » (visent à restreindre le volume des marchandises importées) ou « tarifaires » (un certain quota de marchandises peut être importé à un tarif donné ; une fois le contingent atteint, un droit de douane supérieur s'applique aux nouvelles importations). De même, les normes (techniques, sanitaires, environnementales) peuvent être considérées comme des instruments permettant de limiter l'accès à un marché. On peut également évoquer les « subventions nationales » à l'exportation que les États attribuent à leurs industries. Les coûts générés par les complexités administratives entravant la circulation des marchandises au niveau mondial constituent également des formes de restriction de la circulation internationale des marchandises.

Durant la même période, on verra se constituer une régionalisation de l'économie mondiale. La protection douanière va progressivement s'organiser à d'autres échelles que celle de l'État-nation : celle de la région économique supranationale dans le cadre d'unions douanières, voire de marchés communs. Au système de négociation multilatéral du GATT, on va ainsi voir se surimposer une série d'accords commerciaux régionaux. Par exemple, en Europe, suite à l'émergence de la Communauté économique européenne (CEE) en 1957, un « territoire douanier communautaire » est rapidement établi dès 1968. La signature de l'Acte unique européen en 1986 et la réalisation du Grand marché intérieur européen en 1993 ont approfondi ce processus. Les droits de douane sont désormais perçus aux frontières douanières communautaires : la marchandise, une fois « dédouanée » aux frontières extérieures, est alors « mise en libre pratique » et peut circuler librement au sein de l'espace européen. De même, le pouvoir de négociation en matière de commerce international est aujourd'hui situé à Bruxelles, l'Union européenne disposant d'une politique commerciale commune.

Au niveau multilatéral, un nouveau pas sera cependant franchi avec la création de l'Organisation mondiale du commerce à la suite de l'Uruguay Round (1986-1994). Cette organisation constitue désormais l'espace de négociation et de construction des normes pour la libéralisation du commerce international. Néanmoins, dans le cadre du programme de Doha (Qatar) en 2001 et de la conférence ministérielle de Cancún (Mexique) en 2003, les négociations ont buté sur de nombreuses difficultés, notamment concernant le domaine agricole. La conférence ministérielle de Hong Kong en 2006 a également marqué un échec des discussions. Cet

affaiblissement relatif du cadre multilatéral de négociation s'est soldé par une relance des négociations parallèles entre les grands blocs économiques régionaux. Le partenariat transatlantique de commerce et d'investissement (TTIP), espace de travail constitué entre les États-Unis et l'Union européenne, constitue l'un des exemples les plus éclairants de ces dynamiques interrégionales. Un nouvel accord a néanmoins été récemment conclu au niveau multilatéral, avec l'adoption du « paquet de Nairobi » (Kenya), lors de la dixième conférence ministérielle de l'OMC, qui s'est tenue du 15 au 19 décembre 2015. Celui-ci contient six décisions ministérielles sur l'agriculture, le coton et des questions relatives aux pays les moins avancés (PMA). De même, l'OMC cherche aujourd'hui à promouvoir la mise en œuvre de « l'Accord sur la facilitation des échanges » (AFE) destiné à éliminer un ensemble d'obstacles administratifs au commerce.

Les droits de douane ne semblent donc plus appréhendés comme des instruments de protection économique et commerciale pour les États. Aujourd'hui, la moyenne des droits de douane appliqués a été très largement réduite. Les tarifs douaniers moyens des pays industrialisés ont ainsi été divisés par trois entre la fin des années 1949 et le début des années 1960 [Rainelli, 2002, p. 53]. Olivier Pastré souligne que de 1947 à aujourd'hui, la protection moyenne est passée de 48 % à environ 5 %, avec une multiplication par 22 des exportations. En 2014, selon les données fournies par l'OMC, ils étaient de 5,31 % pour l'Union européenne, de 3,51 % pour les États-Unis, de 4,17 % pour le Canada, de 8,43 % pour la Fédération de Russie, de 9,55 % pour la Chine, de 4,21 % pour le Japon et de 13,48 % pour l'Inde. Leur niveau moyen peut ainsi être considéré comme résiduel. Les droits de douane apparaissent ainsi comme des instruments archaïques de protection pour les pays industrialisés. Ils sont souvent considérés comme des vestiges de temps protectionnistes et renvoient à des périodes de repli, de crise, voire de guerre, que la plupart des acteurs politiques et économiques veulent aujourd'hui conjurer au profit d'une logique d'ouverture et de croissance économique partagée. Cette vision libérale, souvent fondée sur le paradigme de la spécialisation internationale du travail et du « *doux commerce* » cher à Montesquieu, s'est affirmée comme le modèle dominant pour la construction des relations commerciales internationales depuis la fin de la Seconde Guerre mondiale. Ainsi, aucun chef de gouvernement ne se risque, aujourd'hui, à évoquer le retour d'un protectionnisme fondé sur le rétablissement de droits de douane élevés à l'importation.

## La remise en question des protections tarifaires douanières

Les États et les principales organisations économiques internationales, notamment l'OMC, se prononcent pour une libéralisation toujours plus forte des flux commerciaux de marchandises et de services. Néanmoins, les difficultés économiques de certains États occidentaux (dont la France), qui se traduisent par une hausse du chômage et un processus de désindustrialisation, conduisent les opinions publiques et certaines entreprises à demander une plus grande protection des marchés nationaux. Elles ont donné lieu à un retour des arguments protectionnistes dans le débat public et politique (en France, notamment à la veille des élections présidentielles françaises de 2012). On peut identifier, dans l'histoire de la théorie économique, des précurseurs justifiant des formes modérées ou ciblées de protectionnisme. Alexander Hamilton, en 1791, dans son *Rapport sur les manufactures américaines* soulignait la nécessité de protéger les entreprises nouvelles face à la concurrence des entreprises étrangères plus matures. De même, en Allemagne, Friedrich List prônait au XIX<sup>e</sup> siècle un « protectionnisme éducateur » destiné à protéger les industries naissantes au moyen d'une utilisation sélective des droits de douane. Plus récemment, des auteurs se sont prononcés pour la mise en place d'un protectionnisme de zone, notamment au sein de l'Union européenne, tels Jean Marcel Jeanneney, Maurice Allais, et plus récemment Walden Bello, Emmanuel Todd ou Jacques Sapir. L'enjeu n'est alors pas tant de protéger les entreprises que d'offrir une régulation adaptée par rapport à la concurrence des pays « moins-disants » socialement. Le débat sur la taxation des marchandises aux frontières de l'Europe a également pris les atours d'une « fiscalité écologique » afin de taxer les marchandises ne respectant pas des conditions de production respectueuses de l'environnement. Trois journalistes économiques (Franck Dedieu, Benjamin Masse-Stamberger et Adrien Tricornot) publiaient également en 2012, chez Gallimard, un livre au titre particulièrement évocateur – *Inévitable protectionnisme* –, dans lequel ils pointaient la difficulté de remettre en question les dogmes libéraux issus de l'après-Seconde Guerre mondiale. L'ouvrage se prononce pour la définition d'un protectionnisme « positif, européen, social et écologique, à l'opposé du nationalisme et du repli sur soi ».

En France, les partis politiques se positionnent peu sur ces questions. Mis à part quelques débats sur le « patriotisme économique » défendu par un Dominique de Villepin ou une « Démondialisation » soutenue par Arnaud Montebourg, les réflexions politiques se centrent davantage sur la question de la compétitivité que de la défense économique. Le Front national est le seul parti

politique à évoquer une réintroduction de droits de douane aux frontières nationales. Son programme propose que des « protections raisonnées aux frontières nationales, via notamment des droits de douane ou des contingentements, soient déterminées non seulement selon le niveau de protection sociale des pays exportateurs, mais aussi selon la qualité écologique et de sécurité de leur production ». De même, il indique que « toute tentative des institutions européennes d'accepter dans le cadre de l'OMC de nouvelles réductions des tarifs douaniers, du soutien interne, des subventions à l'exportation ou de la protection des indications géographiques rencontrera d'emblée l'opposition de la France. [...] Cette politique se fera parallèlement à la mise en place de protections intelligentes aux frontières face à la concurrence internationale déloyale (droits de douane ciblés et quotas d'importation), c'est-à-dire vis-à-vis des pays qui nous concurrencent de façon déloyale (par exemple la Chine ou certains pays d'Europe de l'Est, mais non les pays de niveau économique, social et environnemental comparable comme l'Allemagne ou les États-Unis) ». Néanmoins, ces instruments existent au niveau européen et sont déjà mobilisés sélectivement dans le cadre des dispositifs de défense commerciale.

La question de la réintroduction de protections commerciales, dont les droits de douane constituent l'archétype, porte cependant au-delà du débat politique. Un sondage commandé par l'association Manifeste pour un débat sur le libre-échange, réalisé par l'IFOP en mai 2011 et publié par le quotidien *La Croix*, interrogeait le projet de réinstaurer des barrières plus fortes aux échanges mondiaux [IFOP, 2011]. Ce sondage, intitulé « Les Français, le protectionnisme et le libre-échange » visait à recueillir l'opinion des Français à l'égard de l'ouverture des frontières et des droits de douane. Ses résultats soulignent le sentiment de « révolte » présent chez de nombreux Français, notamment chez les employés (52 % de révoltés) et les ouvriers (64 %), face à la situation économique et sociale de la France à la veille des élections présidentielles de 2012. Il expose le jugement très négatif porté à l'égard des conséquences de l'ouverture des frontières sur l'économie française. La vision d'une « mondialisation heureuse » semble avoir vécu en ce début de XXI<sup>e</sup> siècle. Le sentiment d'une détérioration des conditions de vie touche d'ailleurs autant les sympathisants de la gauche que de la droite partisane. Ainsi, seuls 24 % des sondés pensaient que l'ouverture des frontières était plutôt une « bonne chose » pour la France. De même seuls 18 % pensaient qu'il s'agissait d'une bonne chose pour les petites et moyennes entreprises françaises, et 13 % seulement une bonne chose pour les salariés français. Les sondés pensaient en revanche que cette ouverture bénéficiait aux sociétés multinationales (54 % des sondés) et aux pays en voie de développement (50 % des sondés). Ces résultats soulignent le clivage existant, dans les perceptions sociales, entre le modèle de la « petite entreprise », fondée sur un

modèle productif attaché au territoire national et souffrant de la concurrence internationale, y compris sur le marché national, et le modèle de la firme multinationale fondé sur des capacités à assurer une mobilisation stratégique de ses ressources financières et productives au niveau global. Les projections réalisées par les sondés sont également très pessimistes : 75 % des sondés déclaraient que l'ouverture des frontières françaises à des marchandises chinoises ou indiennes, et réciproquement, aurait des effets négatifs sur l'emploi. Seuls 11 % des sondés pensaient à des effets positifs sur l'emploi. Ainsi, plus des deux tiers des sondés (soit 70 %) se disaient opposés au faible niveau des taxes appliquées aux marchandises en provenance des pays émergents (dont 40 % de « plutôt opposé » et 30 % de « tout à fait opposé »). Ces sondés se prononçaient ainsi à 65 % pour une augmentation des droits de douane et, ici encore, cet avis transcendait les clivages partisans (71 % pour les sympathisants PS, 75 % pour les sympathisants UMP, et 61 % pour les sympathisants Front national). Seulement 14 % des sondés indiquaient qu'il ne faudrait « pas changer le niveau de ces taxes » et 7 % qu'il faudrait les « baisser ». Les attentes concernant cette hausse des taxes étaient dans l'ordre : la protection du savoir-faire français (59 % pensant que la hausse aurait un impact « positif » en la matière), l'activité des entreprises françaises du secteur de l'industrie (57 % contre 20 %), l'emploi (55 % contre 18 %), la croissance économique en France (50 % contre 19 %), et l'activité des entreprises françaises du secteur de services (42 % contre 19 %). En revanche, les personnes interrogées pensaient que cette hausse des taxes aurait un impact « négatif » sur le prix des produits de consommation en France, donc sur le pouvoir d'achat (44 % déclaraient que la hausse aurait des conséquences « négatives », 29 % des impacts « positifs », 14 % « aucune conséquence »).

Ce sondage est particulièrement intéressant, car il montre un attachement, au sein de la population, à l'instrument tarifaire douanier comme outil de protection de l'économie nationale tant au niveau de la préservation de l'appareil productif que de celle des emplois. Il montre que ce dernier est jugé utile pour protéger les petites et moyennes entreprises plutôt que les firmes multinationales jugées plus aptes à bénéficier de la libéralisation commerciale internationale. Il met également en exergue une forme de découplage entre sphère sociale et sphère politique. Alors que cette dernière tend à souligner les gains liés à l'ouverture réciproque des marchés en matière économique, les populations tendent aujourd'hui à douter des bénéfices de la mondialisation. Les négociations commerciales conduites dans le cadre de l'OMC ou du Partenariat transatlantique de commerce et d'investissement (TTIP) donnent ainsi lieu à de nombreuses contestations, car jugées obscures et éloignées de l'espace démocratique.

## Le démantèlement des dernières barrières douanières

En dépit de ces contestations, la réintroduction de droits de douane traditionnels ne semble pas à l'ordre du jour dans les espaces de négociation commerciale. Dans un document récent de la direction générale au Commerce de la Commission européenne, dénommé « L'UE, commerce et investissements 2014 », on sent même poindre, au sein des institutions européennes, la crainte que ces contestations du libre-échange ne se traduisent par un repli économique généralisé. L'argumentaire européen mobilisé au sein de ce document débute, en effet, par un slogan : « *Protectionnisme ? Non merci !* » (Commission européenne, 2014, p. 5). Il souligne les risques économiques d'une mise à distance de l'économie européenne par rapport aux circuits commerciaux mondiaux. Pour la Commission européenne en effet, « *deux tiers des importations de l'Union européenne concernent des matières premières et des composants entrant dans des processus de production. Accroître le coût des importations rendrait les producteurs européens moins compétitifs aussi bien sur le marché domestique de l'UE qu'à l'exportation, avec pour corollaire direct des pertes de production et d'emplois au niveau européen. En outre, de nos jours, les produits (comme les smartphones) sont rarement fabriqués dans un seul pays. L'adoption par l'Union de mesures protectionnistes exclurait dès lors les entreprises européennes des chaînes d'approvisionnement internationales — le résultat final étant que nous devrions alors payer davantage pour des articles tels que téléphones mobiles et tablettes et que moins de valeur serait produite en Europe. Tout cela démontre que, de plus en plus, les pays doivent importer pour être en mesure d'exporter, ce qui souligne l'importance vitale de l'intégration dans le système commercial mondial pour parvenir à une croissance durable. Un repli protectionniste de l'UE aurait, qui plus est, pour effet de déclencher des actions de rétorsion d'autres niveaux. L'Union serait la première à souffrir d'une guerre protectionniste, à la fois parce qu'elle est un grand exportateur mondial et du fait que nombre de ses partenaires ont libéralisé de façon autonome et appliquent des droits inférieurs à leurs obligations légales, ce qui implique qu'ils pourraient aussi les relever. Durant la crise financière de 2008-2009, alors que, considérées séparément, les mesures aux frontières n'affectèrent qu'environ 1 % du commerce mondial, elles produisirent un effet double sur les exportations de l'Union européenne. En cas de guerre commerciale, l'UE éprouverait aussi plus de difficultés pour financer son déficit croissant en produits énergétiques (458 milliards d'euros en 2012), dû en grande partie à son manque de ressources naturelles. L'Union a aussi pris en interne des mesures importantes afin de réduire le protectionnisme, comme en témoigne, dans le domaine agricole, le plafonnement des aides accordées aux agriculteurs européens* » (Commission européenne, 2014, p.5). Pour les instances européennes, toute réinstauration de droits de douane élevés aurait ainsi des effets pénalisants pour l'ensemble de la zone européenne à la fois en termes

de performance économique et d'emploi. Ainsi, les États encouragent-ils toujours leur démantèlement en dépit de leur niveau déjà réduit.

À ces éléments s'ajoute la prise en considération des nouveaux référentiels d'analyse du commerce mondial qui tendent à démontrer que les droits de douanes, même à un niveau réduit, affectent toujours la performance du commerce international. Ce dernier ne correspond plus à celui qui prévalait au XIX<sup>e</sup> et XX<sup>e</sup> siècle. Comme le note Michalet, « *la part des échanges intra branches, d'un côté, et celle des échanges intra firmes, de l'autre, deviennent toutes les deux de plus en plus importantes dans le commerce total. Il s'ensuit que les échanges sont composés d'une façon croissante de biens intermédiaires et de composants. Ces constats entrent radicalement en contradiction avec les analyses classiques de la spécialisation internationale* » [Michalet, 2007, p. 46]. Cette mutation des échanges internationaux se fonde donc aujourd'hui sur la notion de « *chaîne de valeur mondiale* » [Vadcar, 2015]. La fragmentation des processus de production implique que des droits de douanes, certes désormais minimes mais néanmoins multiples, affectent les nombreux échanges internationaux nécessaires à la réalisation d'un seul et même produit. Ils s'accumulent alors le long de la chaîne de fabrication désormais organisée au niveau international [OMC, 2015]. Ainsi, même résiduels, les droits de douane sont à nouveau considérés comme affectant la compétitivité des entreprises multinationales. Ils font d'ailleurs l'objet d'un chapitre de négociation entre l'Union européenne et les États-unis au sein du TTIP (dans un autre document, « Le partenariat transatlantique de commerce et d'investissement : 10 idées reçues sur le TTIP. Démêler le vrai du faux », la Commission européenne souligne d'ailleurs l'intérêt pour les entreprises à démanteler les derniers droits de douanes existant entre les États-Unis et l'Union européenne).

Par-delà le niveau des stricts droits de douanes, ce sont également les procédures administratives douanières qui sont désormais perçues comme affectant la performance économique des entreprises. On peut ainsi lire sur le site internet de l'OMC : « *selon la Conférence des Nations unies sur le commerce et le développement (CNUCED), pour une transaction douanière il y a en moyenne 20 à 30 intervenants différents, 40 documents, 200 éléments de données (dont 30 se répètent au moins 30 fois), et 60 à 70 % de l'ensemble des données qui sont saisies au moins deux fois. Avec l'abaissement des droits de douane dans le monde entier, le coût des formalités douanières excéderait dans bien des cas le montant des droits à acquitter. Dans l'environnement commercial actuel, qui appelle des méthodes de production et de livraison en flux tendu, il faut que les négociants puissent prévoir et effectuer rapidement la mise en circulation des marchandises* » [site OMC, 2016]. Ainsi, les membres de l'OMC, lors de la conférence ministérielle

de Bali en décembre 2013, ont négocié un « Accord sur la facilitation des échanges » (AFE) et ont adopté, le 27 novembre 2014, un protocole d'amendement pour son insertion au sein de l'Accord sur l'OMC. Celui-ci vise à accélérer le mouvement, la mainlevée et le dédouanement des marchandises, dont les marchandises en transit. Il prévoit également une coopération effective entre les douanes et les autres autorités compétentes pour les questions de facilitation des échanges et de respect des procédures douanières. Il comporte aussi des dispositions relatives à l'assistance technique et au « renforcement des capacités » des administrations douanières. L'objectif n'est donc plus seulement de diminuer le niveau des droits de douane, mais tout simplement de faire disparaître toutes les mesures administratives « douanières » susceptibles de ralentir la circulation internationale des marchandises et qui se traduisent par des coûts pour les entreprises. Pour l'OMC, la mise en œuvre de l'AFE pourrait avoir un effet plus important sur le commerce international que l'élimination de tous les droits de douane restants. Les négociations engagées dans le cadre du TTIP visent, elles aussi, le même objectif.

## Utilisation stratégique de la protection douanière et captation de la valeur mondiale

Néanmoins, les batailles tarifaires et surtout l'ensemble des obstacles aux échanges commerciaux n'ont pas totalement disparu au niveau mondial. Il existe toujours des « pics tarifaires », c'est-à-dire des droits de douanes plus élevés appliqués à certains types de productions. Pour les pays industrialisés, des droits de 15 % ou plus sont généralement considérés comme des « crêtes tarifaires ». L'Union européenne conserve par exemple des droits élevés pour protéger son secteur agricole. Cependant, si le protectionnisme tarifaire n'a pas totalement disparu, il ne constitue plus la seule arme économique « douanière » au sein des politiques commerciales. Bien au contraire, il semble constituer la dernière des stratégies mobilisées, au profit de nouveaux modes d'action.

D'une part, les politiques commerciales comportent d'autres instruments de défense commerciale. Par exemple, en 2009, l'Inde prend des mesures protectionnistes contre l'acier et les jouets chinois, la Russie contre les importations automobiles, les États-Unis contre les pneumatiques et les tubes d'aciers chinois. En 2013, un bras de fer s'établit entre l'Union européenne et la Chine contre le dumping de cette dernière concernant les panneaux solaires. Certes, l'instauration de l'OMC a permis la création d'une

nouvelle instance en son sein, l'Organe de règlement des différends (ORD), chargée de participer à la résolution de ces conflits. Cependant, il n'en demeure pas moins que les États et blocs économiques régionaux mettent en œuvre des enquêtes et des mesures anti-dumping ou anti-subsidies destinées à se protéger de flux commerciaux jugés inéquitables du point de vue concurrentiel. Le 33<sup>e</sup> rapport annuel de la Commission européenne sur les activités anti-dumping, anti-subsidies et de sauvegarde de l'Union européenne (document COM (2015) 385 du 03/08/2015) fait ainsi état de 81 mesures anti-dumping et de 13 mesures anti-subsidies en vigueur dans l'UE en 2014, concernant 0,29 % des importations totales dans l'UE. Un exemple récent est celui de la mobilisation du ministre des Finances français, Emmanuel Macron, pour lutter contre le dumping chinois dans le domaine de la sidérurgie. Celui-ci s'est prononcé, au cours au mois de janvier 2016, pour « *une logique de lutte anti-dumping très claire, massive, directe* » à l'égard de la Chine qui concentre 50 % de la capacité mondiale de production d'acier et dont la concurrence affecte les entreprises nationales et européennes.

Les normes sont également souvent utilisées comme des instruments non tarifaires de protection commerciale. Elles rendent l'accès à certains marchés plus difficiles et font donc l'objet de luttes d'influences dans le cadre de la formulation des instruments de politique commerciale. Le respect de ces normes, dont les administrations douanières nationales doivent veiller à l'application, a donc une importance stratégique dans le cadre des nouveaux affrontements économiques internationaux et l'accès aux marchés. Si l'on met souvent l'accent sur l'importance de la formulation politico-économique de ces normes, on oublie bien souvent de souligner que la question de leur respect (et de la sanction de leur non-respect) constitue également un enjeu tout autant stratégique. C'est ici que les services douaniers interviennent, leurs compétences à réguler, au niveau opérationnel, la circulation des marchandises qui ne satisfont pas à un certain nombre de prescriptions étant au centre de la protection des marchés. Néanmoins, le respect des normes concerne également la protection du consommateur, voire sa sécurité, lorsque certaines marchandises ne respectent pas les règles sanitaires ou de sécurité minimales. Un autre point concerne enfin l'utilisation des missions douanières dites de « sécurité » à des fins de protection commerciale. En effet, un certain nombre de protections mises en œuvre dans le cadre de la lutte contre le terrorisme peuvent dissimuler des mesures de limitation des échanges. Dans cette perspective, c'est le champ de la sécurité et de la lutte contre le terrorisme qui est instrumentalisé pour masquer l'instauration de nouvelles protections commerciales. Si l'économie sert parfois à faire la guerre et si elle peut

également être abordée comme un espace guerrier, on ne doit pas occulter que la guerre sert aussi parfois à faire de l'économie. Les protections douanières réinstaurées à des fins de sécurité nationale visent alors moins à se protéger d'un ennemi extérieur qu'à réinstaurer des formes subtiles d'obstacles au libre-échange pour protéger les marchés intérieurs.

Pour autant, ces mesures de néo-défense commerciale masquent le travail plus profond, mais aussi plus obscur et technique, que les administrations douanières conduisent pour améliorer la compétitivité des territoires, d'une part, et pour améliorer les capacités des entreprises nationales à s'implanter sur les marchés étrangers, d'autre part. Ainsi, les administrations douanières ont vu leur mandat fortement évoluer. Elles inscrivent désormais leur action dans le cadre de nouveaux référentiels de « performance » et, notamment pour les États moins développés, de la « modernisation », qui constituent désormais des éléments d'attractivité pour la localisation des activités économiques sur les territoires. Comme le souligne Michalet, « *depuis quelques années, la politique industrielle de l'État revêt de nouveaux atouts pour s'adapter aux besoins de la multinationalisation croissante des firmes qui portent la dynamique de la mondialisation. Elle se transforme en "politique de l'attractivité". Le renversement de perspective est radical. Il ne s'agit plus, comme dans les années passées, d'encourager des firmes à conquérir des marchés à l'étranger, mais désormais, de capter une partie, la plus grosse possible, de l'investissement provenant de l'extérieur sur le territoire domestique* » [Michalet, 2007, p. 128]. Les entreprises multinationales sont en effet particulièrement attentives à la localisation de leurs activités économiques en fonction de la performance économique des territoires, poussant les États et les grandes mégapoles à offrir toujours plus de services aux acteurs entrepreneuriaux et financiers désireux de maximiser leurs investissements et leurs profits. Une administration douanière peu performante augmente les coûts d'entrée sur des marchés et des territoires, que ce soit au moyen de droits de douane jugés trop élevés ou de procédures de dédouanement trop contraignantes. Les territoires sont d'ailleurs clairement mis en compétition au niveau global. Dans son dernier rapport *Doing Business*, la Banque mondiale classe ainsi la France à la première place des 189 pays en matière de commerce transfrontalier, soulignant sa très forte performance en matière de cadre douanier. L'informatisation et la dématérialisation des procédures et l'allégement des modalités du contrôle douanier participent donc d'une politique d'attractivité du territoire en direction des entreprises qui cherchent à localiser leurs activités au niveau mondial.

Parallèlement, les services douaniers se positionnent de plus en plus comme des « partenaires » des entreprises nationales pour la conquête des marchés à l'export. Ils

constituent par ailleurs des instruments d'intelligence stratégique au niveau du commerce international et de la diplomatie économique. Marie-Christine Kessler souligne ainsi, qu'« *au cours des siècles, les États ont toujours intégré des buts économiques dans leur action extérieure, travaillant à la recherche de garanties, de débouchés, de zones d'influence pour leurs ressortissants et leurs produits. Ils ont utilisé des instruments économiques, faveurs ou sanctions. Ils ont signé des accords de libre-échange ou établi des protections douanières. [...] La diplomatie économique suppose donc un territoire et un État national. Elle se définit par la mise en œuvre par une autorité publique, d'une politique à finalité commerciale et financière, destinée à assurer la prospérité économique du pays à travers les intérêts de ses entreprises, de ses groupes socioprofessionnels, de ses citoyens* » [Kessler, 1999, p. 247]. Autrefois souvent considérés comme les ennemis du commerce par les entrepreneurs économiques transnationaux, les services douaniers se positionnent aujourd'hui comme des partenaires des entreprises pour la conquête de nouveaux marchés. La douane française a ainsi lancé un grand plan d'accompagnement des entreprises dans le cadre de la mise en place du nouveau Code des douanes de l'Union qui entrera en application le 1<sup>er</sup> mai 2016. Ce plan de quarante mesures à destination des entreprises, présenté le 22 septembre 2015 au ministère des Finances, cherche explicitement à faire gagner aux plates-formes logistiques françaises des parts de marché à l'international. Il prévoit par exemple la mise en place de procédures de dédouanement centralisé, d'un Guichet unique national (GUN) pour les formalités administratives de passage aux frontières, de renforcer les Cellules conseil aux entreprises (CCE), de créer un Service grands comptes (SGC) pour les grands groupes, de mettre en place un numéro de téléphone d'accueil privilégié pour contacter l'ensemble des services douaniers, de développer encore la numérisation des procédures, de participer à la sécurisation des flux des opérateurs commerciaux, etc. L'un des objectifs est clairement de fluidifier les procédures, avec par exemple la volonté d'aboutir à plus de 95 % de déclarations dédouanées en moins de 5 minutes à l'horizon 2018 (NB : fin 2014, le délai moyen d'immobilisation des marchandises était de 4 minutes 7 secondes). Le plan prévoit également de multiples outils centrés sur l'amélioration des relations douane-entreprise (ex : formations, forums d'échange, etc.) et l'accompagnement de ces dernières par des services douaniers qui se présentent désormais comme des instances de promotion et d'aide aux acteurs privés pour leur déploiement commercial à l'international (ex : mobilisation des attachés douaniers dans les ambassades, apports de conseil sur la mobilisation des procédures douanières, etc.).

## Protéger et sécuriser le commerce mondial et la chaîne internationale de transport

Les douanes s'affirment enfin comme des polices des flux visant à assurer un respect de prescriptions et de différentes normes (sanitaires, sociales, environnementales) visant à la fois la protection des populations et du tissu économique. Dans un contexte géopolitique, où le terrorisme transnational et la criminalité internationale sont susceptibles d'avoir un impact sur le commerce légitime, on voit ainsi se dessiner de nouveaux rapports entre États et entreprises.

Un premier point concerne la mise en place de procédures de restrictions, voire de sanctions, commerciales entre États. Ces mesures sont susceptibles d'avoir des impacts profonds sur les relations économiques internationales. Par exemple, les sanctions économiques prises à l'encontre de la Russie dans le cadre de la crise ukrainienne de 2014 intègrent un certain nombre de mesures relatives à la restriction des échanges (ex : interdiction des importations de biens en provenance de Crimée ou de Sébastopol, sauf s'ils sont accompagnés d'un certificat d'origine ukrainien ; interdiction d'exportation, vers des entreprises de Crimée ou pour un usage en Crimée, des biens et technologies relatifs aux secteurs des transports, des télécommunications et de l'énergie ou utilisés dans l'exploration pétrolière, gazière et minérale). Dans cette configuration, c'est le politique qui imprime au domaine économique un ensemble de contraintes nouvelles qui redessinent le contexte économique mondial au sein duquel évoluent les entreprises. Ainsi, le champ de la sécurité internationale utilise l'instrument douanier pour limiter ou interdire un ensemble de flux commerciaux entre nations. Les États ferment donc, temporairement ou plus durablement, un certain nombre de canaux commerciaux et de marchés, autrefois jugés légitimes. Ils criminalisent du même coup les flux commerciaux qui ne respecteraient pas les nouvelles conditions de circulation.

Un second point concerne le rôle des services douaniers dans la protection du commerce légitime, notamment en matière de respect des normes et des droits de propriété intellectuelle (DPI). La lutte contre la contrefaçon et plus largement aux DPI est devenue une composante de la protection économique des entreprises assumée par les services douaniers. Au niveau international, l'Organisation mondiale des douanes souligne que les produits les plus fréquemment saisis sont des produits pharmaceutiques (la moitié du nombre total de saisies), des vêtements, des ordinateurs, des chaussures et des appareils électroniques.

Au niveau européen, les statistiques publiées le 27 octobre 2015 par la Commission européenne attestent également de l'augmentation du nombre de saisies en matière de DPI (liée à la multiplication des volumes et à la parcellisation des envois liés au commerce en ligne) représentant une valeur des produits authentiques estimée à plus de 617 millions d'euros. Les saisies concernent principalement les cigarettes contrefaites, les jouets et les médicaments. En France, la direction générale des Douanes et des Droits indirects (DGDDI) a saisi plus de 8,8 millions d'articles en 2014, et agit en coordination étroite avec les représentants des entreprises (ex : Comité national anti-contrefaçon, Institut national de la propriété intellectuelle, Union des fabricants, Comité Colbert, titulaires de marques, sites de vente en ligne).

Un troisième point concerne la sécurité du transport de marchandises et de la chaîne logistique internationale. Les menaces terroristes font peser de nouvelles contraintes sur les opérateurs commerciaux, le transport international de marchandises pouvant être soit la cible directe du terrorisme, soit son vecteur par l'acheminement de marchandises suspectes sur le territoire national. Dans cette perspective, douanes et opérateurs économiques ont reconceptualisé leurs relations pour articuler la libre circulation des marchandises et des personnes avec les nouveaux impératifs de sécurité nationale. Depuis une vingtaine d'années, on a ainsi vu se constituer et se renforcer des partenariats entre sphère publique et privée afin de prévenir ces activités illicites et pour préserver l'intégrité des flux commerciaux et des infrastructures de transport (ex : « Programme StairSec » en Suède, « Partners in Protection » au Canada (PIP), « Frontline and Accredited Client » en Australie, « Partenariat entre la douane et les entreprises contre le terrorisme » (C-TPAT) aux États-Unis, « Frontline and Secure Exports Partnership » en Nouvelle-Zélande, Groupe sur le partenariat Douanes/Entreprises et directives sur la gestion de la chaîne logistique internationale de l'Organisation mondiale des douanes). L'irruption de la menace terroriste et son inscription à l'agenda politique depuis le 11 septembre 2001 ont conforté ce rapprochement entre sphère publique et

privée, notamment sur la question de la sécurisation de la chaîne logistique internationale, thématique reprise par l'Organisation mondiale des douanes (OMD) qui a

*Les menaces terroristes font peser de nouvelles contraintes sur les opérateurs commerciaux, le transport international de marchandises pouvant être soit la cible directe du terrorisme, soit son vecteur par l'acheminement de marchandises suspectes sur le territoire national. Dans cette perspective, douanes et opérateurs économiques ont reconceptualisé leurs relations pour articuler la libre circulation des marchandises et des personnes avec les nouveaux impératifs de sécurité nationale.*

construit un « cadre de normes » en la matière. Ce cadre de normes, aujourd'hui baptisé « SAFE », comprend ainsi un pilier spécifique relatif à la coopération douane-entreprise. L'ensemble de ces initiatives ont progressivement conduit à l'élaboration et à la diffusion d'un nouveau statut pour les acteurs du commerce international, celui d'opérateur économique agréé (OEA), aujourd'hui repris notamment dans le cadre de la réforme du Code des douanes de l'Union européenne. Il introduit certains déplacements dans la façon dont est envisagée la relation entre les autorités douanières et le monde du commerce et du transport. L'opérateur commercial n'est plus d'abord considéré comme un fraudeur potentiel, mais comme un partenaire créateur de richesses dont il s'agit, pour les États, de faciliter les opérations internationales. C'est donc un référentiel fondé sur la confiance qui se substitue à celui du soupçon dans les opérations douanières de contrôle des marchandises. Néanmoins, ce déplacement est encadré puisqu'il passe par l'intermédiaire d'un processus de labellisation et d'agrément douaniers reposant sur des critères rationalisés et déterminés *a priori*. La mise en place de ce système d'agrément des opérateurs économiques participe d'une redistribution des compétences entre le public et le privé en matière de contrôles des flux internationaux de marchandises. Les opérateurs privés se

voient plus ou moins contraints d'adopter des dispositifs de prévention et de contrôle au sein de leurs organisations s'ils veulent bénéficier de facilités douanières pour leurs opérations commerciales. Les services douaniers incitent donc fortement les opérateurs économiques à réduire les risques de fraude ou d'atteinte à la sécurité/sûreté de la chaîne logistique internationale, tout en se posant comme des régulateurs de cette chaîne. Dans cette nouvelle stratégie de contrôle, les opérateurs légitimes du commerce participent à leur propre auto-évaluation en matière de sécurité et internalisent un certain nombre de coûts associés. En échange, les administrations douanières offrent un certain nombre de facilitations commerciales susceptibles de permettre des gains de compétitivité

pour les entreprises. Ce système se fonde également sur l'information préalable des autorités douanières par les acteurs privés concernant les envois commerciaux internationaux qui permettent notamment de procéder à une sélectivité des contrôles et à la mise en œuvre d'analyses de risques.

## Vers un État « néo-douanier »

Ces quelques développements attestent des profondes transformations qui affectent aujourd'hui la relation entre douanes et entreprises. Si les douanes étaient originellement positionnées comme des opérateurs fiscaux au service des États et intervenaient pour assurer une protection de secteurs particuliers de l'économie nationale, leur rôle a profondément évolué. L'affaiblissement généralisé des protections douanières tarifaires (droits de douanes) dans le cadre de la forte libéralisation du commerce international, la régionalisation de l'économie,

de même que la volonté des États de promouvoir une simplification des procédures douanières au bénéfice de la fluidité des échanges, ont abouti à renouveler leurs modes d'interventions. Celles-ci organisent dès lors leur activité dans le cadre d'un nouveau commerce mondial fondé sur la fragmentation internationale des processus productifs et sur la multinationalisation des acteurs économiques. Elles cherchent à développer une approche davantage offensive de leur action en intervenant sur trois dimensions : offrir un cadre optimisé de traitement des flux commerciaux pour capter de la valeur sur le territoire intérieur, accompagner les entreprises dans leurs logiques de performance à l'export, et enfin, sécuriser la chaîne du transport international de marchandises en impliquant directement les acteurs privés du commerce dans la régulation et le contrôle. Cet État « néo-douanier » fonctionne ainsi bien différemment de l'« État douanier territorial » qui s'était constitué à partir du XVII<sup>e</sup> siècle et qui reste, pour beaucoup de citoyens, l'une des figures protectrices d'un territoire national et de frontières aujourd'hui en profonde mutation ■

## Bibliographie

- ALBERT (J.-L.), 2013, *Douane et droit douanier*, Paris, PUF.
- BERR (C. J.), 2008, *Introduction au droit douanier*, Paris, Economica.
- CLINQUART (J.), 1990, *La douane et les douaniers de l'Ancien Régime au Marché commun*, Paris, Tallandier.
- COLLE (D.), 2014, « Les théoriciens de la guerre économique », *Conflits*, Hors-série, n° 1, Hiver, p. 16-18.
- Commission européenne, 2014, *L'UE, commerce et investissements*.
- GAUCHON (P.), 2014, « Nous sommes en guerre économique », *Conflits*, Hors-série, n° 1, Hiver, p. 6-11.
- IFOP, 2011, « Les Français, le protectionnisme et le libre-échange ».
- KESSLER (M.-C.), 1999, *La politique étrangère de la France. Acteurs et processus*, Paris, Presses de Science Po.
- MICHALET (C.-A.), 2007, *Mondialisation, La Grande rupture*, Paris, La découverte.
- OMC, 2015, *Rapport sur le commerce mondial*.
- PASTRÉ (O.), 2006, *La méthode Colbert ou le patriotisme économique efficace*, Perrin.
- RAINELLI (M.), 2002, *L'Organisation mondiale du commerce*, Paris, La découverte, collection Repères.
- SALIN (P.), 2002, *Le libre-échange*, Paris, PUF, collection QSJ.
- VADCAR (C.), 2015, « Les chaînes de valeur mondiales. Paradigme du commerce international », *Friedland Papers*, CCI Paris, mars.

# Les services de sécurité privée en Europe : faits et chiffres

Marc COOLS, Harald OLSCHOK, Veerle PASHLEY et Dany VANDORMAEL

## Introduction

La CoESS – ou « Confédération européenne des services de sécurité » – est une organisation européenne regroupant 26 associations nationales d'entreprises de sécurité privée. L'organisation a pour habitude de présenter un aperçu quantitatif des services de sécurité européens, intitulé *Facts and Figures*. Notre contribution fournit un résumé de son édition de 2013<sup>1</sup>. Nous sommes convaincus que cette contribution peut être envisagée comme une mise à jour d'un précédent article, « La sécurité privée en Europe : analyse des trois livres blancs », paru dans les *Cahiers de la Sécurité*<sup>2</sup>.

Cet article comporte six parties. Dans un premier temps, nous décrirons notre méthodologie. En deuxième lieu, nous

présenterons un résumé quantitatif de l'état du secteur européen de la sécurité privée. Dans une troisième partie, nous nous attarderons sur l'état de la législation européenne en matière de sécurité privée. Notre quatrième partie portera sur la coopération public-privé dans le domaine de la sécurité. En cinquième lieu, nous évoquerons la lutte contre la piraterie en haute mer et la sécurité maritime. Enfin, dans une sixième partie, nous proposerons une vision future des moteurs et des obstacles d'une approche intégrée de la surveillance et de la sécurité des technologies.

Les présents résultats constituent une synthèse d'un rapport intitulé « Private Security Services in Europe – CoESS Facts & Figures 2013 ». Ce document – une quatrième édition<sup>3</sup> – dresse un panorama global du paysage européen des services de sécurité privée et cible une large zone géographique de 34 pays, composée des 28 États membres de l'UE ainsi que de six autres pays européens : Bosnie-Herzégovine, Macédoine, Norvège, Serbie, Suisse et Turquie.

### Marc COOLS



Professeur au sein du groupe de recherche en criminologie, Vrije Universiteit Brussel, et du groupe de recherche en droit pénal et criminologie, Université de Gand.

### Harald OLSCHOK



Chef d'Entreprise du « BDSW – Bundesverband der Sicherheit-swirtschaft » (Union Fédérale allemande des études de Renseignement).

### Veerle PASHLEY



Assistante au sein du groupe de recherche en droit pénal et criminologie, Université de Gand.

### Dany VANDORMAEL



CEO de SERIS BeNeLux.

(1) CoESS, *The new security company: integration of services and technology responding to changes in customer demand, demography and technology*, Berlin, 23 avril 2015, 51 p.

(2) Cools, M., Pashley, V., « La sécurité privée en Europe : analyse des trois livres blancs », *Cahiers de la Sécurité*, Paris, INHESJ, 2012, 40-54.

(3) La CoESS a publié un rapport intitulé *Private Security in Europe – CoESS Facts & Figure*



Le rapport permet de mettre à jour de façon précise l'état du secteur des services de sécurité privée en se concentrant sur les aspects suivants :

- aspects économiques : marché de la sécurité privée, contrats de sécurité privée, entreprises de sécurité privée et agents de sécurité privée ;
- aspects juridiques : législation en matière de sécurité privée, contrôles et sanctions, conventions collectives de travail, conditions et restrictions d'accès, exigences spécifiques, pouvoirs et compétences, armes, K9 (unité cynophile), formation et dispositions connexes, coopération public-privé et lutte contre la piraterie en haute mer.

Nous avons également inclus des informations relatives à la coopération public-privé ainsi qu'à la lutte contre la piraterie en haute mer. Nous fournirons par la suite un aperçu de ces questions.

## Méthodologie

Les informations mentionnées nous ont principalement été fournies par les fédérations membres de la CoESS au niveau national, par d'autres organisations nationales de sécurité privée et par des pays européens<sup>4</sup>. Des informations complémentaires pertinentes ont été recueillies grâce à des recherches documentaires et à l'assistance d'autorités (locales), d'organisations internationales, de structures diplomatiques et universitaires et d'autres organismes compétents<sup>5</sup>.

Avant d'apporter leurs contributions à l'élaboration de ce rapport, les fédérations membres de la CoESS au niveau national, les autres organisations nationales de sécurité privée et les pays européens ont reçu un descriptif détaillé des données attendues. Il convient de préciser que les pays suivants ne nous ont pas fait parvenir de mises à jour : Bosnie-Herzégovine, Bulgarie, Chypre, Danemark, Estonie, Hongrie, Lituanie, Malte, Portugal, République tchèque et Slovaquie. Nous avons recueilli

(4) La CoESS remercie chaleureusement l'ensemble des organisations impliquées pour leurs contributions, ainsi que pour le temps et les efforts investis pour atteindre ce brillant résultat. Leur soutien continu contribue à établir une représentation globale et réaliste de l'état actuel du secteur européen des services de sécurité privées en 2004, 2008 et 2011.

(5) La CoESS exprime sa profonde gratitude pour leurs précieuses contributions.

des informations auprès des pouvoirs publics et des informations juridiques afin de mettre à jour les données de façon aussi précise que possible.

## Résumé du rapport CoESS Fact et Figures 2013

La présentation d'un aperçu quantitatif européen du secteur de la sécurité privée est unique, dans la mesure où la recherche scientifique en la matière est limitée. Néanmoins, plusieurs variables rendent difficile l'obtention d'une analyse fiable. Le secteur de la sécurité privée n'est ni homogène, ni structuré. Les résultats dépendent de la disponibilité des informations. Cela signifie que nous devons compter sur la bonne volonté des organisations à investir sans cesse dans la fourniture de résultats actualisés.

Nous sommes en mesure de présenter une vision d'ensemble des variables suivantes. L'obtention d'une licence pour les entreprises de sécurité privée est imposée par la loi dans 94 % des pays européens. Un « principe de spécialité » pour les entreprises de sécurité privée<sup>6</sup> est intégré à la législation régissant le secteur de la sécurité privée dans 18 % des cas. Le nombre moyen de véhicules blindés en Europe pour les opérations de transport de fonds (CIT) est de 825.

De plus, l'obtention d'une licence pour les agents de sécurité privée est imposée par la loi dans 88 % des cas. L'âge moyen d'un agent de sécurité privée dans le secteur de la sécurité privée est de 35 ans et le pourcentage moyen d'hommes travaillant dans ce secteur est de 83 %, contre 17 % pour les femmes. Une politique d'égalité des chances est en place dans le secteur de la sécurité privée dans 85 % des pays européens. Le taux annuel moyen de rotation du personnel dans le secteur de la sécurité privée est de 33,27 %.

Le secteur de la sécurité privée est réglementé par une législation spécifique au secteur dans 94 % des pays européens. L'autorité nationale compétente chargée

d'élaborer et de modifier la législation réglementant le secteur de la sécurité privée est soit le ministère de l'Intérieur ( $\pm 53\%$ ), soit le ministère de la Justice ( $\pm 16\%$ ), soit la police ( $\pm 6\%$ ), soit un autre organisme ( $\pm 25\%$ ).

L'autorité nationale compétente chargée des contrôles et inspections pour le secteur de la sécurité privée est soit la police ( $\pm 41\%$ ), soit le ministère de l'Intérieur ( $\pm 38\%$ ), soit le ministère de la Justice ( $\pm 3\%$ ), soit un autre organisme ( $\pm 18\%$ ). L'autorité nationale compétente chargée d'imposer des sanctions administratives est soit le ministère de l'Intérieur ( $\pm 38\%$ ), soit la police ( $\pm 29\%$ ), soit le ministère de la Justice/les tribunaux ( $\pm 15\%$ ), soit un autre organisme ( $\pm 18\%$ ). L'autorité nationale compétente chargée d'imposer des sanctions pénales est soit la police ( $\pm 25\%$ ), soit les tribunaux ( $\pm 38\%$ ), soit le ministère de l'Intérieur ( $\pm 22\%$ ), soit un autre organisme ( $\pm 15\%$ ). Dans chacun des pays européens, ces sanctions éventuelles peuvent avoir pour conséquence le retrait de la licence d'une entreprise et/ou le retrait de la licence d'un agent individuel.

Des conventions collectives de travail contraignantes spécifiques au secteur sont en vigueur dans 62 % du secteur de la sécurité privée. Les conditions d'accès pour les entreprises (propriétaires) sont un casier judiciaire vierge ( $\pm 88\%$ ), le contrôle des antécédents et/ou une attestation de bonne moralité ( $\pm 87\%$ ). Les conditions d'accès au niveau du personnel (personnel opérationnel) sont un casier judiciaire vierge ( $\pm 97\%$ ), le contrôle des antécédents et/ou une attestation de bonne moralité ( $\pm 97\%$ ).

L'âge minimum moyen pour qu'un agent de sécurité privée puisse accéder au secteur de la sécurité privée en tant que responsable est de  $\pm 19$  ans et  $\pm 18$  ans pour y accéder en tant que membre du personnel opérationnel. Tous les pays ont des exigences particulières en ce qui concerne les uniformes et les cartes d'identification du personnel de sécurité privée. Les uniformes sont obligatoires dans  $\pm 95\%$  des pays européens et les cartes d'identification dans plus de  $\pm 98\%$  des pays européens.

*Le secteur de la sécurité privée est réglementé par une législation spécifique au secteur dans 94 % des pays européens. L'autorité nationale compétente chargée d'élaborer et de modifier la législation réglementant le secteur de la sécurité privée est soit le ministère de l'Intérieur ( $\pm 53\%$ ), soit le ministère de la Justice ( $\pm 16\%$ ), soit la police ( $\pm 6\%$ ), soit un autre organisme ( $\pm 25\%$ ).*

(6) En matière de sécurité privée, le « principe de spécialité » signifie qu'une entité juridique unique, officiellement reconnue comme entreprise de sécurité privée, est autorisée à fournir uniquement des services de sécurité privée, la fourniture de tous services auxiliaires ou complémentaires lui étant interdite.

## État de la législation européenne

En ce qui concerne les pouvoirs et compétences des agents de sécurité privée, nous pouvons indiquer que dans  $\pm 59\%$  de l'ensemble des pays européens, les agents de sécurité privée ont les mêmes droits que n'importe quel autre citoyen. Dans  $\pm 41\%$  des cas, ils peuvent exercer des pouvoirs additionnels. Par ailleurs, les agents de sécurité privée sont autorisés à effectuer des fouilles et des saisies (complètes ou limitées) dans  $\pm 56\%$  des pays européens.

L'usage des armes est autorisé dans  $\pm 83\%$  des pays européens. Cependant, dans  $\pm 82\%$  des cas, une licence spécifique est nécessaire aux entreprises de sécurité privée proposant des services armés de sécurité privée. En outre, il existe des obligations légales en matière de stockage des armes en dehors des heures de travail ( $\pm 85\%$ ) et les entreprises doivent également tenir un registre des armes détaillé ( $\pm 92\%$ ). Les agents de sécurité privée sont soumis à l'obligation légale de suivre une formation spécialisée afin de pouvoir porter et utiliser des armes dans  $\pm 96\%$  des pays européens.

Des chiens peuvent être utilisés dans le cadre de la fourniture de services de sécurité privée dans  $\pm 91\%$  des cas. Une licence spéciale est nécessaire pour les entreprises de sécurité privée utilisant des chiens dans le cadre de la fourniture de services de sécurité privée ( $\pm 39\%$ ) et les agents de sécurité privée sont soumis à l'obligation légale de suivre une formation spécialisée afin de pouvoir utiliser des chiens dans le cadre de la fourniture de services de sécurité privée ( $\pm 59\%$ ).

Les agents de sécurité privée sont soumis à l'obligation de suivre une formation de base dans  $\pm 97\%$  des pays européens. Ce programme de formation est imposé par la loi ( $\pm 97\%$ ) et le nombre moyen d'heures de formation est de  $\pm 97$ . Après avoir terminé et réussi leur formation de base, les agents de sécurité privée se voient délivrer un certificat de compétence ( $\pm 87\%$ ). Des formations obligatoires spécialisées sont imposées par la loi aux responsables de sécurité privée, autrement dit au personnel d'encadrement opérationnel influant sur les opérations, dans  $50\%$  des cas. Enfin, il existe des formations de suivi et de perfectionnement dans  $\pm 70\%$  des pays européens.

L'état actuel de la législation européenne reflète le niveau de sévérité des législations nationales en matière de sécurité privée en Europe et fournit une analyse des réponses aux questions posées dans la partie « aspects juridiques » du questionnaire *Facts et Figures 2014*.

Les réponses apportées à un certain nombre de questions posées, autrement dit les réponses relatives aux législations nationales en matière de sécurité privée, ont été utilisées pour noter la sévérité de la législation de chaque pays en matière de sécurité privée. Une valeur numérique a été attribuée à chaque pays sur la base des réponses données. Des points ont été alloués à chaque pays en fonction des réponses données et cette valeur, a par la suite, été calculée à partir du nombre total de points. Six critères de jugement ont été imaginés pour le niveau de sévérité de la législation : très sévère, sévère, moyennement sévère, peu sévère, très peu sévère et nul. Une valeur numérique a ensuite été attribuée à chacun de ces critères, comme le montre le tableau ci-dessous. Les pays pouvaient être classés dans différentes catégories et cette évaluation pouvait ensuite être traduite par un graphique visant à figurer les différents niveaux de sévérité.

Note	Niveau de sévérité
0	Nul
1-5	Très peu sévère
6-13	Peu sévère
14-20	Moyennement sévère
21-27	Sévère
28-34	Très sévère

Les questions utilisées pour attribuer une note avaient trait aux dispositions et aux exigences mentionnées dans les législations nationales. Par exemple, il était fondamental d'établir si le secteur des services de sécurité privée était régi par la loi et le cas échéant, de préciser quels domaines du secteur étaient couverts. Par ailleurs, il était nécessaire de déterminer si des sanctions étaient appliquées et s'il existait des conditions ou des restrictions d'accès.



Peu sévère	Moyennement sévère	Sévère	Très sévère
- Autriche - République tchèque - Pologne	- Irlande - Royaume-Uni - France - Allemagne - Bulgarie - Lettonie - Chypre	- Turquie - Grèce - Macédoine - Roumanie - Bosnie-Herzégovine - Croatie - Slovénie - Slovaquie - Italie - Suisse - Pays-Bas - Estonie - Lituanie - Danemark - Norvège - Finlande - Malte	- Serbie - Hongrie - Belgique - Suède - Portugal - Espagne - Luxembourg

- les entreprises de sécurité privée peuvent-elles ou non fournir des services et exercer des activités qui sont ou qui seraient normalement du ressort des forces de police ou d'autres autorités de sécurité publique ?
- quels sont les services que peuvent fournir les entreprises de sécurité privée ?
- dans quel cadre juridique ces services s'inscrivent-ils (législation générale – législation spécifique – accords *ad hoc* avec la police) ?
- la tendance au transfert (total ou à l'appui des forces de police) des compétences policières aux entreprises de sécurité privée est-elle ou non à la hausse ?
- description de ces tendances ;
- domaines dans lesquels les sondés prévoient que davantage d'activités « publiques » seront confiées aux entreprises de sécurité privée.

## Coopération public-privé dans le secteur européen de la sécurité privée

Cette partie donne un aperçu de la coopération public-privé dans 34 pays européens. Nous présenterons succinctement la méthodologie utilisée. Par la suite, nous dresserons un panorama des données.

Cet aperçu de la coopération public-privé s'appuie sur des informations issues des questionnaires, de documents de la CoESS et d'Internet (informations judiciaires). Nous avons également contacté les pouvoirs publics afin d'obtenir des données supplémentaires. Nous n'avons pas obtenu d'informations de la part des pays suivants : Bosnie-Herzégovine, Bulgarie, Chypre, Croatie, Danemark, France, Hongrie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Portugal, République tchèque, Royaume-Uni, Slovaquie et Suède. Ceci peut être dû à une absence de réponse ou à un manque d'informations dans les questionnaires. Nous avons reçu des informations des pays suivants : Allemagne, Autriche, Belgique, Espagne, Estonie, Finlande, Grèce, Irlande, Italie, Macédoine, Norvège, Pologne, Roumanie, Serbie, Slovénie, Suisse et Turquie. Les informations fournies par les pays suivants étaient incomplètes : Allemagne, Autriche, Estonie, Italie et Macédoine.

Cet aperçu fournit des éléments de réponse aux questions suivantes :

Les entreprises de sécurité privée ne peuvent fournir des services ou exercer des activités qui sont ou qui seraient normalement du ressort des forces de police ou d'autres autorités de sécurité publique en Irlande, en Pologne, en Roumanie, en Serbie, en Slovénie et en Turquie.

Les entreprises de sécurité privée peuvent fournir des services ou exercer des activités qui sont ou qui seraient normalement du ressort des forces de police ou d'autres autorités de sécurité publique en Allemagne, en Autriche, en Belgique, en Espagne, en Estonie, en Italie, en Finlande, en Grèce, en Norvège et en Suisse.

Ces services sont :

- Allemagne : transfert des responsabilités du personnel de sécurité dans le secteur de l'aviation ;
- Belgique : soutien des forces de police, déclarations relatives à l'état directement observable des biens du domaine public dans le cadre d'une mission confiée par les pouvoirs publics ou le concessionnaire, accompagnement de groupes de personnes avec pour objectif d'assurer la sécurité routière, accompagnement de convois exceptionnels avec pour objectif d'assurer la sécurité routière ;
- Espagne : services dans les prisons, centres de détention à l'étranger, locaux publics et « participation à la fourniture de services de sécurité publique, à titre complémentaire des activités policières ». Néanmoins, ces services doivent encore être développés et fournis à l'appui des forces de police.

Ces indications sont fondées sur les législations suivantes :

Cadre juridique pour les entreprises de sécurité privée pouvant fournir des services et exercer des activités qui sont ou qui seraient normalement du ressort des forces de police ou d'autres autorités de sécurité publique	
Législation générale	Belgique, Espagne (Loi 5/2014)
Législation spécifique	Allemagne, Finlande (Loi sur l'ordre public 612/2003), Suisse
Accords <i>ad hoc</i> avec la police	Grèce, Italie, Norvège

- Estonie : gestion des radars (les images sont directement transmises aux autorités policières moyennant une somme forfaitaire par image) ;
- Finlande : investigations ; un service d'ordre (ainsi qu'une formation des agents) aide la police à maintenir l'ordre public et la sécurité dans certains lieux tels que les centres commerciaux (loi sur l'ordre public) ;
- Grèce : services de surveillance dans les ambassades et à l'occasion de manifestations sportives ;
- Norvège : services spéciaux, surveillance d'ambassades. Néanmoins, ces activités doivent systématiquement être validées par la police ;
- Suisse : transport de prisonniers, services carcéraux, sécurité ferroviaire, services de migration.

En Macédoine, le ministère de l'Intérieur a créé un service distinct qui travaille exclusivement avec le secteur de la sécurité privée. Ce service organise des séminaires et des ateliers portant sur la mise en œuvre de la nouvelle loi.

La tendance au transfert (total ou à l'appui des forces de police) des compétences policières aux entreprises de sécurité privée est à la hausse en :

- Suisse : délégation des activités qui ne relèvent pas des compétences de base des services de police, telles que le contrôle du stationnement ou la sécurité ferroviaire ;
- Grèce : services de surveillance dans les ambassades ou à l'occasion de manifestations sportives ;

La tendance au transfert (total ou à l'appui des forces de police) des compétences policières aux entreprises de sécurité privée n'est pas à la hausse en Finlande et en Norvège.

Les pays suivants prévoient que davantage d'activités « publiques » seront confiées aux entreprises de sécurité privée :

- Grèce : services de surveillance dans les ambassades ou à l'occasion de manifestations sportives ;

- Suisse : services de sécurité routière, services carcéraux, service de patrouille et de surveillance des parkings.

## Lutte contre la piraterie en haute mer – sécurité maritime

Cette partie donne un aperçu de la sécurité maritime dans les 34 pays européens susmentionnés. Nous présentons brièvement la méthodologie utilisée. Par la suite, nous dresserons un panorama de la sécurité maritime. Nous n'avons pas d'informations relatives à la sécurité maritime pour les pays suivants : Autriche, Bosnie-Herzégovine, Bulgarie, Croatie, Hongrie, Lettonie, Luxembourg, Macédoine, République tchèque, Roumanie, Slovaquie et Suède. Ceci peut-être dû à une absence de réponse ou à un manque d'informations dans les questionnaires.

Les pays suivants nous ont fourni des informations incomplètes : Chypre, Danemark, Italie, Lituanie, Malte, Norvège, Portugal et Royaume-Uni. Cela signifie que nous ne sommes pas en mesure de fournir des informations pour toutes les sections de cet aperçu.

Cet aperçu fournit des éléments de réponse aux questions suivantes :

- les entreprises de sécurité privée peuvent-elles ou non fournir des services et exercer des activités visant à lutter contre les actes de piraterie commis à l'encontre des vaisseaux commerciaux ?
- législation ;
- les entreprises doivent-elles être en possession d'une licence spécifique ?
- formation ;
- usage des armes.

Les entreprises de sécurité privées ne peuvent pas fournir des services et exercer des activités visant à lutter contre les actes de piraterie commis à l'encontre des vaisseaux

Ces indications sont fondées sur les législations suivantes :

Législation relative aux entreprises de sécurité privée pouvant fournir des services et exercer des activités visant à lutter contre les actes de piraterie commis à l'encontre des vaisseaux commerciaux battant pavillon de leurs pays respectifs	
Allemagne	§ 31 Abs. 1 GewO
Belgique	Loi du 16 janvier 2013 concernant les différentes mesures de lutte contre la piraterie
Chypre	Loi de 2012 relative à la protection des vaisseaux chypriotes contre les actes de piraterie et autres actes illégaux (Loi 77(I)/2012)
Danemark	De nouvelles règles sont entrées en vigueur le 1 <sup>er</sup> juillet 2012
Espagne	Loi sur la sécurité privée
Finlande	Loi sur la sécurité privée 282/2002
Grèce	Loi 4058 du 22 mars 2012
Italie	- Décret n° 266 du ministère des Affaires intérieures (28 décembre 2012) - Décret n° 349/2013
Malte	- Obligation de conformité avec l'avis juridique 19 de 2013 - Merchant Shipping Notice 106
Norvège	Forskrift om sikkerhet, pirat- og terrorberedskapsiltak og bruk av maktmidler om bord på skip og flyttbare boreinnretninger (Sikkerhetsforskriften)
Pays-Bas	Pas de cadre juridique pour l'instant. Depuis juin 2011, un armateur peut demander l'aide d'un détachement de protection des navires (équipe militaire)
Pologne	Le recours au PAASP est approuvé par la loi polonaise. Le principal cadre juridique est apporté par la loi relative à la protection des personnes et des biens du 22 août 1997
Royaume-Uni	Sans objet

commerciaux battant pavillon de leurs pays respectifs en Estonie, en France (pas d'autorisation administrative), en Irlande, en Lituanie, au Portugal, en Serbie, en Slovénie, en Suisse et en Turquie.

Les entreprises de sécurité privées peuvent fournir des services et exercer des activités visant à lutter contre les actes de piraterie commis à l'encontre des vaisseaux commerciaux battant pavillon de leurs pays respectifs en Allemagne, en Belgique, à Chypre, au Danemark, en Espagne, en Finlande, en Italie, à Malte, en Norvège, aux Pays-Bas, au Portugal et au Royaume-Uni.

Les entreprises de sécurité privée exerçant ce type d'activités doivent être en possession d'une licence générale ou spécifique en Allemagne, en Belgique, à Chypre, en Grèce, à Malte, en Norvège et au Royaume-Uni.

Nombre d'entreprises détenant une telle licence :

- en Allemagne : sept entreprises sont en possession d'une licence BAFA (BAFA = Office fédéral de l'économie et du contrôle des exportations) ;

- en Belgique : une entreprise de sécurité privée nationale et une entreprise de sécurité privée étrangère détiennent une licence provisoire (valable une année pour la seconde).

Les entreprises de sécurité privée qui exercent ce type d'activité n'ont pas besoin de licence générale ou spécifique en Espagne et en Finlande.

Une formation spéciale pour les agents et les officiers de sécurité fournissant des services ou exerçant des activités visant à lutter contre les actes de piraterie commis à l'encontre des vaisseaux commerciaux battant pavillon de leurs pays respectifs existe en Allemagne, en Belgique (formation de base de 127 heures et formation spécialisée de 40 heures), en Espagne, en Italie, à Malte et au Royaume-Uni.

Une formation spéciale pour les agents et les officiers de sécurité fournissant des services ou exerçant des activités visant à lutter contre les actes de piraterie commis à l'encontre des vaisseaux commerciaux battant pavillon de leurs pays respectifs n'existe pas en Finlande.

Les agents et les officiers de sécurité privée peuvent utiliser des armes à bord dans les pays suivants : Allemagne, Belgique, Danemark, Espagne, Finlande (bien que la législation en la matière ne soit pas claire à 100 %), Grèce, Italie, Malte, Norvège, Pays-Bas et Royaume-Uni.

Types d'armes utilisées :

- Allemagne : toutes les armes sont autorisées à bord, à l'exception des armes militaires ;
- Belgique : armes de calibre 0,50 maximum ;
- Espagne : armes de guerre ;
- Finlande : pistolets ;
- Italie : munitions « explosives » de la classe 1,4s du code IMDG ;
- Norvège : armes légères ;
- Pays-Bas : pistolets et fusils semi-automatiques.

Les agents et les officiers de sécurité privée ne peuvent utiliser d'armes à bord dans les pays suivants : Pologne (pas de fondement juridique).

## Vision future et changement de paradigme en matière de sécurité privée

Comme nous l'avons mentionné ci-dessus, nous devons sans cesse investir dans les résultats quantitatifs du secteur européen de la sécurité privée. L'une des conclusions les plus importantes est que, malgré les difficultés économiques auxquelles nous sommes confrontés en Europe, le secteur de la sécurité privée reste florissant. Si l'on compare les dernières données à celles figurant dans *Facts et Figures*, édition 2011, nous pouvons conclure que le nombre d'entreprises de sécurité privée augmente en Allemagne, en Autriche, en Croatie, en Estonie, en Finlande, en France, aux Pays-Bas, en Roumanie, en Serbie, en Slovénie, en Suisse et en Turquie. Au contraire, leur nombre diminue en Belgique, en Espagne, en Grèce, en Hongrie, en Irlande, en Macédoine, en Norvège et en Pologne.

Le nombre d'agents de sécurité privée augmente en Allemagne, en Autriche, en Belgique, en Croatie, en Espagne, en Estonie, en Finlande, en Grèce, en Norvège, en Pologne, en Roumanie, en Slovénie et en Turquie. Au contraire, leur nombre diminue en Hongrie, en Italie, en Macédoine, aux Pays-Bas, en Serbie et en Suisse. Le taux annuel de rotation du personnel dans le secteur de la sécurité privée augmente en Allemagne, en Autriche, en Belgique, en Croatie, en Espagne, en Finlande, en France, en Grèce, en Norvège, en Pologne, en Suède, en Suisse et en

Turquie et diminue en Irlande, aux Pays-Bas, en Roumanie et en Serbie. Les résultats ne sont pas concluants pour la Bosnie-Herzégovine, la Bulgarie, Chypre, le Danemark, la Lettonie, la Lituanie, le Luxembourg, Malte, le Portugal, le Royaume-Uni et la Slovaquie.

Ce point de vue permet de dégager une vision future des moteurs et des obstacles d'une approche intégrée de la surveillance et de la sécurité des technologies. Le

*Le secteur de la sécurité subit actuellement un changement de paradigme progressif sans précédent. Le marché de la surveillance traditionnel et sa dynamique actuelle appellent à l'accélération de l'intégration des services de surveillance à distance et mobiles à la surveillance traditionnelle sur site, avec l'appui des solutions technologiques et électroniques*

secteur de la sécurité subit actuellement un changement de paradigme progressif sans précédent. Le marché de la surveillance traditionnel et sa dynamique actuelle appellent à l'accélération de l'intégration des services de surveillance à distance et mobiles à la surveillance traditionnelle sur site, avec l'appui des solutions technologiques et électroniques (vidéosurveillance, systèmes de contrôle des accès et systèmes complètement informatisés). Ces tendances vont sans nul doute continuer à dominer l'avenir des activités de sécurité. Par conséquent, de nombreux défis doivent être relevés afin de rencontrer le succès escompté dans les prochaines années.

Un phénomène pénètre le secteur de la sécurité : l'approche marketing du « regroupement », qui associe les différents produits et services dans une proposition unique. Cependant, beaucoup de clients continuent de prendre des décisions distinctes en ce qui concerne leurs achats de services humains et de systèmes de sécurité électroniques. Les réticences des clients à acheter des contrats de services regroupés sont peut-être dues au fait qu'ils perçoivent, à tort ou à raison, qu'ils n'ont plus le contrôle de ces services. Les clients peuvent également avoir le sentiment qu'avoir affaire à un fournisseur unique est plus risqué.

Une forte évolution positive en faveur du développement de cette approche combinée est néanmoins visible. Cette tendance, très probablement irréversible, est étayée par une multitude de facteurs. Tout d'abord, il existe des considérations économiques et opérationnelles globales. L'externalisation combinée devrait permettre de réduire le chevauchement des différents niveaux de gestion. Elle doit permettre de normaliser et de simplifier les opérations et les processus. Qui plus est, elle devrait accélérer les processus d'achat et de passation des contrats, atténuer le risque grâce à un nombre limité de points de contact et simplifier l'ensemble du processus de gestion. Le regroupement devrait également permettre des économies de coûts et une souplesse financière.

Parallèlement à cet argument, nous pouvons mettre en évidence les moteurs responsables du succès ou de l'échec de l'approche combinée en matière de sécurité. Nous avons ainsi identifié les facteurs clients, la réglementation, les avancées technologiques, la réduction des coûts et les efforts déployés en faveur de l'efficacité, la démographie, l'évolution de la main-d'œuvre, les exigences en matière de formation et d'éducation ainsi que les relations sociales en général.

Un certain nombre de facteurs clients jouent un rôle déterminant. D'une manière générale, et même si ce n'est pas toujours le cas, les entreprises les plus grandes et les plus complexes ont tendance à se montrer plus ouvertes

aux propositions intégrées, surtout si elles ont adopté une politique d'achats centralisée. À cet égard, il faut également tenir compte du fait qu'un client se focalise plutôt sur les transactions ou plutôt sur les relations. Dans une certaine mesure, cela peut avoir un lien avec la culture locale, dans laquelle entretenir de bonnes relations peut être perçu comme ayant tendance à favoriser les affaires. Au contraire, certaines entreprises font le choix stratégique délibéré de faire tourner leurs équipes (d'achats) afin de ne pas laisser se développer de relations durables. Il est souvent avancé que les services combinés ont de meilleures chances d'être introduits dans des entreprises ayant une culture plus axée sur les relations. Une solide relation avec la direction contribue à mettre sur pied une « coalition dominante » en faveur d'une évolution vers des projets regroupés. Les organisations familières de l'intégration technologique et qui favorisent les flux d'informations continus préféreront souvent les offres intégrées, puisque ces concepts font déjà partie de leurs activités de base quotidiennes. Elles auront le recul nécessaire pour comprendre et évaluer les avantages que présente une approche intégrée en matière de sécurité. Ce type de clients fait généralement partie de ceux qui aiment se mettre en quête d'éléments innovants et qui ne cessent de chercher à obtenir des solutions de sécurité optimisées et innovantes.

Dans un environnement réglementé, la forte exigence de conformité peut favoriser le regroupement. Les activités de sécurité, comme nous l'avons décrit, sont extrêmement réglementées et l'opposition dialectique qui existe entre sécurité et vie privée est susceptible de conduire à des évolutions dans le domaine de ce qui est toléré par la loi et dans celui des zones d'opération acceptées. Une approche conceptuelle peut soulager (en partie) le client du poids de cette mise en œuvre et intégrer ces aspects à une gouvernance entièrement externalisée.

Les avancées apportées par l'évolution technologique font partie des principaux moteurs du processus d'intégration. Ainsi, nous avons constaté que les services de surveillance sur le terrain (fournis au moyen de dispositifs portatifs et de tablettes) et les opérations dans les salles de contrôle sont de plus en plus souvent complétés par des outils offrant un support technique, une visualisation sur écran d'instructions, de procédures, de plans, etc., ainsi que des comptes rendus en temps réel destinés à la fois à l'organisation interne et au client.

Les produits électroniques traditionnels tels que les dispositifs permettant la détection des intrusions, le contrôle des accès, la détection des incendies et la vidéosurveillance sont généralement rattachés à un tableau de bord et à une source d'énergie et connectés par des kilomètres de câbles propriétaires à des points

d'accès physiques comme les portes. Ces installations sont lentement mais sûrement remplacées par des systèmes logiciels de gestion sur IP de l'identité qui se connectent à des caméras, des portails et des interphones IP situés sur les points d'accès physiques. De la même façon, ces différentes applications finiront par être davantage intégrées aux mêmes plateformes, ou au minimum, devront être capables de communiquer les unes avec les autres. Dans le domaine de la vidéosurveillance en particulier, de très nombreuses innovations intéressantes, encore considérées comme futuristes il y a quelque temps, deviennent aujourd'hui réalité. Il en va ainsi de la criminalistique en temps réel, qui permet d'exploiter des vidéos déjà enregistrées pour analyser une image et obtenir un retour en quelques secondes. Ainsi, en tenant compte d'un certain nombre de caractéristiques, un intrus déjà identifié une fois peut être automatiquement reconnu et suivi en temps réel tout au long de son parcours dans un bâtiment.

Le rapport coût-efficacité apparaîtra lui aussi souvent comme un moteur. En Europe et en Amérique du Nord, où la croissance économique actuelle est faible, les stratégies et les programmes de gestion des coûts mettent l'accent sur la nécessité d'une meilleure efficacité, d'un meilleur équilibre coûts/résultats ou, tout simplement, d'une meilleure sécurité à moindre coût. Le rendement le plus important, le meilleur retour sur investissement, devrait être obtenu grâce aux économies permises par le processus de production et de livraison intégré ainsi qu'à une productivité plus efficace.

Des avantages supplémentaires peuvent même être obtenus en cas de croisement des opérations de sécurité et des opérations commerciales. Les avancées en matière d'analyse de vidéos et d'intégration des systèmes ont transformé la technologie de sécurité en un outil offrant un aperçu des activités commerciales. Par exemple, l'analyse d'images visant à détecter les attroupements peut également être utilisée comme un outil marketing en générant des cartes thermiques figurant les endroits où les gens se rassemblent et effectuent des achats à différents moments de différents jours. Grâce à ces informations, les organisations peuvent améliorer la présentation des magasins et les campagnes marketing et même optimiser les décisions relatives à la planification des horaires des employés. Certains aspects d'une stratégie de gestion des coûts peuvent également être liés aux politiques de

réduction des risques. Les organisations percevant un risque élevé en termes d'informatique ou de complexité sécuritaire et n'ayant pas ou ne souhaitant pas avoir les ressources compétentes, peuvent avoir tendance à favoriser les services regroupés.

La récente crise a durement touché nos économies. Nous nous dirigeons vers de nouveaux équilibres économiques et il est très improbable que nous retrouvions un jour la croissance que nous avons connue préalablement à la récession de 2008. Dans le contexte de ces nouvelles réalités économiques, l'emploi fait partie des nombreux nouveaux défis. Dans l'ancien modèle, le dynamisme d'une économie, que traduisaient les chiffres de la croissance, conduisait généralement à la création d'emplois. La situation observée au cours des deux dernières années a montré une croissance économique en légère augmentation, associée à une reprise de l'emploi plus ou moins paralysée (un phénomène également décrit sous le nom de « croissance sans emploi »). Et en dépit de taux de chômage actuels relativement élevés, il est à prévoir qu'il y aura pendant quelque temps encore une pénurie croissante de main-d'œuvre professionnelle et qualifiée dans différents secteurs de nombreux marchés locaux. Le secteur de la sécurité ne sera pas épargné.

*Sur un marché du travail insuffisant, il ne sera pas simple d'attirer les jeunes générations dans le secteur de la sécurité et de les y retenir. En raison de l'image vieillotte traditionnellement associée au secteur de la surveillance, celui-ci a souvent été perçu comme un environnement de travail peu attirant.*

Par ailleurs, la nature du travail évoluera quant à elle encore plus rapidement d'une décennie sur l'autre; certains emplois disparaîtront même pour être remplacés par d'autres, entièrement nouveaux. Le vieillissement de la main-d'œuvre représente lui aussi un autre phénomène global à l'échelle de l'Europe. Tous les secteurs sont confrontés au risque potentiel de voir un nombre considérable de leurs employés quitter le marché du travail dans les quelques années à venir, les enfants du baby-boom atteignant l'âge traditionnel de la retraite, sans qu'ils soient pour autant complètement remplacés par les nouvelles générations arrivant sur le marché. Il convient donc d'explorer d'autres solutions. Ainsi, l'un des défis pourrait être de promouvoir l'allongement du temps de travail des employés actuels et le recrutement de travailleurs seniors. Mais des mesures actives devraient également être prises afin de favoriser l'employabilité, la mobilité professionnelle, les opportunités de formation continue et autres points d'intérêt; en outre, des efforts devraient être déployés pour que les agents de sécurité les plus âgés restent plus longtemps en poste.

Sur un marché du travail insuffisant, il ne sera pas simple d'attirer les jeunes générations dans le secteur de la sécurité et de les y retenir. En raison de l'image vieillotte traditionnellement associée au secteur de la surveillance, celui-ci a souvent été perçu comme un environnement de travail peu attirant. Cependant, ces dernières années, un certain nombre de campagnes ont été lancées afin de redorer l'image de l'agent de sécurité. Les jeunes agents qui arrivent dans le métier – des hommes, mais aussi des femmes, assurément – ont une vision précise et différente de l'endroit où se situent les limites de leur flexibilité. Attirer davantage de personnel féminin représente un défi considérable, mais aussi une opportunité. Par ailleurs, la nécessité d'avoir du personnel maîtrisant correctement la langue locale et ayant une bonne compréhension et une bonne connaissance de la culture et de la législation locales rend difficile, au moins sur le court terme et sans mesures décentes d'intégration, de recruter des agents de sécurité potentiels issus de cultures et de régions éloignées. Dans le domaine de la sécurité électronique, la situation est dans l'ensemble très similaire, même si le contexte sous-jacent est parfois différent. La disponibilité d'une main-d'œuvre technique qualifiée pose problème depuis un certain temps en raison de la pénurie globale de profils techniques par rapport à la demande croissante du marché pour ce type de personnel technique spécialisé.

Les générations actuelles et futures d'agents de sécurité devront être plus compétentes à divers niveaux d'aptitudes et de savoir-faire. De nouveaux besoins éducatifs et de nouvelles exigences, différents et en constante évolution, voient le jour. La formation relative aux obligations légales et à la connaissance des règles et règlements demeurera essentielle et pourrait même être intensifiée dans un monde où la criminalité demeure un sujet de préoccupation majeur pour les citoyens et les entreprises et où le secteur de la sécurité privée sera amené à jouer un rôle de plus en plus important auprès des autorités policières, en remplissant un devoir sociétal de prévention du crime et de protection dans les situations de crise.

Mais aujourd'hui, les clients attendent bien davantage du personnel de sécurité, comme des compétences en matière de gestion des conflits ou des compétences linguistiques dans un environnement de plus en plus international et multiculturel. Au contraire, ces exigences ne sont pas aussi évidentes pour bon nombre d'agents plus âgés qui souhaitent rester en poste. Actuellement, nombre d'entre eux peinent malheureusement à acquérir les compétences informatiques liées à l'évolution des exigences.

Dans les centres de réception d'alertes et les salles de vidéosurveillance, le niveau technique et informatique des opérateurs doit être conforme aux spécifications des

solutions technologiques installées et connectées. En outre, que ce soit dans les locaux des clients ou dans le cadre d'opérations mobiles, les agents de sécurité devront se familiariser avec – et rester familiers de – l'utilisation des plateformes de sécurité électroniques qu'ils sont amenés à faire fonctionner dans les centres de contrôle locaux, ainsi qu'avec l'utilisation d'ordinateurs de poche (PDA), de tablettes ou d'autres dispositifs employés dans l'approche processus professionnalisée des activités de surveillance telles que décrites précédemment. L'éducation devra impérativement continuer de figurer au centre des préoccupations dans un monde qui évolue rapidement. L'évolution des connaissances, afin de suivre le rythme des évolutions dans les domaines de l'informatique, des systèmes de gestion de l'information en matière de sécurité physique et des *big data*, devra elle aussi faire l'objet d'une attention particulière.

Dans un environnement foisonnant ainsi de brillantes évolutions, les relations avec les partenaires sociaux devront elles aussi revêtir une structure et un contenu différents. Nous observons, plus que jamais auparavant, bien plus de différences en termes d'âges, de compétences, de besoins opérationnels, d'exigences et de désirs personnels dans les constellations de travail « partagé ». Dans un environnement de travail plus complexe, il conviendra sans doute de mettre plus particulièrement l'accent sur les opportunités futures. Aujourd'hui, nous vivons dans un monde où les talents individuels seront le facteur déterminant des attentes futures, au détriment de critères généralisés appliqués à des groupes classifiés selon de vieilles formules qui, de plus en plus, cesseront d'exister. Dans ce cas, le dialogue social et le débat modernes ne devraient-ils pas être revisités de concert par les syndicats et les employeurs, et évoluer progressivement dans le contexte d'une main-d'œuvre changeante et plus complexe ? Ne faudrait-il pas se concentrer davantage sur la gestion des carrières et les changements d'emploi associés à un niveau nécessaire de protection de l'emploi ? Sur la formation et le développement ? Et du point de vue philosophique, sur les opportunités futures plutôt que sur les vieux modèles ?

## La nouvelle entreprise de sécurité

Il est évident que de nombreuses questions déterminantes se posent quant au développement et à la mise en œuvre d'une stratégie de regroupement qui finira par porter ses fruits. Dans la mesure où une offre combinée en matière de sécurité implique l'intégration d'une gamme de services et de produits, elle exacerbe la complexité et l'importance de la résolution de ces questions et difficultés en vue de

glaner les profits potentiels. Une stratégie qui semble simple et gagnante, si elle n'est pas gérée correctement, pourrait avoir des conséquences désastreuses sur le résultat financier et économique d'une entreprise.

Les services de sécurité intégrés peuvent être fournis en associant des produits de différentes organisations réunissant leurs compétences au nom d'un projet donné. Dans ce cas, à quoi la nouvelle entreprise devrait-elle ressembler ? Si l'objectif est de proposer une offre de concepts complets, l'entreprise devrait être en mesure de réunir un certain nombre de compétences et de transformer une organisation en vase clos en une organisation collaborative. En effet, de très nombreux processus de gestion des flux de services et des installations autonomes du point de vue opérationnel doivent aboutir directement à une solution de sécurité.

Cette mécanique complexe devrait non seulement fonctionner lors de la phase d'exécution d'un contrat, mais le prestataire de sécurité devrait en outre être capable de démontrer en amont les avantages escomptés à son client, lors des phases de prospection et de vente. Cela nécessite une stratégie marketing et commerciale convaincante et convenablement élaborée. Un intégrateur performant devra être capable de comprendre et de présenter professionnellement la sécurité physique et électronique, en mettant sur la table sa solide connaissance de l'informatique et des réseaux.

Plusieurs obstacles devront être surmontés lors du processus de préparation et de mise en œuvre de ce type de projets de sécurité. Des obstacles ou des barrières en termes de communication interne – ainsi que des seuils hiérarchiques – placés entre les éléments constitutifs de l'approche intégrée, doivent être franchis. Il faudra également s'attaquer aux conséquences cannibaliques. En effet, la technologie remplacera bien souvent, par exemple, un certain nombre d'activités humaines de base. La clé du succès réside dans l'intégration réussie de produits et de plateformes technologiques, tout en maintenant la capacité toujours nécessaire des agents à interpréter les informations et y réagir au sein d'une constellation parfaitement complémentaire. C'est là que se trouve la véritable valeur ajoutée opérationnelle.

Une organisation devrait également pouvoir s'appuyer sur un nombre approprié de ressources humaines ayant un niveau de qualification suffisant afin d'être en mesure de mettre en œuvre des concepts de sécurité complets, performants et harmonieux. Accessoirement, la situation de bon nombre d'entre elles, qui continuent à privilégier une approche en vase clos en matière d'offres de sécurité électronique ou de surveillance, est tout aussi critique.

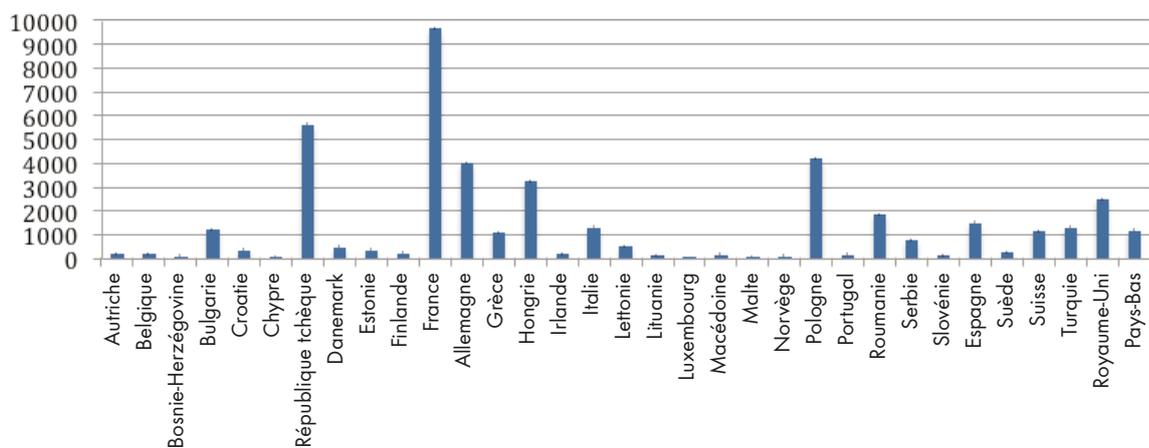
La nouvelle entreprise de sécurité sera quoi qu'il en soit capable de faire face à l'évolution sociodémographique des places de marché actuelles et futures dans une nouvelle dynamique économique. Cela entraîne des difficultés en termes de ressources humaines, difficultés qui sont d'une nature différente de celles rencontrées il y a quelques années. La nouvelle approche doit considérer les talents comme des ressources rares et précieuses, éduquées et formées à différents niveaux de la population active, et une importance croissante doit être accordée aux approches personnalisées ou différenciées afin de satisfaire simultanément ces tranches d'âge et ces générations différentes.

En raison de la complexité que présente le pilotage de différentes cultures d'installation et de service, si l'on souhaite proposer une offre combinant la surveillance et l'électronique et s'inscrivant dans cette vision de la sécurité sans cesse réinventée du point de vue technologique, de nouveaux besoins organisationnels et de nouveaux besoins en matière de compétences apparaissent, ainsi que nous l'avons expliqué précédemment. Et il s'agit plutôt de nécessités fondamentales que de différentiateurs très recherchés.

Par conséquent, la cohérence de la stratégie est plus que jamais essentielle. Opter pour un processus particulier ne signifie pas simplement privilégier les éléments qui constituent ses points forts. Diverses variables influent sur le succès potentiel d'une approche intégrée. Si les zones les plus risquées ne sont pas solidement gérées et qu'en raison de cela, les « lacunes » deviennent trop importantes, celles-ci auront sans doute une incidence dramatique sur l'efficacité de la performance et au final, influenceront de manière négative sur le rendement et les résultats finaux – du point de vue opérationnel et financier.

Il apparaît clairement que la tendance à l'externalisation de la sécurité dans le cadre d'une approche de concepts complets gagne de plus en plus de terrain ; cela peut être dû au fait que les clients qui en perçoivent les avantages sont plus nombreux qu'avant, ou au fait qu'il pourrait s'agir d'une nouvelle évolution cyclique causée par la priorité accordée aux coûts. La vitesse des évolutions et avancées technologiques, alimentée par la créativité sans borne des ingénieurs de développement, est vouée à se maintenir. Ainsi, opter pour la voie du « SAAS » – la sécurité en tant que service d'éléments intégrés – implique de se tenir sans cesse au courant de ces vagues de renouveau. Et comprendre les besoins de plus en plus tranchés et complexes des clients sera essentiel dans le processus visant à déterminer les bons choix stratégiques ■

## Annexe : nombre d'entreprises de sécurité en Europe



Nombre total : ± 41 300

Données manquantes : Slovaquie



## La machine de guerre économique américaine

Ali LAÏDI

Ali LAÏDI



Docteur en sciences politiques et chercheur à l'Institut de relations internationales et stratégiques (IRIS). Il suit les questions de

guerre économique depuis 1997. Il intervient depuis de nombreuses années à l'Institut national des hautes études de la sécurité et de la justice (Inhesj). Auteur de plusieurs ouvrages : *Le Jihad en Europe*, Seuil, 2002 ; *Les secrets de la guerre économique*, Seuil, 2004 ; *Retour de flamme. Comment la mondialisation a accouché du terrorisme*, Calmann-Lévy, 2006 ; *Les États en guerre économique*, Seuil, 2010, Prix Turgot IES 2010 ; *Aux sources de la guerre économique*, Armand Colin, 2012.

Le monde post-guerre froide est celui de l'hyper-compétition économique. Les vents féroces de la concurrence soufflent si puissamment qu'ils ravagent en un clin d'œil les positions acquises. « Dans l'hypercompétition [...] c'est souvent en attaquant qu'on se défend le mieux<sup>1</sup> ». Dans son livre « Hypercompétition » publié en 1994, le professeur Richard d'Aveni use de termes particulièrement guerriers pour

décrire les relations économiques mondiales. Il parle d'entreprises qui détruisent, neutralisent ou réduisent à l'obsolescence les avantages concurrentiels de leurs rivales. Il préconise des stratégies de destruction « créative » de l'avantage de l'adversaire. Il explique comment « semer la perturbation ». Le temps du doux commerce est, selon lui, totalement révolu. « Avec l'intensification de la concurrence, les entreprises ne peuvent plus s'offrir le luxe de respecter les traditions d'élégance du passé. La chevalerie est morte<sup>2</sup> ».

À la fin du siècle dernier, l'Amérique mesure parfaitement les enjeux de ce nouveau

(1) D'Aveni (R.), 1995, « Hypercompétition », Paris, Vuibert, p. 10.

(2) D'Aveni (R.), 1995, *idem*, p. 38.

front économique. Débarrassé de l'ennemi soviétique, Washington déclare que sa priorité absolue est la défense de ses intérêts économiques. Initiée par le président Bush père, la politique nationale d'intelligence économique est poursuivie et consolidée par son successeur démocrate Bill Clinton. À partir de 1993, le président reformate son administration pour la mettre en ordre de bataille. Du département du Commerce aux agences de sécurité et de renseignements, tous les fonctionnaires sont mobilisés pour affronter cette guerre économique. Les présidents G. W. Bush et Barack Obama confirment et même renforcent cette stratégie de leadership économique mondial, faisant de leur pays un des grands guerriers économiques de la mondialisation.

## Le réveil américain

Après la chute du mur de Berlin, les Américains ont le sentiment d'avoir accompli leur mission : éradiquer la menace communiste. Toutefois, un dernier job les attend avant d'asseoir leur domination sur le monde : expulser l'armée de Saddam Hussein du Koweït. La démonstration de force qu'ils réalisent dans le Golfe hisse les États-Unis au statut d'Hyperpuissance<sup>3</sup>. En 1991, l'Union soviétique disparaît et l'Irak rentre dans le rang. Plus rien ne s'oppose à l'Empire américain. Washington réoriente ses priorités nationales sur la défense des intérêts économiques de la nation. Les Américains ont le sentiment de les avoir délaissés. Au point d'être moqués. Ne dit-on pas au tournant des années 1990 que les vrais vainqueurs de la guerre froide ne sont pas les États-Unis, mais l'Allemagne et surtout le Japon, deux pays dont les économies se portent très bien à l'époque. Ce qui n'est pas le cas de l'économie américaine. Les États-Unis ne sont plus le phare de l'économie mondiale. À l'époque, le monde des affaires a les yeux rivés sur Berlin et surtout Tokyo. Ce sont eux les modèles à suivre, pas l'Amérique ; deux pays vaincus quarante ans plus tôt par les GI's ! Les multinationales allemandes et japonaises brillent de mille feux ; partout dans le monde on cherche à copier leurs techniques de management pour se hisser au plus haut niveau de la compétition mondiale. Or, au début des années 1990, les États-Unis sont à la traîne : géant politique et surtout militaire, Washington est à la peine

dans le domaine économique. Pas pour longtemps, car l'Amérique se réveille. Le danger communiste étant définitivement écarté, les États-Unis ont les mains libres pour reprendre le leadership économique mondial. Désormais, ils considèrent que tous ses amis d'hier et d'aujourd'hui doivent être traités comme des adversaires commerciaux. Plus question de prendre des pincettes : dans le monde des affaires, chacun joue sa partition et tant pis si certains ne suivent pas ou si d'autres profitent de leur force pour accumuler des parts de marché.

Le président Bush père, sorti vainqueur de la première guerre du Golfe, lance l'offensive. Ancien dirigeant de la CIA, il connaît la valeur de l'information et il sait que les concurrents de l'Amérique veulent piller sa technologie. Il renforce le rôle des services de renseignement au sein de l'Information Security Oversight Office (ISOO) créé en 1978 par le Président Jimmy Carter. Parmi ses missions, l'ISOO est chargée de « soutenir le Président et son gouvernement » dans leur mission de défense du savoir et du savoir-faire des entreprises américaines<sup>4</sup>. Dans la foulée, le président Bush sensibilise son administration et la communauté scientifique américaine à la nécessité de protéger les informations vitales pour la sécurité économique du pays. À cette occasion, il crée le National Industry Security Program (NISIP) le 6 janvier 1993, soit quelques jours avant de céder son poste à la Maison-Blanche au Président démocrate Bill Clinton, nouvellement élu. Le NISIP est le gardien des renseignements classifiés fournis aux organismes et entreprises avec lesquels les administrations sont en relations<sup>5</sup>.

Depuis les années 1970, l'information occupe une place importante dans la relation public-privé. Des chercheurs travaillent sur son rôle dans les stratégies concurrentielles des entreprises. Les résultats de leurs travaux font de l'information, de son recueil et de son analyse, l'une des conditions primordiales du succès commercial<sup>6</sup>. Souvent cité comme ouvrage pionnier, le livre d'Harold Wilensky fait référence dans ce domaine<sup>7</sup>. Pour Wilensky, les deux mamelles de la croissance économique d'un État reposent sur la coopération entre son administration et les entreprises et la capacité des acteurs qu'ils soient étatiques ou privés à recueillir l'information, l'analyser et la transformer en connaissance dans le but de préserver un avantage concurrentiel.

(3) Expression forgée par Hubert Védrine, ancien ministre français des Affaires étrangères.

(4) <http://www.archives.gov/isoo/about/>. Consulté le 23 juin 2015.

(5) <http://www.archives.gov/isoo/policy-documents/eo-12829.html>. Consulté le 23 juin 2015.

(6) Voir Keegan (W.J.), 1974, «Multinational scanning: a study of information sources utilized by headquarters executives», *Administrative Science Quarterly*, septembre, p. 411-421 ; Fahey (L.), King (W.R.), 1977, «Environmental scanning for corporate planning», *Business Horizons*, août, p. 61-71 ; Allen (T.), 1977, «Managing the flow of technology», Cambridge, MIT press.

(7) Wilensky (H.L.), 1967, *Organizational intelligence, knowledge and policy in government and industry*, New York, Basic Books.

C'est dans ce nouveau contexte économique international que le démocrate Bill Clinton, arrive à la Maison-Blanche en 1993. Il poursuit et même renforce la stratégie de défense économique initiée par son prédécesseur républicain. Pour lui, il est clair que la compétition économique mondiale remplace la guerre froide. Son secrétaire d'État Warren Christopher le déclare officiellement le 13 janvier 1993 devant le Congrès. « *La sécurité économique américaine doit être élevée au rang de première priorité de la politique étrangère américaine [...] Il faut promouvoir la sécurité économique américaine en lui accordant autant d'énergie et de ressources qu'il en fallut pour la guerre froide.* » L'Amérique entre en guerre économique. Et son objectif est évidemment de remporter ce nouveau conflit. Pour Warren Christopher, la sécurité nationale des États-Unis est inséparable de sa sécurité économique<sup>8</sup>.

Dans cet affrontement, les armes changent. Les salariés remplacent les bataillons de soldats. Ils montent au front pour conquérir les marchés internationaux. La puissance de feu fait place à la puissance financière. La télévision, le cinéma, les jeux vidéo, la culture en général sont des armes bien plus efficaces que les canons, les tanks et les avions de chasse pour imposer dans la douceur son modèle économique. C'est le fameux concept de « soft power » imaginé par le professeur Joseph Nye<sup>9</sup> en 1990 pour contrer la thèse sur le déclin américain<sup>10</sup>. Avec ses cinq piliers – sa monnaie, son armée, Hollywood, CNN et Internet – les États-Unis bénéficient d'un « *polygone de domination*<sup>11</sup> » sans équivalent dans l'histoire. Il suffit à l'Amérique de s'appuyer sur ses cartes maîtresses pour rester la « *seule nation indispensable*<sup>12</sup> » et de formater le monde pour le mettre au service de la société américaine,

comme le déclare Madeleine Albright en 1997 : « *Nous devons continuer à façonner un système économique global qui travaille pour l'Amérique*<sup>13</sup> ». Et comment façonne-t-on le monde pour qu'il se mette au service des États-Unis ? Certainement pas en créant un empire territorial : trop lourd, trop complexe à diriger. Établir son hégémonie est un chemin moins risqué. Et pour cela, il y a rien de mieux que l'économie. Dans un monde où les démocraties sont censées ne pas se faire la guerre, le commerce est le meilleur moyen d'imposer son leadership : faire boire du Coca-Cola plutôt que du Perrier, vendre des Hamburgers plutôt que du couscous ou des kebabs, inonder le monde de films hollywoodiens plutôt que de longs métrages des enfants de la Nouvelle vague... Dans ce monde post-guerre froide, les multinationales et leurs filiales remplacent les troupes d'occupation. Cela coûte moins cher et rapporte plus.

COMMENT FAÇONNE-T-ON LE MONDE POUR QU'IL SE METTE AU SERVICE DES ÉTATS-UNIS ? CERTAINEMENT PAS EN CRÉANT UN EMPIRE TERRITORIAL : TROP LOURD, TROP COMPLEXE À DIRIGER. ÉTABLIR SON HÉGÉMONIE EST UN CHEMIN MOINS RISQUÉ. ET POUR CELA, IL Y A RIEN DE MIEUX QUE L'ÉCONOMIE.

Pour façonner le monde (*shapping the World*), l'administration américaine invente de nouveaux outils théoriques. Le président Bill Clinton est l'initiateur du concept de

« recherche de maintien et de supériorité économique<sup>14</sup> ». Sa stratégie économique se nourrit des travaux de plusieurs chercheurs qui annoncent la radicalisation des rapports économiques internationaux. Parmi eux, on trouve Lester Thurow<sup>15</sup>, Edward N. Luttwak<sup>16</sup>, Robert Reich<sup>17</sup> et Jeffrey Garten<sup>18</sup>. D'ailleurs, les deux derniers rejoignent les équipes présidentielles. Imprégné de cette atmosphère de guerre économique, Bill Clinton prend ses dispositions.

Le 30 septembre 1993, il signe le Trade Promotion Coordinating Committee (TPCC<sup>19</sup>). Le TPCC coordonne

(8) *Washington Post*, 5 novembre 1993.

(9) Nye (J.), 1990, *Bound to Lead: The Changing Nature of American Power*, New York, Basic Books.

(10) Thèse notamment portée par Paul Kennedy dans *Naissance et déclin des grandes puissances*, Paris, Payot, 1988.

(11) Sur (S.), 2007, « Impérialisme et droit international en Europe et en Amérique », in Jouannet (E.) et Ruiz Fabri (H.) (dir.), *Impérialisme et droit international en Europe et en Amérique*, Société de législation comparée, p. 318-334.

(12) Discours inaugural du deuxième mandat du président Bill Clinton en 1997.

(13) Déclaration du 8 janvier 1997 devant le Senate Committee on Foreign Relations (SCFR), United States Information Service, 9 janvier 1997, p. 8.

(14) Daguzan (J.-F.), 1997, « Les États-Unis et la recherche de la supériorité économique », *Revue française de géoéconomie*, n° 2, été.

(15) Thurow (L.), 1992, *Head to Head: The Coming Battle among America, Japan and Europe*, New-York, William Morrow, 1992.

(16) Luttwak (E.N.), 1995, *Le rêve américain en danger*, Paris, Odile Jacob.

(17) Reich (R.), 1993, *L'économie mondialisée*, Paris, Dunod ; 2008, *Supercapitalisme*, Paris, Vuibert.

(18) Garten (J.), 1992, *A Cold Peace: America, Japan, Germany and the Struggle for the Supremacy*, New-York, Time Books.

(19) Executive order 12870.

la politique de promotion, de soutien et de financement des exportations américaines et en définit la stratégie. Installée au département du Commerce, cette agence intergouvernementale regroupe les départements d'État, de l'Agriculture, de l'Intérieur, du Trésor, de l'Énergie, des Transports, de la Défense, du Travail, les agences de l'aide au développement, de l'environnement, de l'information... ainsi que le Conseil national de sécurité et enfin toutes les agences que le Président juge opportun d'y ajouter. Autrement dit, les services de renseignement<sup>20</sup>. Toujours en 1993, Bill Clinton crée le National Economic Council (NEC). C'est l'équivalent du Conseil national de sécurité (National Security Council) mais pour les affaires économiques. Le NEC conseille le président sur la stratégie économique à l'heure de la globalisation, accorde la politique économique nationale et internationale et s'assure enfin de la mise en œuvre des décisions gouvernementales. Il rassemble tous les conseillers économiques du président des États-Unis et son directeur travaille directement avec le conseiller à la sécurité nationale. D'ailleurs, le NEC peut faire appel à toutes les ressources du gouvernement y compris celles des agences de renseignement et de sécurité. En février 2011, un rapport du NEC insiste sur la nécessité de protéger les informations des entreprises innovantes face aux nombreuses attaques des concurrents étrangers. Un besoin vital qui engage, selon lui, la croissance et plus largement l'avenir du pays<sup>21</sup>.

Troisième initiative du président Clinton en 1993 : l'Advocacy Center. C'est un organisme intergouvernemental lui aussi géré depuis le département du Commerce. Sa mission est d'encourager et de soutenir concrètement les entreprises américaines qui concourent sur des marchés publics à l'étranger. L'Advocacy center (ou Advocacy Networks) veille à ce que les biens et services produits par des Américains aient « *les meilleures chances dans la compétition économique mondiale. Le service est large et varié ; il s'adresse à des entreprises qui souhaitent faire passer un message à des gouvernements étrangers ou à des sociétés publiques* »<sup>22</sup>. Ce message consiste généralement à alerter les autorités publiques étrangères d'un risque de distorsion de concurrence ou pire, d'une compétition biaisée. L'Advocacy Center utilise les ressources de l'ensemble des ministères et peut également faire appel aux services

de renseignements et de sécurité. À l'étranger, les ambassades sont invitées à ouvrir leur carnet d'adresses et à soutenir les offres du *Made in USA*. L'Advocacy center publie régulièrement des rapports sur ses activités. Sont détaillés ses modes d'interventions, exemples à l'appui : appel téléphonique et/ou déplacement du secrétaire d'État au commerce ; réceptions et rencontres organisées par les diplomates à l'étranger ; intervention directe du président des États-Unis... Dans un rapport du Parlement européen sur Echelon (système d'écoute et d'espionnage électronique dirigé par les États-Unis avec la Grande-Bretagne, le Canada, la Nouvelle-Zélande, l'Australie<sup>23</sup>), on trouve un tableau fort intéressant fourni par le journaliste d'investigation Duncan Campbell. Ce tableau liste les marchés remportés par des entreprises américaines de 1993 à 2000 grâce aux interventions directes de l'Advocacy center, soit plus de 26 milliards de dollars de chiffre d'affaires encaissés par les Américains au détriment des Français, Allemands, Hollandais, Italiens, Danois, Suédois, Anglais, Espagnols...<sup>24</sup> L'Advocacy Center, service public, peut ainsi se vanter auprès des citoyens américains, d'avoir enrichi le pays et d'avoir contribué à sauvegarder des milliers d'emplois, voir à en créer autant.

Le soutien, le lobbying, et même l'influence ne sont pas les seules armes à la disposition de l'Advocacy Center. Comme nous l'avons dit, il bénéficie aussi de l'aide des services de renseignement. Lorsqu'un marché étranger risque d'échapper à une entreprise américaine, l'Advocacy Center se transforme en *War Room*. Comme le lui permet la loi (cf. TPCC), et si ses membres ont le sentiment que les concurrents ne respectent pas les règles, il emploie les grands moyens : CIA, NSA... entrent en action. C'est ainsi que la France a été victime à deux reprises au moins de ces méthodes particulièrement agressives. En 1994, la société française Thomson CSF est en train de remporter le marché SIVAM de surveillance électronique de l'Amazonie au Brésil. Placée sur écoute par la National Security Agency (NSA), la délégation française est immédiatement suspectée de corrompre des officiels brésiliens. La presse brésilienne s'en fait l'écho et Thomson perd ce marché d'1,4 milliard de dollars au profit de l'entreprise américaine Raytheon. Les mêmes procédés sont utilisés par les Américains un an plus tard dans la vente d'avions civils à l'Arabie saoudite. Avec leur

(20) <http://www.archives.gov/federal-register/executive-orders/pdf/12870.pdf>. Consulté le 23 juin 2015.

(21) « A Strategy for American Innovation : Securing Our Economic Growth and Prosperity », NEC, février 2011. Consulté sur internet le 24 juin 2015. <https://www.whitehouse.gov/innovation/strategy>

(22) Site de l'Advocacy Center. Consulté le 24 juin 2015. <http://www.export.gov/advocacy/index.asp>

(23) [http://vadeker.net/humanite/geopolitique/rapport\\_echelon\\_fr.pdf](http://vadeker.net/humanite/geopolitique/rapport_echelon_fr.pdf). Consulté le 23 juin 2015. Voir également l'étude du service de recherche du parlement européen (EPRS) sur « L'affaire Echelon » de Franco Piodi et Lolanda Mombelli, octobre 2014 PE 538.877. <http://www.europarl.europa.eu/EPRS/EPRS-Study-538877-Echelon.pdf>

(24) [http://www.duncancampbell.org/menu/surveillance/echelon/Contract\\_analysis.pdf](http://www.duncancampbell.org/menu/surveillance/echelon/Contract_analysis.pdf). Consulté le 23 juin 2015.

avion européen, les Français sont persuadés de remporter le marché. À tort, quelques écoutes de la NSA plus tard et des articles sortent dans la presse et désignent les Français comme des corrupteurs. Un coup de fil du Président Clinton au roi d'Arabie saoudite et l'affaire retombe dans le panier des Américains. La perte est estimée à 6 milliards de dollars pour Airbus au profit de Boeing et de MacDonnel Douglas.

Le système national d'intelligence économique américain repose sur une collaboration étroite entre secteur public et privé. À travers ses ministères et ses agences, le gouvernement américain se met à la disposition des entreprises pour échanger des informations utiles à la connaissance et à la conquête des marchés étrangers. Toutes les agences publiques participent, même celles qui sont liées à la sécurité nationale. Il existe ainsi de nombreux canaux d'échange entre le privé et le public. L'Overseas Security Advisory Council (OSAC<sup>25</sup>), créé en 1985, permet aux directeurs de sécurité des multinationales américaines de côtoyer les fonctionnaires du Bureau of Diplomatic Security rattaché au département d'État. L'OSAC accueille également des membres de l'appareil de sécurité et de renseignement américain. L'OSAC publie régulièrement des alertes sur les risques politiques, sociaux et économiques dans la plupart des pays ainsi que des études géographiquement ciblées. Outre les questions de sécurité, l'OSAC promeut plus largement les intérêts économiques américains à l'étranger. Plus de 3 500 entreprises, ONG, établissements d'enseignement ou de religion... adhèrent à l'OSAC qui compte plus de 16 000 utilisateurs de ses services. Autre pont entre le secteur public et le secteur privé : le Business Executives for National Security (BENS) fondé en 1982<sup>26</sup>. Grâce au BENS, le privé propose des solutions au gouvernement pour améliorer la sécurité des États-Unis. Piloté depuis 2013 par le Général Norton A. Schwartz, il est composé de dirigeants et de cadres issus des grandes entreprises américaines. Comme il est indiqué sur son site,

le BENS « *travaille avec toutes les unités combattantes* » et publie des rapports sur la sécurité intérieure des États-Unis. Il propose aussi ses conseils pour améliorer l'efficacité des forces armées et traite des dossiers aussi différents que le gaz de schiste ou la cyber-sécurité... Cette proximité entre privé et public avantage les deux parties. Pour le public, l'enjeu est de mieux comprendre les problématiques de sécurité des entreprises. Pour le privé, il est double : être mieux protégé et s'ouvrir de nouveaux marchés publics en y imposant ses normes techniques. Améliorer la compréhension du monde des affaires permet au gouvernement de mieux le surveiller.

Les Américains ne s'en sont jamais cachés : leurs services de renseignement servent aussi à espionner leurs alliés.

LES AMÉRICAINS NE S'EN  
SONT JAMAIS CACHÉS :  
LEURS SERVICES DE  
RENSEIGNEMENT SERVENT  
AUSSI À ESPIONNER LEURS  
ALLIÉS. BIEN AVANT LES  
RÉVÉLATIONS D'EDWARD  
SNOWDEN EN JUIN 2013 SUR  
LA SURVEILLANCE GLOBALE  
DE LA NSA, UN ANCIEN  
DIRECTEUR DE LA CIA  
(1993-1995) LE RECONNAÎT  
PUBLIQUEMENT EN 2000.

Bien avant les révélations d'Edward Snowden en juin 2013 sur la surveillance globale de la NSA, un ancien directeur de la CIA (1993-1995) le reconnaît publiquement en 2000. En effet, le 17 mars 2000, James Woolsey rédige une tribune dans le *Wall Street Journal* clairement intitulé « *Why we spies our allies ?* » (Pourquoi nous espionnons nos alliés ?). Il justifie l'espionnage des entreprises européennes au nom de la suspicion de corruption qui pèse sur elles. James Woolsey pense que le système libéral américain permet aux entreprises de fabriquer de meilleurs produits que ceux des concurrents européens. Par conséquent, les entreprises du vieux continent n'ont d'autre choix que de recourir à la corruption pour écouler leurs marchandises ! « *Votre saint patron économique, écrit-il à l'adresse des Européens, est encore Jean-Baptiste Colbert, quand le nôtre est Adam Smith*

[...] *Oui, chers amis continentaux, nous vous avons espionnés parce que vous distribuez des pots-de-vin. Les produits de vos compagnies sont souvent plus coûteux, moins avancés sur le plan technologique, ou les deux à la fois, que ceux de vos concurrents américains. En conséquence de quoi vous pratiquez beaucoup la corruption. Vos gouvernements sont tellement complices que dans plusieurs pays européens les pots-de-vin sont encore déductibles des impôts*<sup>27</sup> ».

(25) [www.osac.gov](http://www.osac.gov)

(26) <http://www.bens.org>

(27) Vous retrouvez l'intégralité de la tribune de James Woolsey à l'adresse suivante : <http://cryptome.org/echelon-cia2.htm>. Consulté le 24 juin 2015.

En juin 2013, les révélations d'Edward Snowden, ancien consultant à la NSA et ex-agent de la CIA, confirment l'existence d'une surveillance globale du monde par les grandes oreilles américaines. Tout est écouté, enregistré, stocké dans d'immenses bases de données : téléphone fixe ou mobile, fax, PC, tablette, internet... rien n'échappe aux antennes de la NSA. *Big Brother* n'est pas un mythe, il est bien réel et il est américain. La NSA explique que 35 % de ses ressources sont allouées à la lutte antiterroriste. Quid des 65 % restants ? « *C'est pour l'espionnage politique, militaire et surtout économique* » assure un spécialiste de la sécurité des systèmes de communication<sup>28</sup>. D'où les révélations sur les écoutes effectuées par la NSA sur des individus et des entreprises qu'il est difficile de soupçonner de lien avec le terroriste : les téléphones portables de la chancelière allemande Angela Merkel et des présidents français (Jacques Chirac, Nicolas Sarkozy et François Hollande), l'espionnage du géant pétrolier brésilien Petrobras, des fleurons de l'industrie européenne avec la complicité des services de renseignement allemand... Bref, le marché est en proie à une guerre du renseignement économique !

## Les services de renseignement américains sur le front économique

Les Américains jouent sur les mots. Ils affirment que l'espionnage économique ne profite pas à leurs entreprises, mais nourrit l'analyse du gouvernement. Vu les liens étroits entre public et privé, on est tenté de s'interroger : comment être sûr que des informations récupérées par la CIA ou la NSA et destinées aux dirigeants politiques ne tombent pas entre les mains des entrepreneurs américains ? Après les mensonges sur l'Irak en 2003 et les tentatives de l'administration Obama de nier l'ampleur de la surveillance globale, comment croire encore en la parole des dirigeants américains ? D'autant que le débat sur l'utilisation des services de renseignement dans la compétition économique mondiale

n'est pas nouveau. Dès la chute du mur de Berlin, les Américains s'interrogent sur les missions de leur appareil de surveillance. L'ours soviétique est mort, que faire des 16 agences de renseignements ? En 1996, le Congrès réfléchit donc à la question. La Commission Harold Brown et Warren B. Rudman<sup>29</sup> apportent une réponse : pas question de délivrer des informations aux entreprises américaines sur leurs concurrents étrangers. En revanche, Brown et Rudman invitent le renseignement américain à fournir à la Maison-Blanche ainsi qu'aux départements d'État et du Commerce des renseignements économiques (*Economic Intelligence*) sur les pratiques commerciales des entreprises et des États qui ne respectent pas les règles de la concurrence pure et parfaite<sup>30</sup>. La nuance est-elle vraiment de taille ? Pas vraiment. Elle concerne le destinataire, pas l'objet : les services de renseignement américain sont bien autorisés à pratiquer l'espionnage économique. Quatre ans avant la commission Brown et Rudman, la CIA reconnaît par la voix de son directeur Robert Gates que « *40 % des demandes qui nous sont faites sont de nature économique. La plupart des membres du gouvernement estiment que les menaces et les opportunités de la nouvelle décennie porteront sur les questions économiques internationales* »<sup>31</sup>. Une semaine après sa déclaration fracassante, Robert Gates tente de rectifier le tir. Il précise, dans la presse, que la CIA n'espionne pas les entreprises étrangères... seulement celles qui sont déloyales envers leurs concurrents américains<sup>32</sup>. Une chose est sûre : le business mondial est devenu l'affaire de la CIA<sup>33</sup>. Et la Maison-Blanche ne se gêne pas pour lui passer commande. En 1995, le président Bill Clinton demande à la CIA de mener des opérations contre les concurrents commerciaux des États-Unis<sup>34</sup>. Tous les concurrents ? Oui même ceux de ses plus fidèles alliés, comme la Grande-Bretagne. Irritée, Londres fait part de son mécontentement face à l'infiltration d'agents américains dans ses entreprises<sup>35</sup>. En 1995, l'administration Clinton s'explique et publie un texte sur la sécurité des États-Unis<sup>36</sup>. Elle avance trois arguments pour justifier l'engagement de l'appareil de sécurité et de renseignement dans le commerce : lutter contre la délinquance économique, plus particulièrement la corruption ; protéger les secrets technologiques, commerciaux et scientifiques

(28) Entretien avec Franck Leroy en avril 2015, auteur de *Surveillance. Le risque totalitaire*, Arles, Actes Sud, 2014.

(29) «Preparing for the 21 st Century: An Appraisal US intelligence», <http://www.gpo.gov/fdsys/pkg/GPO-INTELLIGENCE/content-detail.html>

(30) «Preparing for the 21 st Century: An Appraisal US intelligence», <http://www.gpo.gov/fdsys/pkg/GPO-INTELLIGENCE/content-detail.html>, p. xvii.

(31) Discours tenu le 13 avril 1992 devant le Club économique de Detroit. Lire Stanley Kober, « The CIA as Economic Spy: The Misuse of US Intelligence after The Cold War », *Cato Institute, Policy analysis*, n° 185, 8 décembre 1992. Consulté le 25 juin 2015 : <http://www.cato.org/publications/policy-analysis/cia-economic-spy-misuse-us-intelligence-after-cold-war>

(32) *Time Magazine*, 20 avril 1992.

(33) Johnson (L.K.), 1997, «Economic Intelligence and the CIA», *South-eastern Political Review*, vol. 25, n° 3, septembre.

(34) Risen (J.), 1995, «Clinton Reportedly Orders to Focus on Trade Espionage», *Los Angeles Times*, 23 juillet.

(35) Adams (J.), 1995, «CIA Unleashes Spy Teams on Foreign Firms», *Sunday Times* (Londres), 6 août.

(36) White House, 1995, «A National Security Strategy of Engagement and Enlargement», février, p. 19-21.

américains ; renforcer les positions des États-Unis dans les négociations commerciales internationales. À l'un de ses agents qui lui demande ce que doit être le rôle de la CIA dans la défense des intérêts économiques américains, voici ce que répond John Deutch, alors directeur de la CIA : « *Je ne crois pas que l'Agence doive soutenir directement les positions commerciales des États-Unis. Mais je pense que l'Agence a un rôle important à jouer dans ce que j'appelle le renseignement économique pour informer la classe politique américaine. Elle a également un rôle dans la contre-intelligence pour aider les entreprises américaines qui y sont confrontées. Mais offrir une assistance personnelle aux firmes américaines, je pense que ce serait une grave erreur qui doit être évitée*<sup>37</sup> ». Pas d'assistance directe donc aux firmes américaines. Mais rien ne garantit que les renseignements et les analyses de la CIA qui transitent par les ministères n'aboutissent dans le QG des grandes entreprises américaines via par exemple les syndicats patronaux ou les fédérations sectorielles. Que fait l'Oncle Sam des renseignements tirés de l'espionnage des grandes entreprises européennes comme Airbus, Safran ou Gemalto ? Le doute existe. Or, les marchés n'aimant pas l'incertitude, il est possible que certaines entreprises non américaines se résignent à accepter ce qui s'apparente à une distorsion de concurrence.

La CIA ne se contente pas de monter au front économique comme agence de renseignement. La Centrale de Langley est aussi un entrepreneur. En 1999, elle crée In-Q-Tel, un fonds d'investissement spécialisé dans les nouvelles technologies. Installé au cœur de la Silicon Valley, In-Q-Tel achète des parts dans les start-up d'avenir<sup>38</sup>. La CIA veut maîtriser les futures technologies liées à la

cyber-surveillance. À ses débuts, In-Q-Tel bénéficie d'une force de frappe non négligeable avec 30 milliards de dollars. Nanotechnologies, biotechnologies, logiciels d'analyses, de traduction, d'interprétation des langues étrangères (particulièrement orientales), communication et infrastructures réseaux, *Big Data*... la CIA est présente dans le capital de plus de 100 start-up ! Le *Digital World* est sa cible numéro 1. Quand les États-Unis ne disposent pas de certains joujoux technologiques, In-Q-Tel s'approvisionne à l'étranger, quitte à avancer masqué. Comme dans le cas Gemplus, société française leader mondial des cartes à puce<sup>39</sup>. En 2000, Gemplus est racheté par le fonds Texas Pacific Group (TPG) qui place Alex Mandl à la tête de l'entreprise. Alex Mandl est un ancien d'AT & T et surtout il est membre d'In-Q-Tel !

Garder la *pole position* dans la compétition internationale, c'est aussi protéger ses bijoux de famille. En janvier 2001, la communauté du renseignement américaine crée le National Counterintelligence Executive (NCIX<sup>40</sup>). L'objectif du NCIX<sup>41</sup> est de lutter contre toutes les menaces pesant sur la sécurité nationale, particulièrement les risques d'espionnage industriel et économique<sup>42</sup>. Le NCIX rebaptisé

depuis National Counterintelligence and Security Center (NCSC) participe au dialogue entre les membres de la communauté du renseignement et les acteurs économiques. Ensemble, ils dressent la liste des technologies vitales à la bonne santé économique du pays. Le NCSC publie régulièrement des guides pour les entreprises et des rapports sur l'état des menaces. Ce qui lui permet de fournir des statistiques sur les secteurs économiques américains

QUE FAIT L'ONCLE SAM DES  
RENSEIGNEMENTS TIRÉS DE  
L'ESPIONNAGE DES GRANDES  
ENTREPRISES EUROPÉENNES  
COMME AIRBUS, SAFRAN OU  
GEMALTO ? LE DOUTE EXISTE.  
OR, LES MARCHÉS N'AIMANT  
PAS L'INCERTITUDE,  
IL EST POSSIBLE QUE  
CERTAINES ENTREPRISES  
NON AMÉRICAINES SE  
RÉSIGNENT À ACCEPTER  
CE QUI S'APPARENTE À  
UNE DISTORSION DE  
CONCURRENCE.

(37) Voir également John Deutch, ancien directeur de la CIA (1995-1996), «DCI Remarks at CIA Town Meeting», 11 mai 1995. Consulté le 25 juin 2015. [https://www.cia.gov/news-information/speeches-testimony/1995/dci\\_speech\\_51195.html](https://www.cia.gov/news-information/speeches-testimony/1995/dci_speech_51195.html)

(38) <https://www.iqt.org>

(39) Moinet (N.), 2003, « Les batailles secrètes de la science et de la technologie », Panazol, Lavauzelle.

(40) *Presidential Decision Directive* (PDD)-CI-21, «US Counterintelligence Effectiveness-Counterintelligence for the 21 st Century». Consulté le 26 juin 2015. <http://fas.org/irp/offdocs/pdd/pdd-75.htm>

(41) [www.ncsc.gov](http://www.ncsc.gov)

(42) Voici les principaux objectifs du NCIX listés dans un document daté du 27 mars 2007 ([ncix.gov](http://ncix.gov)) : « *Secure the Nation Against Foreign Espionage and Electronic Penetration ; Protect the Integrity of the US Intelligence System ; Support National Policy and Decisions ; Protect US Economic Advantage, Trade Secrets and Know How ; Support US Armed Forces ; Manage the Counterintelligence Community to Achieve Efficient Coordination ; Improve Training and Education of the Counterintelligence Community ; Expand National Awareness of Counterintelligence Risk in the Private as well as Public Sector* ».

les plus attaqués et de pointer certains pays comme étant particulièrement agressifs envers les firmes américaines. Chine, Iran, Russie... mais aussi certains alliés des États-Unis comme la France ou l'Allemagne ! Le NCSC délivre également des informations pratiques à destination des cadres américains qui voyagent dans le monde afin de protéger les secrets commerciaux et technologiques de leur entreprise : utilisation du téléphone, des tablettes et des ordinateurs, des mails, des clés USB...<sup>43</sup>

Depuis 1993, les États-Unis bénéficient d'un écosystème économique offensif et défensif que le président démocrate Barack Obama confirme et renforce même. Au cours de son premier mandat, le 28 février 2012, il annonce la création d'un nouvel organisme, l'Interagency Trade Enforcement Center (ITEC) rattaché à l'Office of the United States Trade Representative (USTR<sup>44</sup>). Départements d'État, du Commerce, des Sciences et de l'Énergie, du Trésor, de la Sécurité intérieure... siègent à l'ITEC aux côtés des services de renseignement. L'ITEC enquête et surtout dénonce les mauvaises pratiques commerciales des concurrents étrangers, lesquelles bloquent la croissance et détruisent les emplois des Américains<sup>45</sup>. L'ITEC fournit des informations au président pour alimenter ses discussions avec les partenaires commerciaux de Washington. Les résultats de ses travaux enrichissent les données du rapport annuel sur les barrières commerciales dans le monde, le *National Trade Estimate Report on Foreign Trade Barriers* (NTE<sup>46</sup>). Barack Obama appuie également la diplomatie économique d'Hilary Clinton, alors Secrétaire d'État. Exit le *soft power*, l'ex-première dame des États-Unis fait la promotion du *smart power* qu'elle définit ainsi : « *Nous devons faire usage de ce qu'on appelle le smart power, c'est-à-dire la panoplie complète des outils qui sont à notre disposition (diplomatie, économie, armée, politique, droit, culture) en utilisant chacun d'entre eux ou une combinaison de tous ces outils. Grâce au smart power, la diplomatie deviendra l'avant-garde de la politique étrangère*<sup>47</sup> ». Une avant-garde particulièrement discrète. En 2009, Wikileaks<sup>48</sup>, le site de Julian Assange, révèle qu'Hilary Clinton demande à tous ses diplomates de mener des actions d'espionnage sur leurs homologues étrangers. Leur mission : récupérer toutes les informations possibles sur leurs interlocuteurs,

de l'adresse mail personnelle jusqu'au numéro de carte de crédit ! La secrétaire d'État est particulièrement active en matière d'intelligence économique. Elle crée deux outils pour appuyer l'US Inc. En novembre et décembre 2011, elle installe le Bureau For Energy Resources et le Foreign Affairs Policy Board. Le premier soutient les pétroliers et gaziers américains dans la conquête de nouveaux gisements dans le monde, particulièrement au Moyen-Orient. Le second réunit diplomates, anciens hauts fonctionnaires, politiciens et membres des grands cabinets de conseil des multinationales américaines pour booster la diplomatie économique de Washington.

## Un arsenal juridique unique, défensif et offensif

Les États-Unis sont une démocratie, respectueuse de la gouvernance internationale. Toutefois, lorsque leurs intérêts économiques ne coïncident pas avec les lois internationales, les parlementaires votent des lois extraterritoriales. « *Il existe bien un principe de "présomption contre l'extraterritorialité", écrit un juge de la Cour suprême, qui postule l'inapplicabilité à l'étranger d'une loi américaine*<sup>49</sup> ». Mais il semble que ce principe ne soit plus guère opérationnel en ces temps de mondialisation où les lois américaines prétendent s'appliquer sur toute la planète ! L'idée consiste à « adapter » le droit international à leurs intérêts nationaux. Autrement dit, de créer selon la formule d'Alejandro Lorite Escorihuela, un « *droit international nationaliste*<sup>50</sup> ». Certaines lois américaines ont donc une portée internationale. Celles par exemple qui concernent les pays classés dans la liste des États voyous (*Rogue States*) par Washington. Il s'agit de la loi d'Amato-Kennedy (1996), qui sanctionne les pays soutenant le terrorisme, ayant la volonté de se procurer des armes de destruction massive ou refusant le processus de paix au Moyen-Orient. Et aussi de la loi Helms-Berton (1996) spécialement dirigée contre le régime de La Havane. Ces lois autorisent la poursuite devant la justice américaine des individus, groupes ou entreprises en relation avec ces fameux *Rogue States* : Cuba, Iran, Libye, Soudan... Elles s'appliquent autant aux entreprises et aux

(43) Laïdi (A.), 2010, *Les États en guerre économique*, Seuil, p. 180-184.

(44) <https://www.whitehouse.gov/the-press-office/2012/02/28/executive-order-establishment-interagency-trade-enforcement-center>

(45) <http://trade.gov/enforcement/itec/index.asp>

(46) <https://ustr.gov/about-us/policy-offices/press-office/reports-and-publications/2015/2015-national-trade-estimate>

(47) Hilary Clinton, audition le 13 janvier 2009 devant la Commission des affaires étrangères du Sénat.

(48) Dans une directive datée de 2009 et révélée par Wikileaks, intitulée *National Humint Collection Directive*, on apprend qu'Hilary Clinton a demandé à tous les diplomates américains de récupérer un maximum d'informations sur leurs interlocuteurs : noms, titres, numéros de téléphone professionnels et personnels, fax, "adresse" internet, pseudonymes, numéros de carte de crédit, numéros de carte de fidélité, horaires de travail, et autres informations biographiques jugées importantes.

(49) Breyer (S.), 2015, *La Cour suprême, le droit américain et le monde*, Paris, Odile Jacob, p. 116.

(50) Escorihuela (L.), 2007, « L'impérialisme comme produit dérivé : une lecture partisane de la doctrine internationaliste contemporaine aux États-Unis », in Jouannet (E.) et Ruiz Fabri (H.) (dir.), *op. cit.*

citoyens américains qu'aux étrangers et à leurs sociétés. La loi d'Amato-Kennedy interdit à tout acteur (État ou entreprise) d'investir plus de 40 millions de dollars par an dans le secteur pétrolier et gazier de ces États voyous. La loi Helms-Burton interdit tout « trafic » (*trafficking*) avec Cuba sur des biens qui auraient appartenu directement ou indirectement à des Américains (ou cubains naturalisés) avant la révolution cubaine (1959-1961). Les sanctions vont de l'impossibilité de faire du commerce aux États-Unis à l'interdiction d'entrée sur le territoire étatsunien pour les personnes concernées et leurs enfants mineurs ! Ces lois sont présentées comme des armes économiques qui servent un objectif politique. Toutefois, elles permettent aussi de viser un objectif purement économique en interdisant par exemple aux sociétés étrangères de faire des affaires dans des pays où l'Oncle Sam refuse l'accès à ses propres entreprises. C'est une façon de garder le terrain vierge afin de ne pas pénaliser le *Made in USA*, le jour où la Maison-Blanche lèvera ses sanctions. Le pétrolier français Total a longtemps été critiqué et même menacé par le département d'État américain pour ses activités en Iran. Les Américains estiment que le marché iranien appartient à sa compagnie Conoco qui s'est retirée du pays des Mollah après le vote de la loi d'Amato-Kennedy. « Ces lois [...] mêlent des considérations de politique internationale, de moralité dans les affaires internationales, et de défense des intérêts commerciaux américains<sup>51</sup> ». À l'époque où elles sont votées, l'Union européenne assure 45 % du commerce avec Cuba et le Canada est le premier partenaire de La Havane avec plus de 500 millions de dollars d'échange annuel. Par conséquent, les États d'Amérique latine, l'Union européenne et le Canada condamnent ces injonctions juridiques américaines et prennent des mesures pour protéger leurs ressortissants et les entreprises susceptibles d'être poursuivies<sup>52</sup>. Dans certains cas, la protection de l'État originaire de l'entreprise ne suffit pas. La société française Pernod-Ricard, victime de la loi Helms-Burton, en sait quelque chose. Après avoir créé un *joint-venture* avec les Cubains en 1993 pour commercialiser la marque de rhum Havana Club, Pernod est poursuivi devant le tribunal de New-York. Les Américains dénie au géant des spiritueux français le droit d'utiliser cette marque sur son territoire. La France porte plainte devant l'Organisation mondiale du commerce (OMC) qui condamne les États-Unis en 2002. Mais rien n'y fait, Washington refuse de modifier sa législation. Pernod porte l'affaire jusqu'à la

Cour suprême mais perd. Ce qui signifie que même si l'embargo contre Cuba est levé, la marque Havana Club est *persona non grata* aux États-Unis, du moins tant que la loi Helms-Burton n'est pas amendée. L'enquête de consultants en intelligence économique du cabinet Cairn Executive commandée par Pernod-Ricard révèle qu'elle est victime d'une attaque contrôlée en sous main par son concurrent Bacardi. La société Bacardi, autre géant des spiritueux, appartient à une grande famille cubaine exilée en Floride<sup>53</sup>. Celle-ci n'accepte pas qu'un Français s'aventure dans ce qu'elle considère être sa chasse gardée. D'après Hernando Calvo Ospina, la société Bacardi entretient des liens étroits avec la CIA qui compte sur elle pour reprendre les rênes économiques de l'île à la fin de l'ère castriste<sup>54</sup>.

La législation américaine en matière d'intelligence économique est aussi offensive que défensive. Les États-Unis disposent d'un véritable arsenal juridique pour protéger leurs intérêts économiques : l'*Industrial Espionage Act*, l'*Economic Security Act* et l'*Economic Espionage Act*, trois lois votées par le Congrès en 1996. L'objectif est de décourager toute tentative d'espionnage industriel et économique, la loi américaine définissant l'espionnage économique par le fait que « quiconque sachant que l'infraction profite à un gouvernement, une organisation ou un agent étranger, vole sciemment ; s'approprie, soustrait, emporte ou dissimule, sans autorisation, ou obtient un secret d'affaires par fraude, ruse ou tromperie, reproduit, établit des croquis ou dessins, photographie, sans autorisation copie, transfère ou charge par voie informatique, modifie, détruit, photocopie, transmet, livre, envoie, expédie, communique ou transfère un secret d'affaires, reçoit, achète, détient, un secret d'affaires sachant qu'il a été volé, obtenu, approprié ou détourné sans autorisation... encourant... une amende d'un montant maximal de 500 000 dollars et, au plus, 15 ans d'emprisonnement, ou l'une de ces deux peines seulement<sup>55</sup> ».

La justice américaine défend les entreprises nationales et attaque leurs concurrents étrangers. Depuis quelques années, elle brandit son étoile de shérif du business international. Au moindre soupçon de fraude ou de triche, l'entreprise étrangère est sommée d'enquêter sur ses pratiques, voire carrément de démontrer elle-même sa culpabilité. Si la justice, plus exactement l'administration américaine, juge que l'entreprise collabore gentiment, l'amende n'est pas élevée. Si au contraire, elle résiste,

(51) Cosnard (M.), 1996, « Les lois Helms-Burton et d'Amato-Kennedy, interdiction de commercer avec et d'investir dans certains pays », *Annuaire français de droit international*, vol. 42, n° 42, p. 35.

(52) *Ibid*, p. 46.

(53) Laidi (A.), Lanvaux (D.), 2004, « Les secrets de la guerre économique », Paris, Seuil, p. 104-107.

(54) Calvo Ospina (H.), 2000, *Rhum Bacardi. CIA, Cuba et mondialisation*, Bruxelles, EPO.

(55) Traduction par J. Dupré et M. Pasquier, tirée des annexes de la thèse d'Hélène Masson, accessible sur <http://masson-intelligence-economique.blogspot.com/>

l'amende promet d'être conséquente. Enfin, si l'entreprise n'est pas suffisamment obéissante, elle risque très gros, c'est-à-dire son exclusion du marché américain. Et pour quel crime ? L'utilisation du dollar dans des transactions avec des pays mis au ban des nations par Washington (Soudan, Cuba, Iran...). C'est pour cette raison, qu'en juillet 2014, BNP écope d'une amende de 9 milliards de dollars sans passer par la case procès, car tout s'est joué au niveau administratif, le juge ne faisant qu'apposer sa signature sur l'accord entre l'administration et l'entreprise. La banque préfère payer plutôt que d'aller en justice et perdre définitivement sa licence aux États-Unis. BNP, Crédit Agricole, UBS, HSBC... sont passées à la caisse. La Société Générale, Volkswagen, la FIFA et bien d'autres pourraient les suivre. *« Les entreprises du monde entier sont confrontées à une pratique inédite de la part des autorités américaines telles que les agences de régulation comme l'Office of Foreign Asset Control (OFAC) ou la Securities and Exchange Commission (SEC), relayés par l'administration elle-même comme le Department of Justice (DOJ) ou les procureurs des États [...] La nouveauté et la généralisation de cette pratique invitent non*

*seulement les entreprises mais aussi le barreau, les pouvoirs publics et les institutions européennes à s'interroger ou à réagir devant ce qui apparaît comme un nouveau mode de régulation de la mondialisation économique par le droit<sup>56</sup> ». À réagir ? Pour l'heure, c'est le silence radio aussi bien en France qu'à Bruxelles.*

L'Amérique est puissante et impose sa loi dans les affaires politiques, militaires et économiques. Rares sont ceux qui en Europe osent s'y opposer. De temps en temps, la France et l'Allemagne protestent, mais finissent toujours par se résigner. Sur le Vieux Continent, les révélations Snowden ne font pas bouger les lignes d'un millimètre. Seul le Parlement européen hausse le ton devant les dérives du système d'intelligence économique américain (affaire Swift, affaires des données personnelles des passagers, affaire Snowden...). Mais dans cet affrontement économique globalisé, les mots ne pèsent guère s'ils ne sont pas accompagnés par des actions concrètes. Dans ce domaine, l'Europe semble paralysée face à une Amérique qui reste conquérante ■

---

(56) Garapon (A.), Servan-Schreiber (P.), 2013, *Deals de justice. Le marché américain de l'obéissance mondialisé*, Paris, PUF, p. 4-5.



## Une sécurité sans frontières pour les entreprises

Philippe CHAPLEAU

### Philippe CHAPLEAU



Philippe Chapleau suit, au sein du service Politique du quotidien Ouest-France, les questions de

défense et de politique étrangère et anime le blog Lignes de Défense. Il intervient à l'Institut national des hautes études de la sécurité et de la justice (INHESJ) où il est coordinateur d'enseignement, à l'IHEDN et à l'École des Transmissions où il enseigne les techniques de communication appliquées aux armées. Depuis une quinzaine d'années, ses recherches portent sur l'externalisation en matière de défense et sur les sociétés militaires privées. Il est l'auteur de *Mercenaires SA* (1998, Desclée de Brouwer), *Sociétés militaires privées. Enquête sur les soldats sans armées* (2005, L'Art de la guerre, Le Rocher), *Les Mercenaires. De l'antiquité à nos jours* (2006, Edilarge), *Les nouveaux entrepreneurs de la guerre* (2011, Vuibert) et *Piraterie maritime : Droits, pratiques et enjeux* (Vuibert, 2014).

**S'**il est un sujet qui est diversement pris au sérieux dans les entreprises, c'est bien celui de la sécurité à l'étranger. Pourtant, chaque dirigeant devrait garder à l'esprit l'avertissement du ministre français des Affaires étrangères. Le 30 janvier 2014, lors des VIII<sup>e</sup> Rencontres sur la sécurité des entreprises françaises à l'étranger, Laurent Fabius avait bien rappelé que « *c'est vous les responsables des entreprises qui êtes, bien sûr, au premier chef, responsables de la sécurité de vos collaborateurs, de vos entreprises, de vos investissements* ».

Selon un sondage publié en décembre 2014 par le Club des directeurs de sécurité des entreprises (CDSE), 74 % des dirigeants interrogés se sentent concernés par la question de l'insécurité à l'étranger. Cependant, l'insécurité n'a pas le même périmètre pour tous : les accidents de la circulation arrivaient en tête des préoccupations pour 57 % des sondés. *Quid* des « cybermenaces, déstabilisation, virtualisation des fraudes, trafics illicites transnationaux, kidnapping, radicalisme » que le CDSE liste parmi les menaces<sup>1</sup> ?

La désinvolture de certaines équipes dirigeantes a de quoi surprendre, voire exaspérer, lorsque l'on considère les nombreux, et souvent dramatiques,

(1) C'est d'ailleurs le thème du colloque du 10 décembre 2012 organisé par le CDSE. Voir <https://www.cdse.fr/9e-colloque-annuel-du-cdse-10>.

exemples de pénétrations de sites (intrusions physiques et cyberattaques), de pertes de contrats (pour cause d'espionnage économique, de malveillance, de comportements irresponsables de membres du personnel) et d'enlèvements d'employés dans des zones clairement identifiées « hautement à risques ».

À l'inverse, l'ampleur exagérée de certains plans de protection (centrés sur le seul risque terroriste par exemple) et la robustesse des moyens parfois mis en œuvre (avec une militarisation à outrance) témoignent d'une inclinaison sécuritaire quasi paranoïaque mais, finalement, à peine critiquable.

La prévision et la gestion des risques ne sont pas une mince affaire. Et ce sont souvent, outre la conscience plus ou moins aiguë que les dirigeants ont de la menace, des facteurs budgétaires qui guident les choix sécuritaires. Toutes les entreprises n'ont pas les moyens de TWDC, par exemple.

The Walt Disney Company a recruté, en septembre 2015, un « Senior manager, Global Intelligence Threat Analysis<sup>2</sup> ». Ce manager pilote une équipe d'analystes responsables du décèlement et de la gestion des risques. Cette équipe est composée de cinq analystes (avec des stagiaires) et de seize *contractors* fournis par des sous-traitants spécialisés.

Ce recrutement et les précisions que fournit l'avis appellent deux remarques. D'abord, il s'agit bien de « *Global Intelligence and Threat Analysis* ». La description du poste précise que l'équipe GITA « *provides strategic intelligence, threat assessments, vulnerability mitigation strategies and in-depth analytical products covering existing and developing threats that include counter terrorism, physical threats, cyber-attacks and all reputational risks to TWDC* ».

Ensuite, l'équipe de TWDC a un champ d'action mondial puisque sont prises en compte, outre l'intégralité des activités du groupe, l'abolition des frontières géographiques et la transcontinentalité des menaces.

La posture adoptée par la société américaine ne doit pas être perçue comme un épiphénomène, mais comme l'aboutissement d'une réflexion globale en matière de sécurité. Réflexion qui gomme, en particulier, toute

distinction entre le théâtre métropolitain/national et le théâtre étranger/international.

## Territorialité globalisée

En matière de sécurité globalisée, la question de la territorialité ne devrait pas se poser. Certes, les organismes fédéraux américains et de nombreuses entreprises conservent la distinction entre le CONUS (le « Continental US ») et l'OCONUS (« Outside continental US »), mais cette distinction est désormais surannée. En 2008, Nicolas Arpagian et Éric Delbecq, dans leur introduction au livre *Pour une stratégie globale de sécurité nationale*<sup>3</sup>, avertissaient que « *l'intérieur et l'extérieur constituent des distinctions qui ne sont plus totalement pertinentes* ».

Puisque faire du « business en milieu hostile », pour reprendre le titre du numéro 2 de la revue *Défis* de l'INHESJ<sup>4</sup>, ne relève plus nécessairement de l'expatriation, cartographier les risques ne doit plus se restreindre à une simple « mapemondisation » des menaces où l'identification et la hiérarchisation des zones à risques sécuritaires relèvent d'un simple code couleur.

Il est désormais urgent de penser en termes de sécurité globalisée, de conduire une réflexion cohérente et géographiquement unifiée, de mettre en place des procédures uniformisées et de compter sur des équipes chargées de la prévision et de la gestion des menaces dans leur globalité. Cartographier les risques pour une entreprise, c'est désormais la placer, elle, au centre d'un univers complexe de réseaux (humains, physiques, financiers, numériques, terroristes même) à évaluer et protéger. C'est en faire l'épicentre d'une nouvelle représentation du monde dans ses différentes acceptions.

Certes, certains théâtres physiques conservent une part de spécificité : ainsi les crises sanitaires, comme Ebola, affectent généralement des zones localisées et appellent des réponses *ad hoc*. Cependant, ces cas relèvent d'un traitement « tactique », alors que la doctrine et les procédures relèvent d'une réflexion « stratégique » conduite en amont par l'ensemble des équipes dirigeantes d'une entreprise.

(2) Voir le blog *Lignes de Défense* : <http://lignesdedefense.blogs.ouest-france.fr/archive/2015/09/10/dysney-recherche-un-analyste-specialise-dans-la-prevision-de-14657.html>

et l'offre d'emploi : <https://www.globaljobs.org/jobs/4248-burbank-california-the-walt-disney-company-senior-manager-global-intelligence-threat-analysis>

(3) Arpagian (N.), Delbecq (E.) (dir.), 2008, *Pour une stratégie globale de sécurité nationale*, Paris, Presaje/Dalloz, 2008.

(4) Voir <http://www.inhesj.fr/sites/default/files/defis2.pdf>. Le titre est lui-même inspiré par celui du livre *Business en milieu hostile* de Fanny Lecarpentier et Dimitri Linardos paru chez Vuibert en 2010.

## Au-delà la sécurité physique

Preuve que l'approche reste encore très axée sur la sécurité physique, les recrutements de directeurs de la sécurité sont encore très souvent effectués dans le vivier des anciens hauts fonctionnaires de la police nationale ou des « services » (62 % des directeurs de sécurité viennent des forces de polices et de gendarmerie ou des armées, selon le CDSE qui a enquêté auprès de 69 entreprises en septembre 2014). Certes, il s'agit de « professionnels chevronnés de la sécurité », mais leur expérience du monde de l'entreprise est souvent limitée et leur conscience de la polymorphie des menaces parfois réduite.

En outre, leur positionnement au sein des entreprises est trop fréquemment équivoque. De qui dépendent-ils directement ? De la direction générale (trop rarement, puisque selon un sondage du CDSE, seuls 42 % des directions de sécurité et de sûreté sont rattachées au directeur général de l'entreprise et 6 seulement sur les 69 interrogés étaient membres du comité exécutif<sup>5</sup>) ? Des ressources humaines ? À quel niveau peuvent-ils s'exprimer ?

Autre faiblesse : le faible niveau des moyens (budget, ressources humaines) qui leur sont alloués et qui limite leur efficacité. « Certains directeurs de la sécurité ressemblent à un vigile dans une guérite de poste de garde, alors que le site dont ils filtrent les accès n'est même pas entouré de grillage », résume, ironique, un spécialiste du conseil en sûreté.

## Externaliser

Le coût d'équipes multi-disciplinaires dédiées peut paraître prohibitif, mais rien n'interdit, en particulier aux PME, de recourir à une aide extérieure spécialisée et ponctuelle. TWDC fait bien appel à des « contractors », c'est-à-dire à des sous-traitants (il y a quelques années, par exemple, Total Intelligence Solutions et le Terrorism Research Center avaient travaillé pour Disney).

Il existe en France des entreprises spécialisées et aux compétences reconnues qui peuvent guider la réflexion et accompagner les entreprises (qui disposent bien sûr souvent de compétences internes), et leurs éventuelles directions de la sécurité, dans leur stratégie de protection. Parmi les plus connues, citons Risk & Co, Amarante, Geos, Control Risk, Gallice, Anticip, Erys Group, ESEI (filiale d'EPEE), International SOS... Certaines d'entre

elles évoluent au sein du CEFISI (Club des entreprises françaises de sûreté à l'international).

Des structures de conseil anglo-saxonnes, mais aussi européennes et asiatiques offrent également des services de qualité.

## Tentation du « low cost »

Cette externalisation, elle aussi, a un coût, bien sûr. Et les moyens à consacrer à la sécurité globalisée nécessiteront des efforts budgétaires que toutes les entreprises ne pourront/voudront consentir.

Quelles solutions envisager ?

Compter sur la puissance publique et le fameux partenariat public-privé ? Certes l'État répond présent en cas de crise majeure (on l'a vu dans le cas des prises d'otages français en Afrique), mais il ne dispose plus des moyens humains, matériels et financiers pour accompagner l'effort permanent de sécurité globale du secteur privé. Ce sont donc bien les entreprises qui doivent initier et accompagner leurs efforts sécuritaires.

Chercher des compétences *low cost* ? C'est déjà le cas en matière de sécurité embarquée puisque de nombreuses équipes de protection armées sont fournies, à bas coûts, par des entreprises de services de sécurité et de défense (ESSD) étrangères ou puisque des sociétés françaises de sécurité maritime font appel à des agents asiatiques ou africains pour rester compétitives.

Faire l'économie de la sécurité globalisée ? La question ne se pose pas pour les grands groupes (Areva, Total, Suez par exemple) qui ont enclenché une extension, ou plutôt une reconfiguration, du périmètre traditionnel de la sécurité, en gommant la notion d'extraterritorialité.

Pour les sous-traitants de ces grands groupes et les PME, la tentation est grande d'apporter des réponses *ad hoc* aux crises sectorielles qui les frappent. Mais ce n'est pas parce que le monde apparaît fragmenté qu'il faut appliquer une stratégie fragmentée, dissociant stratégie de sécurité intérieure et stratégie de sécurité extérieure. Et ce n'est pas parce que le monde apparaît chaotique que la réponse à la menace doit être chaotique. La vulnérabilité des entreprises qui feraient un tel choix n'en serait que plus grande ■

(5) Voir <https://www.cdse.fr/enquete-exclusive-du-cdse-relative> .



## La consolidation du droit applicable aux activités d'importance vitale

Xavier LATOUR

Depuis plusieurs années, la France protège les éléments particulièrement sensibles de son patrimoine industriel et économique. Sur le fondement des articles L 1332-1 et suivants du Code de la défense<sup>1</sup>, elle impose des obligations renforcées à des gestionnaires publics (collectivités, établissements publics) et privés (sociétés, associations, fondations) d'activités qualifiées d'importance vitale<sup>2</sup> (AIV).

La prise en considération d'une dimension économique de la sécurité n'est pas nouvelle. Déjà, l'ordonnance 59-147 du

7 janvier 1959 portant organisation générale de la défense, traduisait une vision globale de la défense, tandis que l'ordonnance 58-1371 du 29 décembre 1958 traitait plus particulièrement de la « protection des installations d'importance vitale ». Depuis, la stratégie de sécurité nationale développée par le *Livre blanc* de 2008, puis par celui de 2013, a confirmé la nécessité d'appréhender de nouvelles menaces de manière élargie.

La nation est menacée de multiples façons. En plus de l'espionnage traditionnel du savoir-faire et des informations commerciales, elle l'est, par exemple, par l'intermédiaire des réseaux de communication dématérialisés aussi mondialisés que vulnérables. Elle l'est, évidemment, par de nouvelles formes de terrorisme visant des sites industriels.

(1) « Les opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation, sont tenus de coopérer à leurs frais dans les conditions définies au présent chapitre, à la protection desdits établissements, installations et ouvrages contre toute menace, notamment à caractère terroriste. Ces établissements, installations ou ouvrages sont désignés par l'autorité administrative ». Les dispositions législatives sont complétées par un important cadre réglementaire (articles R 1332-1 et suivants du Code de la défense).

(2) « La protection des installations vitales », *Sécurité et Stratégie*, novembre 2010, n° 4.

Xavier LATOUR



Professeur de droit public à l'Université de Nice Sophia Antipolis (CERDACFF, EA 7267)

et secrétaire général de l'Association française de droit de la sécurité et de la défense.

C'est pourquoi, le dispositif créé par le décret 2006-212 du 23 février 2006<sup>3</sup> relatif à la sécurité des AIV, a évolué. La France est consciente de l'ampleur des besoins pour sécuriser une douzaine d'activités publiques et privées à risques<sup>4</sup>. Cela passe par la protection des sites, ainsi que par la prise en considération des impératifs de cybersécurité<sup>5</sup>. À ce titre, la récente stratégie nationale pour la sécurité du numérique, présentée le 16 octobre 2015 par le Premier ministre, constitue un élément essentiel pour améliorer les partenariats entre l'État et les entreprises, particulièrement celles gérant des infrastructures critiques. Cela justifie une amélioration des capacités d'expertise, un renforcement de la veille, ou encore une amélioration des capacités de gestion de crise.

En l'espace de quelques mois, le droit d'origine interne s'est consolidé<sup>6</sup>. La loi de programmation militaire (LPM), dans sa version 2013-1168 du 18 décembre 2013 et dans sa version 2015 (loi 2015-918 du 28 juillet 2015) a renforcé les dispositions applicables aux AIV. Parallèlement, en 2014, une instruction modernisée a remplacé la précédente version datant de 2008<sup>7</sup>. Elle insère clairement la protection des AIV dans l'environnement de la lutte contre le terrorisme, en insistant sur la mise en cohérence des dispositifs avec le plan Vigipirate. L'amélioration de la réponse aux crises a, également, motivé la modification du droit applicable aux moyens mobilisables, grâce à l'élaboration des mesures d'application des dispositions du Code de la défense relatives au service de sécurité nationale et à la réserve de sécurité nationale (décret 2015-508 du 7 mai 2015).

De son côté, l'Union européenne ne demeure pas inactive. Elle travaille à l'élaboration d'un cadre harmonisé par la voie de directives. Elle a ainsi adopté un texte relatif aux

attaques contre les systèmes d'information (directive 2013/40 du 12 août 2013), et en prépare un autre sur la sécurité des réseaux et de l'information dans le prolongement de sa stratégie de cybersécurité<sup>8</sup>.

*Les intérêts particuliers sont, plus que jamais, à concilier avec l'intérêt général. Des menaces protéiformes conduisent à inventer des réponses évolutives dans le cadre de nouveaux partenariats. Seules, les entreprises ne sont pas en mesure de se protéger alors que, parallèlement, l'État n'est plus l'acteur unique de la sécurité pour assurer la sauvegarde des populations et la continuité de l'activité.*

Dans une société globalisée, les partages de compétences entre le public et le privé sont moins nets. Les intérêts particuliers sont, plus que jamais, à concilier avec l'intérêt général. Des menaces protéiformes conduisent à inventer des réponses évolutives dans le cadre de nouveaux partenariats. Seules, les entreprises ne sont pas en mesure de se protéger alors que, parallèlement, l'État n'est plus l'acteur unique de la sécurité pour assurer la sauvegarde des populations et la continuité de l'activité. La France agit en conciliant le traditionnel interventionnisme régalién et le transfert massif de charges vers le privé. Ainsi, l'entreprise aussi entretient des liens étroits avec la sécurité nationale<sup>9</sup>.

La construction des dispositifs qui en découlent n'est pas exempte de difficultés. Malgré l'imbrication des enjeux, il n'est pas évident pour l'État de trouver la juste façon de s'immiscer dans le fonctionnement d'entreprises privées et, pour certaines, largement internationalisées.

Si les évolutions du droit applicable aux AIV témoignent d'une politique réaliste et volontariste à l'égard des menaces, elles doivent être lues à la lumière de leur portée véritable.

Les réformes opérées n'ont d'intérêt qu'à la condition de réellement consolider, d'une part, les règles de prévention des atteintes aux AIV et, d'autre part, celles applicables à la résilience en cas de crise.

(3) Complété par l'arrêté du 2 juin 2006 (modifié par l'arrêté du 3 juillet 2008) fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs

(4) Activités civiles de l'État ; activités militaires de l'État ; activités judiciaires ; espace et recherche ; santé ; gestion de l'eau ; alimentation ; énergie ; communication, électronique, audiovisuel et information ; transports ; finances ; industrie. On compte environ 250 opérateurs d'importance vitale.

(5) Bockel (J.-M.), 2012, Rapport d'information sur la cyberdéfense, Sénat, n° 681.

(6) Watin-Augouard (M.), 2013, « Le droit s'adapte aux exigences de la cybersécurité », *Rev. gendarmerie nationale*, n° 48, p. 92.

(7) Instruction interministérielle relative à la sécurité des activités d'importance vitale, 7 janvier 2014.

(8) Commission européenne, 7 février 2013, « Un cyberspace, ouvert, sûr et sécurisé ».

(9) Pauvert (B.), 2015, « L'entreprise et la sécurité nationale », in Gohin (O.), Pauvert (B.) (éd.), *Le droit de la sécurité et de la défense en 2014*, Marseille, PUAM, p. 183.

## La consolidation de la prévention des atteintes aux AIV

La protection des AIV bénéficie de quelques années de recul et d'une intense réflexion internationale sur le sujet, la quasi-totalité des démocraties libérales disposant d'un droit applicable aux infrastructures essentielles. Tout en confirmant les principes en vigueur depuis 2006, le droit positif innove sur plusieurs points.

### La confirmation des principes

Le niveau institutionnel auquel se traite la sécurité des AIV témoigne de l'importance que l'État attache au sujet. Le suivi des AIV appartient au Premier ministre. Un tel choix est doublement justifié. D'une part, il est conforme aux prérogatives de police administrative du Premier ministre ; d'autre part, il exige une coordination interministérielle, notamment pour l'identification des secteurs concernés (avis de la commission interministérielle de défense et de sécurité des secteurs d'AIV), et leur suivi par un ministre coordonnateur. Ce dernier élabore les directives sectorielles, identifie les opérateurs d'importance vitale (OIV) et assure le suivi des plans élaborés par les opérateurs.

Depuis 2006, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) pilote la gestion des AIV et, plus concrètement, des OIV. Il administre la base de données d'importance vitale (DIVA).

L'administration centrale n'est pas la seule concernée. L'encadrement des AIV passe aussi par une implication des échelons déconcentrés en raison de leur proximité avec la plupart des OIV. Les commissions zonales des secteurs d'activité d'importance vitale contribuent à l'identification des OIV. Ce domaine relevant de la défense non militaire, le préfet de zone dirige l'action des préfets de département (article R 122-5 du Code de la sécurité intérieure), lesquels ont particulièrement la charge de répondre aux demandes d'avis des OIV sur les personnes autorisées à accéder aux points d'importance vitale (PIV). Cette coopération indispensable compense l'incapacité juridique des opérateurs d'enquêter directement sur les individus.

Il convient, également, de signaler l'implication des référents sûreté de la gendarmerie nationale,

particulièrement sensibilisée au titre de son action en direction de l'intelligence économique.

Sur le fond, la France a fait le choix d'un système contraignant. Contrairement à d'autres États (en particulier l'Allemagne), le volontariat des acteurs privés n'est pas le moteur de la protection. L'État ne se contente pas de proposer des outils, il les impose aux entreprises privées dans le cadre d'un partenariat, en tout état de cause, déséquilibré.

À partir des instructions nationales (directives nationales de sécurité), les OIV élaborent un Plan de sécurité opérateur (PSO), et des plans particuliers de protection (PPP). De leur côté, les préfets ont la charge des plans de protection externe (PPE). Tous font passer la réflexion du niveau stratégique au niveau tactique. Après l'identification de points névralgiques (points d'importance vitale), parmi lesquels les infrastructures de communication en réseau, les opérateurs construisent leurs réponses de sécurité. L'application des DNS les incite, par voie de conséquence, à un utile travail de réflexion.

Pour l'approbation de leur projet de plan particulier de protection, les OIV le transmettent aux autorités (préfet de département ou aux autorités militaires) qui statuent dans un délai de six mois.

Les entreprises tirent les conséquences de l'identification des menaces et ont l'obligation de prendre les mesures utiles (article L 1332-4 à 6 du Code de la défense). La protection des sites implique la création de services internes de sécurité et le recours à des prestataires d'activités privées de sécurité. Pour établir le lien avec les pouvoirs publics, elles nomment des délégués pour la défense et la sécurité de l'OIV.

Les opérateurs s'appuient aussi sur des structures étatiques dédiées. Dans le prolongement du *Livre blanc* de 2008, la France a créé l'Agence nationale de la sécurité des systèmes d'information<sup>10</sup>. Placée auprès du SGDSN, elle accompagne les OIV, et est compétente en matière de qualification des prestataires de services de confiance et des produits de sécurité<sup>11</sup>. L'ANSSI participe, par ailleurs, à la coopération internationale sur le sujet.

Si les cybermenaces retiennent l'attention, elles n'occultent pas les dangers plus traditionnels. À ce titre, la protection des sites industriels n'est pas négligée et les obligations des opérateurs rappelées par la puissance publique. À

(10) Décret n° 2009-834 du 7 juillet 2009.

(11) Décret n° 2010-112 du 2 février 2010.

la suite d'actions violentes, le Gouvernement a élaboré une instruction datée du 30 juillet 2015 relative au renforcement de la sécurité des sites Seveso contre les actes de malveillance<sup>12</sup>, ce qui comprend éventuellement des PIV<sup>13</sup>. En plus des autoévaluations par les industriels concernés, les actions préventives nécessitent un renforcement des contrôles sur site par l'inspection des installations classées et, pour les PIV, par la commission zonale de sécurité. Les contrôles permettent de s'assurer du respect des réglementations en vigueur et de la fiabilité des plans particuliers de protection (à la charge des entreprises) et des plans de protection externe (à la charge des préfets). Parallèlement, un exercice par zone de défense et de sécurité complète l'ensemble.

Ce cadre a été progressivement modifié et fait l'objet de différentes innovations.

### Les innovations apportées

La prise en considération des AIV fait évoluer les relations entre la puissance publique et les opérateurs privés, exposés à des menaces communes.

Afin de poursuivre le décloisonnement, l'État a apporté une réponse institutionnelle en créant, fin 2014, la fonction de préfet chargé de la lutte contre les cybermenaces<sup>14</sup>. Parmi ses axes de travail et dans une logique interministérielle, le préfet Latournerie travaille sur l'identification actualisée des menaces et le renforcement des capacités de réponse, ainsi que sur l'amélioration de la prévention dans les entreprises.

Parallèlement et depuis 2012, la sensibilisation aux cybermenaces concerne les citoyens eux-mêmes. À cette fin, une réserve citoyenne cyberdéfense a été constituée avec notamment la mission de sensibiliser les entreprises.

Dans un registre plus spécifique, la loi de programmation militaire pour la période 2015-2019 confirme l'attention particulière portée aux AIV relevant des « activités militaires de l'État » et des « activités industrielles de l'armement ».

À cette fin, l'État peut compter sur la direction de la Protection des installations, moyens et activités de la défense (DPID) créée par décret du 19 août 2015 (décret 2015-1029) après quelques mois de fonctionnement

informel. Conformément à l'article 1<sup>er</sup> du texte, la Direction est compétente à l'égard des installations intéressant la défense nationale, qu'elles relèvent ou non du ministère de la Défense. À ce titre et sous l'autorité directe du ministre de la Défense, elle « *élabore et propose au ministre de la Défense la politique de protection des installations, des moyens et des activités de la défense. Elle en supervise la mise en œuvre* » (article 5). Dans le cas des AIV, elle supervise l'élaboration et l'actualisation des référentiels de menaces dont le ministre de la Défense est le ministre coordonnateur. Elle s'assure du respect de ces référentiels et rend des avis sur les plans particuliers de protection (article 6) mentionnés à l'article L 1332-3 du Code de la défense.

Là où la direction de la Protection et de la Sécurité de la défense (DPSD) évalue et prévient la menace, et participe à la recherche des atteintes (article D 3126-6 du Code de la défense), en appartenant à la communauté du renseignement, la DPID élabore et coordonne la politique de protection. Si les sphères sont apparemment distinctes et les missions de nature différente, il sera intéressant d'observer les relations entre les deux services.

Les créations n'excluent pas les suppressions. Ainsi, le Comité national des SAIV a été abrogé par le décret 2014-132 du 17 février 2014 portant suppression de commissions administratives à caractère consultatif. Il était présidé par le secrétaire général de la défense et de la sécurité nationale, et conçu comme une instance d'échanges entre la sphère publique et la sphère privée. Comme le soulignait la réponse à une question ministérielle, il était pourtant « *la seule instance d'échanges de haut niveau existante entre la puissance publique et des dirigeants d'opérateurs privés qui constituent un panel représentatif des secteurs d'activité d'importance vitale et dont les décisions stratégiques sont susceptibles d'avoir des conséquences sur la sécurité de la Nation*<sup>15</sup> ». Sacrifié sur l'autel de la simplification administrative, il souffrait sans doute d'un positionnement à un niveau trop global.

Surtout, la loi de programmation militaire de 2013 a renforcé les dispositions spécifiques à la sécurité des systèmes d'informations (articles L 1332-6-1 à 6 du Code de la défense). Intervenue dans un contexte de grande inégalité dans la perception des dangers par les entreprises, elle traduit la détermination de l'État à faire prendre conscience aux entreprises des enjeux, y compris par le biais d'obligations.

(12) Instruction DEVP1518240J.

(13) Le Gouvernement a d'ailleurs amorcé le classement de nouveaux sites Seveso en PIV.

(14) Décret du 4 décembre 2014.

(15) Question n° 9927, réponse publiée dans le JOAN du 28 mai 2013, p. 5483.

L'article L 1332-6-1 confirme le rôle du Premier ministre et accentue ses prérogatives de police administrative<sup>16</sup>. Il peut, en effet, imposer des règles de sécurité organisationnelles ou techniques. Comme l'ont mis en évidence les travaux préparatoires de la loi, les mesures sont adaptées à chaque secteur et permettent, par exemple, de renforcer les moyens de détection des attaques informatiques. Il revient à l'Agence nationale de sécurité des systèmes d'information d'assister le Premier ministre dans l'élaboration des règles de sécurité des « systèmes d'information d'importance vitale » et les entreprises dans la manière d'y faire face.

De plus, la loi renforce les capacités d'audit et de contrôle des systèmes d'information, déclenchés par le Premier ministre (article L 1332-6-3 du Code de la défense), en restant à la charge des opérateurs. De la sorte, le code étend aux AIV une disposition déjà applicable aux opérateurs de communications électroniques.

Cette disposition renforce les capacités existantes d'audits par des services ministériels dédiés (exemple du Bureau des exercices et inspections des OIV), à l'initiative des préfets de département en application des orientations fixées par la commission interministérielle. Les commissions zonales sont, elles aussi, compétentes pour déclencher des inspections. Les visites sont annoncées conformément à l'esprit de partenariat qui doit présider aux relations entre les différents acteurs. Des sanctions pénales peuvent être infligées aux entreprises en application de l'article L 1332-7 du Code de la défense qui ne respectent pas leurs obligations. Les entreprises récalcitrantes sont ainsi passibles de fortes amendes (150 000 euros).

Tout en étant bien établi, l'environnement juridique des AIV n'est pas exempt d'interrogations.

La première est liée à la définition des AIV. Opter pour une conception trop large fait courir un risque d'éparpillement quand, à l'inverse, une vision trop précise peut conduire au blocage.

Une autre renvoie à l'éclatement du droit applicable. Les dispositions relatives aux AIV sont contenues dans le Code de la défense mais, plus largement, les cybermenaces concernent plusieurs autres codes (Code des postes et des communications électroniques, Code de la sécurité intérieure, Code de la propriété intellectuelle, Code monétaire et financier). Faute d'un Code de

la sécurité nationale, cette sédimentation perdurera vraisemblablement longtemps.

En outre, dans des secteurs ouverts à la concurrence, la désignation des OIV se doit d'être la plus transparente possible. Cette transparence est néanmoins susceptible de se heurter aux règles relatives au secret et, plus généralement, aux échanges d'informations entre les entreprises et les services de l'État. L'identification des OIV est d'autant plus importante qu'elle implique un coût pour eux et, par voie de conséquence, de possibles distorsions de concurrence avec les autres entreprises déchargées d'obligations aussi contraignantes tout en intervenant dans des domaines proches. Les obligations réglementaires relatives à la protection des systèmes d'information sont, à cet égard, exemplaires.

Dès lors, les entreprises pourraient être tentées de sous-évaluer les risques ou d'opter pour des méthodes de protection minimale. Ainsi, la norme est efficace à la condition d'être suivie des financements nécessaires à sa concrétisation. En l'état actuel des choses, la charge financière repose exclusivement sur les entreprises à partir de scénarios lourds identifiés par l'État. La possibilité reconnue par l'État<sup>17</sup> de déduire du résultat imposable de l'entreprise les charges exposées dans l'intérêt direct de l'exploitation (article 39 du Code général des impôts) n'est peut-être pas une compensation suffisante.

L'existence d'OIV pose, aussi, la question de leurs sous-traitants et prestataires de services. Il est demandé aux opérateurs d'inclure dans les contrats les dispositions garantissant la prise en compte de l'existence d'une AIV. L'État est pragmatique en ne s'immiscant pas directement dans les relations contractuelles. Il privilégie, au contraire, la responsabilisation des donneurs d'ordres.

Enfin, les menaces pesant sur des sites industriels obligent à repenser les moyens disponibles pour leur sécurisation. La seule présence de moyens publics est inconcevable. Mais, parallèlement, le recours à des moyens humains

*Ainsi, la norme est efficace à la condition d'être suivie des financements nécessaires à sa concrétisation. En l'état actuel des choses, la charge financière repose exclusivement sur les entreprises à partir de scénarios lourds identifiés par l'État.*

(16) Le décret 2015-351 du 27 mars 2015 en assure la mise en application avec des arrêtés sectoriels.

(17) Réponse du ministre des Finances en date du 11 août 2015 (JO p. 6167) à la question du député Bourdoux en date du 4 novembre 2014 (JO p. 9213).

privés (services internes et/ou prestataires de services) laisse sceptique. Les prérogatives accordées et la formation des personnels obèrent leur capacité à faire obstacle à une attaque terroriste. Utile pour détecter une intrusion grâce notamment à des moyens technologiques, la sécurité privée n'est pas nécessairement en mesure de réagir efficacement.

Prévenir la crise a pour corollaire la préparation des moyens afin de la surmonter si elle vient à se produire. Dans le cas des AIV, la puissance publique et le secteur privé disposent de capacités diversifiées afin de réagir, conformément au principe de résilience.

## La consolidation de la résilience des atteintes aux AIV

La prévention, aussi poussée soit elle, ne met pas totalement à l'abri les opérateurs. L'article L 2151-4 du Code de la défense impose aux opérateurs contribuant à la sécurité nationale de disposer de plan de continuité et de rétablissement de l'activité.

Tout comme la prévention, les réponses à une crise s'inscrivent dans des obligations partenariales. Si la puissance publique est en première ligne, la résilience passe aussi par l'action des entreprises.

### Les moyens publics

La résilience justifie la mobilisation des capacités institutionnelles et opérationnelles de l'État à l'échelon central comme dans les échelons déconcentrés.

La remise en état de fonctionnement des services d'importance vitale est conditionnée par la réactivité des acteurs publics. Dans le cas des atteintes touchant aux réseaux de communication numérique, la réactivité est justifiée par l'interdépendance des systèmes et par la solidarité des acteurs. Sur ce point, le rôle de l'ANSSI est crucial en collectant les données d'incidents facilitant la réponse et la recherche de victimes en cascade. Dans un tel cas, la garantie de l'anonymat des victimes est un élément essentiel pour les inciter à respecter leurs obligations de notification. Un plan « Piranet » organise la coopération entre l'État et les opérateurs.

Le ministère de l'Intérieur a un rôle central et s'appuie sur les préfets de zone ainsi que sur les préfets de département.

Le droit institutionnel a évolué en direction d'un renforcement continu des prérogatives des préfets de zone<sup>18</sup>. Le préfet de zone coordonne l'action des préfets des départements de sa zone dans une situation de crise ou d'événement d'une particulière gravité, et lorsque cela dépasse le cadre d'un département.

Le décret 2014-96 du 6 mars 2014 accentue le rôle de coordination de la zone en créant les Secrétariats généraux pour l'administration du ministère de l'Intérieur (SGAMI) qui remplacent les Secrétariats généraux pour l'administration de la police. Conformément à l'objectif de rationalisation du ministère de l'Intérieur, les SGAMI contribuent à mutualiser les fonctions de soutien des services et unités de la sécurité intérieure et à faire de l'échelon zonal celui de droit commun pour la mise en œuvre des fonctions support de la police et de la gendarmerie, sous l'autorité du préfet de zone de défense et de sécurité.

Tout cela contribue à garantir les capacités de réaction des forces de sécurité intérieure, lesquelles doivent entretenir avec les opérateurs privés des relations suffisamment étroites pour pouvoir adapter leur dispositif à la particularité des sites.

Le préfet de département, y compris dans le cas des AIV, peut mobiliser ses moyens traditionnels dans le cadre du plan Orsec départemental. En cas de crise grave, l'état d'urgence (loi 55-385 du 3 avril 1955) permet au préfet de déterminer les zones d'importance vitale et les PIV faisant l'objet de restrictions de séjour ou de circulation.

Parce que l'État est décentralisé, le regard se tourne aussi vers les maires en raison de leur proximité avec les populations et de leurs traditionnels pouvoirs de police. À la fois représentants de l'État dans la commune et exécutifs de la collectivité territoriale, ils sont des relais indispensables en cas de crise. Disposant parfois de solides services municipaux, voire de polices municipales, ils ont une réelle capacité d'action. Cette dernière pourrait d'ailleurs être consolidée par une utilisation plus performante des réserves communales de sécurité civile<sup>19</sup>, encore trop discrètes et cantonnées à la lutte contre les incendies.

En cas de crise, il est assez fréquent que les moyens civils bénéficient du renfort des moyens militaires. La remise

(18) Gohin (O.), 2001, « Le préfet de zone de défense », *RDP*, p. 1369 ; Renaudie (O.), 2014, « Le préfet de zone de défense et de sécurité : quelles (r)évolutions ? » in Vallar (C.), Latour (X.) (dir.), *Le droit de la sécurité et de la défense en 2013*, p. 79.

(19) Latour (X.), 2006, « Les nouveaux instruments communaux au service de la sécurité civile », *BJCL*, février, p. 82

en état des services n'échapperait pas à cette constante. Les capacités de réaction militaires peuvent être de plusieurs sortes et nécessitent d'être coordonnées avec les moyens civils.

Pour ce qui concerne les réseaux de communication numérique, deux capacités de réaction sont principalement évocables.

D'une part, les armées ont une pratique bien rôdée de la sécurisation de leurs équipements électroniques et réseaux de communication. La guerre électronique fait partie intégrante des éléments constitutifs de leur savoir-faire. Ingérence et contre-ingérence sont développées par des services spécialisés pouvant mettre leur expérience à la disposition des OIV. Dans un même ordre d'idées, les forces de sécurité intérieure ont développé de réelles capacités de lutte contre la cybercriminalité, qui sont utilisables au profit de la protection des AIV.

D'autre part, les forces armées disposent de réseaux de communication sécurisés et distincts des réseaux civils. Les réseaux militaires protégés, en particulier celui de la gendarmerie, permettraient de préserver la continuité de l'action de l'État et de faciliter le retour à la normale. Au pire, le recours à des moyens plus traditionnels (type transmission radio) n'est pas impensable. Par conséquent, il est essentiel d'entretenir plusieurs réseaux sûrs, éventuellement étendus aux OIV afin de limiter les risques de concentration des moyens entre les mains d'opérateurs privés, eux-mêmes confrontés à des risques de rupture.

La gestion de crise passe par une combinaison de moyens. Grâce notamment à des circuits d'alerte et d'information efficaces<sup>20</sup>, les moyens publics sont renforcés par des moyens privés.

### Les moyens privés

Pour ce qui concerne les capacités privées, la réquisition demeure la règle. Parallèlement, dans le prolongement des AIV, la formation des hommes et la préparation des entreprises demeurent des conditions de base d'une réaction performante. À ce titre, le cadre légal et réglementaire de l'État est complété par la normalisation internationale, comme en témoigne la norme ISO 22301 sur la continuité de l'activité, adoptée le 15 mai 2012.

L'une des principales exigences est d'améliorer la circulation de l'information entre la puissance publique et les opérateurs privés.

La LPM (article L 1332-6-2 du Code de la défense) a créé une obligation d'information « sans délai » d'incidents affectant le fonctionnement ou la sécurité des systèmes d'information des OIV.

De la sorte, l'ANSSI dispose des éléments lui permettant de cerner l'ampleur et les caractéristiques d'une attaque pour informer les autres opérateurs concernés. À l'effort de coordination motivé par l'interconnexion des réseaux s'ajoute la volonté de pallier la discrétion (voulue ou pas) des opérateurs, lesquels ont parfois du mal à admettre avoir fait l'objet d'une attaque.

Par ailleurs, l'article L 1332-6-4 du Code de la défense autorise le Premier ministre à imposer aux opérateurs la prise de contre-mesures en cas de crise majeure.

Nul doute que cela se ferait par l'intermédiaire de l'ANSSI et prendrait, par exemple, la forme d'une déconnexion. Comme l'ont également mis en évidence les travaux préparatoires, cette disposition a aussi pour portée d'exonérer les OIV de leurs responsabilités vis-à-vis de leurs clients.

En outre, la sécurisation des sites des OIV implique des opérateurs privés de sécurité. Ces derniers ne verraient pas leurs missions se limiter à des actions préventives. Au contraire, étant au cœur de la crise, il serait normal de les associer à sa résolution.

Ainsi, c'est une profonde mutation des sociétés de sécurité privée qui est engagée. Les missions qui leur sont confiées se complexifient et se diversifient. Non seulement la sécurité n'est plus appréhendée comme le monopole de la puissance publique, mais encore, elle se dématérialise sous l'effet des réseaux de communication numérique. Par voie de conséquence, les sociétés privées de sécurité n'ont plus seulement à sécuriser des enceintes, elles doivent acquérir des capacités d'anticipation et de réaction face aux atteintes de différentes natures sur des réseaux.

Par ailleurs, le recours à des moyens humains complémentaires (aux côtés des réservistes, en particulier la réserve de sécurité nationale, articles L 2171-1 et s. du Code de la défense) pourrait compenser les pertes éventuelles d'effectifs dans les services de l'État.

La résilience suppose, enfin, la mobilisation des moyens de l'entreprise elle-même. À ce titre, la loi 2011-892 du 27 juillet 2011 a créé un service de sécurité nationale (article L 2151-1 et s. du Code de la défense<sup>21</sup>). Annoncées pour

(20) Notamment sur le fondement de l'article R 741-1 CSI pour les sites Seveso.

(21) Cléach (M.-P.), 2014, Rapport d'information sur la loi 2011-892, Sénat, n° 725, 15 juillet.

la fin de l'année 2014, les mesures d'application ont été prises par le décret 2015-508 du 7 mai 2015 relatif au service de sécurité nationale et au dispositif de réserve de sécurité nationale, dans le prolongement des articles L 2151-1 (service de sécurité nationale) et L 2171-1 du Code de la défense (réserve de sécurité nationale). Le premier autorise le Premier ministre à obliger par décret les salariés de certaines entreprises (par exemple, celles dotées d'un plan de continuité d'activité ou exploitant d'une activité d'importance vitale) à rester à leur poste ou à le rejoindre. L'autre permet la mobilisation par décret du Premier ministre en cas de crise grave de réservistes dans des conditions dérogatoires au droit commun (allongement de la période d'activité de 30 jours consécutifs, renouvelable une fois).

Le service de sécurité nationale oblige l'OIV à identifier les personnels concernés et à tenir ces informations à la disposition des autorités. En cas de déclenchement sur tout ou partie du territoire, pour des entreprises identifiées et une durée fixée par le Premier ministre, le personnel a trois jours pour rejoindre son poste.

La loi 2015-918 actualisant la programmation militaire pour la période 2015-2019 parachève le dispositif en accordant un régime particulier aux OIV. Sur demande de l'employeur, les réservistes peuvent être dégagés de leurs obligations si leur présence est nécessaire à la poursuite de la production de biens ou de services ou à la continuité du service public, *a fortiori* dans un contexte de crise (article 4221-4-1 du Code de la défense).

La conception française des AIV cherche à concrétiser une évolution en profondeur des rapports entre la puissance publique et les entreprises en matière de sécurité globale. La démarche ne manque pas d'ambition tant en matière de prévention des atteintes que des moyens de réaction. Tous les acteurs concernés paraissent avoir compris la nécessité de ne pas se contenter d'une construction intellectuelle intéressante pour passer à un stade opérationnel efficace ■

# Entre guerre et affaires

## Pourquoi les doctrines militaires inspirent souvent le monde des affaires

Jelle JANSSENS, Veerle PASHLEY, Marc COOLS

Sun Tzu, Carl von Clausewitz, Winston Churchill, Norman Schwarzkopf, David Petraeus... Autant de noms célèbres qui ont un point commun : ce sont tous de grands penseurs militaires qui ont influencé la vision de la guerre et de la politique à leur époque et bien au-delà. Leurs idées n'ont pas seulement eu un impact sur les experts militaires et politiques, mais aussi sur les dirigeants d'entreprise et managers dans différents domaines du marché. Du moins, c'est ce que l'on suppose. Dans cette contribution, nous chercherons à répondre à la question suivante : pourquoi les doctrines et idées militaires inspirent-elles souvent le monde de l'entreprise ?

Cette recherche d'une réponse plongera le lecteur dans l'histoire du concept de stratégie, dans l'exploration des processus stratégiques clés, dans l'analyse d'opérations militaires et économiques ainsi que dans l'étude des principes édictés par le grand sage et philosophe chinois Sun Tzu.

### Introduction

« Si ton ennemi t'est supérieur, évite-le. S'il est coléreux, irrite-le. À forces égales, affronte-le. Sinon, romps et réévalue. »  
[Bud Fox, *Wall Street*, 1987]

Dans le film *Wall Street*, un classique des années 1980 mettant en scène un jeune courtier en bourse qui veut faire ses armes chez un grand investisseur, Bud Fox – le personnage joué par Charlie Sheen – paraphrase Sun Tzu, le général philosophe chinois supposé avoir

rédigé le célèbre ouvrage *L'Art de la Guerre*. Ce traité, qui date du V<sup>e</sup> siècle avant J.-C., contient des consignes et des concepts philosophiques destinés à gagner des batailles et des guerres. Le livre a connu une première grande vague de succès dans le milieu des affaires à la fin des années 1980 grâce, entre autres, au film *Wall Street*, mais aussi à l'esprit de l'époque [Cantrell, 2004]. Les années 1980 étaient la décennie de Ronald Reagan et Margaret Thatcher, dont la politique économique était fortement influencée par les idées économiques de l'École de Chicago dirigée par Milton Friedman, qui privilégiait le côté « offre » de l'économie et voulait diminuer l'influence de l'État [Frazer, 1982]. Dans un article rédigé dans le *New York Times*, Friedman déclare que la responsabilité (sociale) d'une entreprise consiste à chercher à augmenter ses bénéfices [Friedman, 1970].

Jelle JANSSENS



Professeur du département de la criminologie, le droit pénal et le droit social, Université de Gand.

Veerle PASHLEY



Assistant au sein du groupe de recherche en droit pénal et criminologie, Université de Gand.

Marc COOLS



Professeur au sein du groupe de recherche en criminologie, Vrije Universiteit Brussel, et du groupe de recherche en droit pénal et criminologie, Université de Gand.



Le dirigeant d'entreprise sait ainsi quelle est sa mission : maximiser le profit. Pour atteindre cet objectif dans un environnement économique concurrentiel, des stratégies et idées militaires comme celles formulées dans *L'Art de la Guerre* peuvent s'avérer bien utiles. La forte économie japonaise incite par ailleurs les dirigeants d'entreprise à s'inspirer de l'Extrême-Orient [Ping, n.d.].

Dans le film, le jeune Bud Fox applique les anciennes sagesse militaires chinoises à un marché concurrentiel caractérisé par des « rachats hostiles » : connais « l'ennemi » et connais-toi toi-même. Il s'agit donc de connaître non seulement les forces et les faiblesses de sa propre organisation, mais aussi celles de l'ennemi. Une stratégie est ensuite formulée en s'appuyant sur cette analyse interne et externe. Des analyses SWOT, donc... mais en plus, Sun Tzu donne des directives stratégiques, et c'est justement là que se cache tout l'attrait du livre.

Rick Wartzman, directeur général du Drucker Institute, a un jour écrit dans le célèbre magazine économique américain *Forbes* : « *Demandez à des hommes d'affaires de citer l'auteur dont la pensée se reflète le mieux dans le monde militaire et celui des entreprises, et il y a de fortes chances pour que vous entendiez le nom de Sun Tzu* » [Beyer, 2014]. Le site CEO.com a d'ailleurs inséré le célèbre traité dans la liste des 23 ouvrages de *leadership* à lire absolument avant de mourir [*Ibid.*], indiquant que les notions militaires exposées

dans cet ouvrage sont un excellent guide de stratégie, de tactique et de succès dans le monde des affaires [CEO.com, 2013]. L'utilisation fréquente de ces notions dans le monde économique se reflète dans l'offre abondante d'ouvrages de management évoquant le philosophe : *Sun Tzu : Strategies for Marketing — 12 Essential Principles for Winning the War for Customers* ; *Sun Tzu for Women: The Art of War for Winning in Business* ; *The Complete Sun Tzu for Business Success : Use the Classic Rules of The Art of War to Win the Battle for Customers and Conquer the Competition* ; *Sun Tzu — The Art of War for Managers : 50 Strategic Rules Updated for Today's Business* ; *Sun Tzu and the Art of Business : Six Strategic Principles for Managers* ; etc.

Impossible de nier, donc, que *L'Art de la Guerre* a eu et a peut-être toujours de l'influence sur les dirigeants d'entreprise. Mais ce traité n'est pas un cas isolé. De toute évidence, diverses branches de la littérature académique (consacrée au management) se réfèrent régulièrement à des doctrines, concepts et stratégies militaires. Et ce, aussi bien dans le domaine du management stratégique [Mintzberg, 1987 ; 1990] que dans ceux de la gestion des ressources humaines [Lengnick-Hall & Lengnick-Hall, 1988], de la gestion de projets [Shenhar, 1998 ; Payne & Turner 1999], du développement des plans d'entreprise [Branch, 1957 ; Mintzberg, 1994 ; Honig 2004], du développement de l'organisation [Feld, 1959 ; Rutner, 2012], du *team-building* [Cannon-Bowers, Salas *et al.* 1993 ;

Albanese, 1994] et du leadership [Wong, Bliese *et al.*, 2003]. Tous ces domaines empruntent des idées et des principes au monde militaire pour rendre le monde des affaires plus efficace et plus performant. Internet propose lui aussi d'innombrables renvois à ces deux mondes. YouTube, par exemple, montre toute une série de vidéos dans lesquelles d'(anciens) experts militaires partagent leurs expériences avec des hommes d'affaires ou dans lesquelles le monde des affaires est expliqué d'un point de vue militaire (voir ex. TEEX 2013).

Bref, les entreprises modernes ont, dans une large mesure, emprunté les idées de management, méthodes organisationnelles et autres concepts de leadership au management militaire [Hadjiphanis, 2010]. Le jargon militaire a, lui aussi, fait son entrée dans le monde des entreprises. Exemples : le terme « headquarter » (qui désigne le siège social d'une entreprise), les systèmes de gestion des processus de production, les stratégies d'entreprise [Farrell & DeRose, 2000]. Il nous a été demandé dans le cadre de la présente contribution de réfléchir aux raisons pour lesquelles les doctrines militaires inspirent souvent le monde des affaires. Pour ce faire, nous allons examiner d'où vient ce lien et nous allons explorer les éléments pouvant expliquer les parallèles et les analogies entre ces deux mondes. Enfin, nous nous attarderons sur les principes de Sun Tzu, la manière dont ceux-ci se sont infiltrés jusque dans la littérature consacrée au management et les idées qu'ils peuvent proposer au monde des affaires.

## Le lien historique : la stratégie

Les armées et les entreprises ont un point commun : réussir. Gagner une guerre ou diriger une entreprise dépend de l'environnement, des circonstances, de la mission et des objectifs... qui sont remplis différemment, bien sûr : là où une armée se bat avec l'ennemi et remporte des batailles, une entreprise cherche à avoir un avantage concurrentiel sur le marché [Hadjiphanis, 2010]. La durabilité d'une organisation est souvent exprimée en termes de réussite ou de rendement. Pour réaliser ces objectifs fondamentaux, les organisations ont, d'après les livres de management, besoin d'une stratégie s'articulant autour de quatre axes : les objectifs de l'entreprise, son environnement, les moyens dont elle dispose et la manière de distribuer ces moyens et, enfin, la culture d'entreprise avec ses valeurs et ses normes [Heene, Van Looy *et al.*, 2003]. Ces éléments sont très proches des cinq principes fondamentaux présentés par Sun Tzu comme déterminants dans une victoire militaire : les conditions climatiques, les conditions géographiques, le dirigeant, l'organisation et la discipline, et l'autorité morale [Sun Tzu, 2008].

S'il faut chercher quelque part un lien entre les entreprises et les organisations militaires, c'est dans la manière dont les premières sont dirigées. C'est le concept de « stratégie » qui permet de faire le lien entre les doctrines militaires et le monde des affaires. Le mot « stratégie » vient du grec *strategos*, ce qui signifie chef, commandant, général. Le verbe grec *strategeo* veut dire conduire, diriger une armée, mais aussi utiliser un stratagème [Bartelink, 1966]. En d'autres termes, engager les moyens avec un maximum d'efficacité en vue d'atteindre un objectif. Le concept de stratégie, utilisé aussi bien dans son contexte militaire que politique, est resté au premier plan tout au long de l'Histoire et a été abordé par de grands auteurs tels que Shakespeare, Montesquieu, Kant, Mill, Hegel, Clausewitz et Tolstoï. Les concepts stratégiques imaginés par ces auteurs ont été utilisés par de nombreux théoriciens militaires et politiques comme Machiavel, Napoléon, Bismarck, Yamamoto et Hitler [Bracker, 1980].

Le premier exemple connu d'une stratégie appliquée au monde des affaires est celui de Socrate conseillant Nichomachides, un militaire grec qui venait de perdre une élection au poste de général. Socrate compara les obligations d'un général avec celles d'un homme d'affaires et démontra à Nichomachides la nécessité, dans les deux cas, de planifier l'usage des moyens pour atteindre ses objectifs. Selon Bracker [1980], cette notion s'est cependant perdue au moment de la chute des cités grecques pour ne réapparaître qu'après la révolution industrielle. Une assertion confirmée par Freedman [2013], qui situe l'introduction du concept de stratégie tel que nous le connaissons aujourd'hui à la fin du XVIII<sup>e</sup> siècle, introduction due au Siècle des Lumières, mais aussi à l'impact des guerres napoléoniennes sur la pensée militaire et politique de l'époque. La stratégie était considérée comme une solution permettant d'entremêler « art » militaire et objectifs politiques [Economist, 2013]. Ou, comme l'a affirmé Carl von Clausewitz : « *la guerre n'est pas seulement un acte politique mais aussi un véritable instrument politique, elle est la continuation de la politique par d'autres moyens* » [von Clausewitz, 1989, p. 87].

Pendant la deuxième révolution industrielle, différentes écoles de management élitistes ont été fondées aux États-Unis, comme la Wharton School en 1881. C'est la Harvard Business School, fondée en 1908, qui a été une des premières institutions à promouvoir l'idée de la nécessité, pour les futurs dirigeants, d'adopter une pensée stratégique et de ne pas se contenter d'être des gestionnaires d'entreprise fonctionnels [Ghemawat, 2002].

La nécessité de disposer d'une stratégie dans le monde des affaires gagne en importance après la Seconde Guerre mondiale, quand le monde assez stable des

affaires se transforme en un environnement concurrentiel en rapide évolution. Deux facteurs sont attribués à cet environnement versatile : d'une part, les grands changements qui surviennent au sein des entreprises et, d'autre part, l'application accélérée des sciences et des technologies [Ansoff, 1969]. Ces changements plus rapides encouragent la naissance d'une nouvelle possibilité : anticiper le changement, profiter de nouvelles opportunités et entreprendre des actions à temps pour éviter les situations susceptibles de menacer l'organisation [Bracker, 1980]. En d'autres termes, c'est un avenir de plus en plus incertain qui a entraîné la réintroduction du concept de stratégie dans le monde des entreprises. Les premiers auteurs modernes à avoir associé cette stratégie au monde des affaires sont Von Neumann et Morgenstern [1947]. D'autres auteurs tels que Drucker, Chandler et Mintzberg ont développé des concepts de stratégies d'entreprise dans les 50 à 60 dernières années [Bracker, 1980]. C'est également pendant cette période que l'on constate une évolution au sein de la pensée stratégique. Dans les années 1950, on réfléchit à l'adéquation d'une entreprise au monde concurrentiel du moment ; après les années 1950, il s'agit de guider [diriger] l'entreprise au moyen d'objectifs clairement formulés [*management by objectives*]. Dans les

années 1960, la pensée concurrentielle se traduit par l'introduction d'une analyse des forces et des faiblesses de l'organisation associée à ses opportunités et ses menaces, analyse qui sera ultérieurement mieux connue sous l'abréviation SWOT. C'est dans les années 1960-70 que sont apparues les pratiques de consultance stratégiques, notamment sous l'influence de l'innovation technologique et du dynamisme économique. Ces consultants introduisent entre autres la courbe d'expérience et les analyses de portefeuille. Au cours des années suivantes se sont développées diverses méthodes d'analyse consacrées à la pensée dynamique [options, gestion du changement], tout en se souciant des clients et des actionnaires. C'est seulement depuis la fin du XX<sup>e</sup> siècle que la stratégie est utilisée sciemment dans l'environnement des affaires et dans un contexte concurrentiel [Ghemawat, 2002].

La nécessité de disposer d'une stratégie dans le monde des affaires gagne en importance après la Seconde Guerre mondiale, quand le monde assez stable des affaires se transforme en un environnement concurrentiel en rapide évolution. Deux facteurs sont attribués à cet environnement versatile : d'une part, les grands changements qui surviennent au sein des entreprises et, d'autre part, l'application accélérée des sciences et des technologies

Freedman [2013] distingue trois types de stratégie. Premièrement, les « stratégies de force » qui se rapportent à la stratégie militaire : de von Clausewitz à la guerre asymétrique d'aujourd'hui. Deuxièmement, la « stratégie vue d'en bas » qui analyse les principes politiques et en particulier ceux des révolutionnaires du XIX<sup>e</sup> siècle comme Marx, qui se considéraient comme l'état-major général des opprimés. Et troisièmement, la « stratégie vue d'en haut » qui analyse le développement de la stratégie dans les entreprises. Ces trois types de stratégie ont un point commun : la stratégie est un moyen d'arriver à une victoire convaincante et donc à un résultat durable [Economist, 2013], ce dont Freedman doute très fort. Pour lui, en effet, il est nécessaire d'adapter les stratégies aux circonstances [Freedman, 2013]. Ainsi, Selon Keller [2008], bien que des plans de guerre soient méticuleusement préétablis, ils sont très rarement exécutés pendant le conflit exactement comme ils ont été projetés. Les organisations militaires et les entreprises n'opèrent pas dans un contexte statique ; elles doivent donc aussi adapter leurs stratégies à ces changements d'environnement.

## Deux mondes ou pas ?

Bien que la stratégie soit le concept qui relie le monde de la guerre et le monde des affaires, une question se pose : dans quelle mesure les idées et concepts de ces deux mondes sont-ils interchangeables ? Certains auteurs comme Hadjiphanis [2010] parlent d'un « lien de parenté » entre la guerre et la planification dans les entreprises. Keller [2008] reconnaît ce lien, mais ajoute que les doctrines et stratégies militaires ne sont pas forcément les seules sources d'inspiration des dirigeants d'entreprise. Des techniques de planification applicables au monde des affaires, écrit-il, peuvent également se rencontrer en cuisine, par exemple. Et celui-ci de se référer à *Isabella Beeton : Management Lessons From The Kitchen*, où Wesley [2004] avance une série d'éléments pertinents pour la vie économique moderne.

Bien que les dirigeants d'entreprise modernes puissent s'inspirer de différentes sources, l'analogie avec les organisations militaires semble dominer, surtout en matière de planification et de développement stratégique. C'est pourquoi il est important de tenter d'établir une distinction entre planification militaire et planification d'entreprise. Les deux peuvent-elles s'enchevêtrer ?

Là où la planification militaire consiste à préparer constamment les missions futures et à étudier tous les aspects des opérations militaires [Wong, Maher *et al.*, 1998], le management est un processus visant à planifier,

organiser, diriger et gérer les moyens en vue de réaliser les objectifs de l'organisation avec un maximum d'efficacité [Daft, 2013]. Selon Hadjiphanis [2010], ces deux définitions renferment des caractéristiques semblables qui se rapportent à des objectifs futurs et des processus visant des buts différents. Dans le monde militaire, le succès a souvent une autre signification que dans le monde des affaires. D'après Hadjiphanis [2010], la grande différence entre ces deux mondes réside dans le fait que les plans militaires se rapportent à des forces armées prêtes à combattre et gagner. Keller [2008] est du même avis, affirmant que le but fondamental d'un plan militaire est d'imposer les conditions du vainqueur au vaincu, bien qu'il reconnaisse l'existence d'autres buts : la saisie de biens étrangers, l'intimidation ou la construction d'une ligne de défense active en vue de protéger la frontière. Dans le monde des affaires, le succès peut être déterminé par l'achat d'un concurrent, la prise d'une part de marché, l'évitement d'une perte de parts de marché ou la protection d'une technologie [Keller, 2008]. En d'autres termes, dans le monde des entreprises le point de départ est le suivant : définir et mettre en œuvre divers plans et stratégies contribuant au succès de l'organisation sur le marché concurrentiel.

Bref, bien que le monde militaire et celui des entreprises soient fondamentalement différents en matière d'objectifs préétablis, il semble à première vue que stratégies et concepts puissent être partagés par ces deux mondes dans la mesure où ceux-ci ont des processus clés similaires (planification, formulation de stratégies, analyse de l'environnement et gestion des ressources).

Observateurs et analystes utilisent ce dénominateur commun pour établir des parallèles, effectuer des analogies et tirer les leçons de leurs activités réciproques. Et ce, à deux niveaux différents. Premièrement, au niveau de ce que l'on pourrait appeler « grand stratégies », c'est-à-dire les stratégies et doctrines globales qui gouvernent les activités militaires. Deuxièmement, au niveau de l'analyse des sous-processus qui font partie intégrante de ces stratégies et doctrines. Les processus décisionnels, l'information, la communication et le leadership, par exemple. Des « microanalyses » qui sont très proches des « principes » de guerre exposés dans *l'Art de la Guerre*.

## Guerre et affaires

Au premier niveau, donc, le type de guerre est analysé en vue d'établir des parallèles avec la vie en entreprise et d'en tirer des leçons, le plus important étant d'examiner les deux mondes de façon plus globale en s'attardant sur les interactions qui s'opèrent avec leur environnement.

Aujourd'hui, la lutte armée est à mille lieues de cette vision statique caractérisée par la présence d'un ennemi unique qui se fait anéantir grâce à une action spécifique décisive. La planification traditionnelle d'une guerre de position entre États avec des ennemis identifiés dans des zones géographiques bien définies alterne avec des guerres asymétriques, des conflits de faible intensité et des combats contre des acteurs non étatiques [Rushin, 2012].

Rushin [*Ibid.*] compare les stratégies d'entreprise avec les différents types de guerre. Et celui-ci de commencer par la guerre limitée. En guise d'exemple, Rushin évoque le conflit militaire entre les États-Unis et les sandinistes nicaraguayens, où les Américains ont utilisé une violence ciblée écrasante pour vaincre les sandinistes. Dans le monde des entreprises, l'auteur donne l'exemple de Microsoft qui, dans les années 1980 et 1990, a bloqué des fabricants de logiciels de moindre envergure à coups de brevets pour garantir sa position dominante sur le marché.

Un autre type de guerre, très privilégié ces derniers temps, est la contre-insurrection (*Counter-Insurgency*, en abrégé COIN). Elle a été utilisée par l'armée américaine dans sa lutte contre les talibans afghans. Comme une victoire définitive ne pouvait probablement pas être atteinte par le biais d'une guerre classique, une stratégie COIN a été utilisée pour empêcher le rassemblement de petits groupes grâce à une tactique de division et de domination. Ici aussi, il est fait référence à Microsoft qui a proposé Internet Explorer par défaut pour faire barrage aux plus petits fournisseurs comme Opera et Netscape [Rushin, 2012].

Un troisième type de guerre est celui de la guerre totale ; dans le monde militaire, l'exemple tout trouvé est la Seconde Guerre mondiale entre l'Allemagne nazie et l'Union soviétique. Dans ce type de guerre, on cherche la victoire à tout prix, même une trêve n'est pas envisagée. Dans le monde des entreprises, on peut citer l'exemple de Volkswagen et Porsche : les deux constructeurs se sont menés une guerre d'usure qui s'est terminée par la reprise de Volkswagen par Porsche [Rushin, 2012].

Pour guider les entreprises en temps de crise, Tsang [2000] s'inspire quant à lui de la doctrine militaire « C3I » (*command, control, communication and information*). Celui-ci a étudié les cas de Perrier, Vita Soy et Coca-Cola pour montrer comment la doctrine C3I peut aider les entreprises [Keller, 2008]. Dans son étude des stratégies d'intimidation, James [1985] s'est, pour sa part, inspiré des principes de la guerre froide et recommande également ceux-ci aux entreprises pour conserver leurs parts de marché [Keller, 2008].

Selon Pech et Durden [2003], l'histoire a régulièrement montré que les stratégies militaires classiques et prévisibles mènent à de longues guerres d'usure. Les stratégies s'appuyant sur la surprise, la vitesse, l'innovation semblent plus efficaces. Ces auteurs plaident donc en faveur de stratégies d'entreprise reposant sur le paradigme militaire de la guerre de mouvement. Et ceux-ci de se référer au terme d'« hypercompétition » utilisé par D'Aveni [1994] pour décrire l'environnement moderne des entreprises, qui est comparé à une zone de guerre surtout au niveau du processus décisionnel. Ce que ces auteurs veulent avant tout souligner, c'est que les dirigeants d'entreprise ne peuvent pas, dans leur processus décisionnel, tomber dans le piège suivant : partir du principe que tout est ou peut être sous contrôle. Les auteurs renvoient dans ce cadre à quatre fausses idées qui sont souvent à la base des processus décisionnels, idées mises en avant par Lissack et Roos [2001] :

1. Le monde est suffisamment stable pour pouvoir prévoir les changements ;
2. Les prévisions sont possibles ;
3. Les frontières sont clairement définies ;
4. Les résultats sont plus importants que les processus.

À l'instar de Rushin [2012], Pech et Durden [2003] pensent que de nombreux parallèles peuvent être établis entre les processus militaires et les processus décisionnels en entreprise. Et ceux-ci d'énumérer dans leur article une série d'exemples d'échecs militaires et commerciaux démontrant précisément que les entreprises, comme les militaires, tombent dans le piège des quatre fausses idées précitées.

## Tirer les leçons de grands échecs militaires et commerciaux

Pech et Durden développent les recherches de Norman Dixon [1976] qui a étudié les échecs militaires et tenté d'en déceler les raisons. Dixon a trouvé dans le processus décisionnel un tronc commun pouvant expliquer ces échecs. Pech et Durden [2003] avancent quant à eux une série d'explications, aussi bien dans le monde militaire que celui des affaires. Première explication : l'attachement aux traditions et le goût pour un conservatisme fondamental. Dixon donne l'exemple des revers militaires subis par les Britanniques pendant la Première Guerre des Boers [1880-1881] : alors que les Britanniques privilégiaient contre vents et marées le drill et la parade militaires, l'ennemi

leur opposait des tactiques de guérilla et des stratégies non conventionnelles. Au lieu de s'adapter, les Britanniques ont continué à s'accrocher aux traditions. Pech et Durden donnent en regard l'exemple de la réticence d'IBM à pénétrer le marché des ordinateurs de bureau et leur décision de continuer à utiliser la puce Intel 286 au lieu de la 386. Des concurrents comme Compaq et Apple ont alors fait bon usage du conservatisme d'IBM pour revendiquer ce marché [*Ibid.*].

Autre explication mise en avant par les auteurs : la tendance à ignorer des informations qui sont désagréables ou qui ne correspondent pas aux idées préconçues des dirigeants. L'exemple cité est celui du fiasco de la baie des Cochons, où des informations accablantes selon lesquelles le débarquement serait un échec n'ont pas pu empêcher les plans militaires. Les États-Unis ont lancé une attaque contre l'armée de Castro en s'appuyant sur une série de fausses idées. Rien n'a fonctionné comme prévu ; le deuxième jour, l'envahisseur était cerné par la « faible » armée de Castro et le troisième jour, tout était fini. Ici est établie l'analogie avec l'industrie automobile des années 1940, quand Henry Kaiser, connu pour l'entreprise Kaiser steel, a poursuivi son idée d'introduire une nouvelle voiture de luxe malgré toutes les prédictions de fiasco. Une décision qui a finalement entraîné la chute de l'empire Kaiser [*Ibid.*].

Une autre explication très proche de cette tendance à ignorer les informations est l'entêtement à atteindre un objectif malgré les signes clairs invitant à y renoncer. L'exemple militaire avancé dans ce cadre est l'obsession d'Hitler de conquérir Stalingrad coûte que coûte. Malgré les plaidoyers de son chef d'état-major en faveur d'un retrait, Hitler ne voulait ou ne pouvait reconnaître qu'il sacrifiait la 6<sup>e</sup> armée pour un plan bancal. Un exemple semblable peut être trouvé chez Rolls Royce qui, à la fin des années 1960, a misé énormément sur un nouveau moteur pour avions, le RB-211. Malgré des projections financières alarmantes, l'entreprise a maintenu le cap. Et au moment où le moteur a commencé à produire les performances attendues, les frais de production étaient tellement montés en flèche que les acheteurs avaient fui [Pech et Durden, 2003].

L'hybris – la démesure inspirée par l'orgueil, bien connue des tragédies grecques –, semble aussi être un piège tant dans le monde militaire que dans celui des affaires. La tendance à sous-estimer l'ennemi et à surestimer ses possibilités se retrouve dans les débâcles militaires subies au Viêt Nam, par exemple, mais aussi en Afghanistan. Pech et Durden [2003] se réfèrent ici à Miller [1990], qui a attribué la débâcle ou la disparition d'entreprises autrefois prospères au paradoxe d'Icare, selon lequel les entreprises

à succès deviennent trop sûres d'elles et leurs dirigeants négligents, voire obsédés par un but déterminé ou une stratégie précise. C'est alors la porte ouverte à tous les excès et les extrêmes qui, entre autres, peuvent mener à une sous-estimation de la concurrence et à une surestimation de ses propres possibilités [Pech et Durden, 2003]. Ce paradoxe peut s'illustrer par l'exemple du président de General Motors, Roger Smith, qui, au début des années 1980, a attribué le succès de la pénétration des petites voitures japonaises sur le marché américain uniquement au prix de l'essence dû à la crise pétrolière. Une fois que le prix baisserait, pensait-il, le succès des Japonais aurait aussi du plomb dans l'aile. Mais ce que le président de GM n'a pas vu, c'est que le succès des Japonais n'était pas uniquement attribuable à la consommation d'essence, mais aussi à la qualité, aux performances et au style de leurs voitures [Ibid.].

On dit parfois que les armées doivent anéantir l'ennemi. Pourtant, les Romains laissaient un « pont d'or » ouvert pour permettre à l'ennemi de se retirer après une défaite [Pech et Durden, 2003]. Peut-être cette pratique peut-elle s'expliquer grâce à Sun Tzu, qui a écrit ceci : « *une fois qu'une armée se trouve en "terrain mortel", elle va se battre comme une lionne, car il lui est impossible de s'échapper* ». Sun Tzu conseille donc de laisser une échappatoire à l'ennemi au moment de l'encerclement [Sun Tzu, 2008]. Après l'invasion de l'Europe occidentale, Hitler s'est également abstenu d'anéantir l'armée expéditionnaire britannique à Dunkerque. Il s'agit cependant là d'une arme à double tranchant dans la mesure où ce faisant, les troupes en retrait peuvent panser leurs plaies, se regrouper et lancer une nouvelle attaque. Selon Pech et Durden [2003], le fait de ne pas exploiter totalement le terrain conquis et d'hésiter à procéder à une victoire finale peut avoir des répercussions négatives. Et les auteurs de s'en référer à American Tobacco, qui a refusé de placer des filtres sur les cigarettes. Pall Mall était à l'époque la marque la plus vendue sur le marché, mais à cause de ce refus, elle est tombée à la cinquième place. Donc, en concluent les auteurs, une fois que vous avez le marché en main, vous devez continuer à observer les changements qui s'y produisent, tendre vers une victoire complète et ne pas vous contenter de la situation actuelle [Ibid.].

Comme nous l'avons vu dans les exemples ci-dessus, l'information est capitale. Une mauvaise compréhension et reconnaissance de l'ennemi peuvent mettre les armées en difficulté, comme dans la baie des Cochons et au Viêt Nam. Dans le monde des affaires aussi, une mauvaise compréhension de la situation et un manque de reconnaissance peuvent mettre à mal les entreprises. Lorsqu'on a demandé à Ed Brennan, directeur général de Sears, quel était le plus grand défi de sa société pour l'année

à venir à une époque où Wal-Mart et K-Mart mettaient en péril la position de son entreprise, celui-ci a répondu qu'il ne voyait pas de problèmes notables. Le directeur général s'appuyait sur la position historique forte de Sears sur le marché sans voir ou pouvoir évaluer convenablement la menace qui pesait sur l'entreprise [Pech et Durden, 2003].

Bien que l'histoire militaire ait régulièrement montré qu'une attaque frontale du point le plus fort de l'ennemi se passait souvent mal, une jeune compagnie aérienne néozélandaise, Kiwi Air, a essayé d'attaquer Air New Zealand – une compagnie bien établie sur le marché – au moyen d'une guerre des prix. Air New Zealand a répondu en diminuant ses prix. Comme Kiwi Air était plus petite et qu'elle pouvait moins facilement encaisser les pertes, elle a perdu sa guerre [Ibid.].

La guerre des tranchées de la Première Guerre mondiale montre bien l'issue funeste et le non-sens de la croyance selon laquelle il faut utiliser la force brute et non la ruse pour arriver à ses fins. Les guerres que Coca-Cola et Pepsi se sont menées dans les années 1950-60 ont vu s'affronter deux concurrents qui s'attaquaient à coups de stratégies et tactiques identiques, ce qui a entraîné l'absence d'une victoire finale et des frais gigantesques [Ibid.].

Les parallèles établis par Pech et Durden [2003] entre guerres militaires et stratégies d'entreprise les mènent à la conclusion suivante : les stratégies s'appuyant sur l'innovation, la surprise, la vitesse et l'attaque indirecte de la concurrence sur ses points faibles sont beaucoup plus efficaces que les stratégies classiques caractérisées par des attaques directes, prévisibles. Le maître mot est donc la flexibilité. Un grand nombre des leçons tirées des échecs militaires et commerciaux se rapporte aux processus décisionnels, à l'information ainsi qu'au positionnement sur le marché et le champ de bataille.

*Le maître mot est donc la flexibilité. Un grand nombre des leçons tirées des échecs militaires et commerciaux se rapporte aux processus décisionnels, à l'information ainsi qu'au positionnement sur le marché et le champ de bataille.*

## Retour aux sources : ce que dit Sun Tzu...

Une série de leçons utiles aux entreprises modernes peuvent être tirées des exemples ci-dessus et des parallèles établis entre les stratégies militaires et les stratégies d'entreprise. Ces leçons et autres notions expliquent également le succès des penseurs militaires. Dans son traité *L'Art de la Guerre*, le général philosophe chinois

Sun Tzu mentionné dans l'introduction expose divers principes qui présentent de grandes similitudes avec les leçons précitées. C'est pour cette raison que de nombreux analystes, dirigeants d'entreprise et étudiants s'inspirent de l'auteur de la « Bible » de la stratégie [Keller, 2008]. D'après Wong, Maher et Lee [1998], les principes de Sun Tzu peuvent généralement être répartis en deux volets : connais-toi toi-même et connais ton ennemi. *L'Art de la Guerre* souligne également l'importance de la planification. Et selon Sun Tzu, les armées doivent, lors de leurs préparatifs, prendre divers éléments en considération : les armes, les forces combattantes, le terrain et le soutien logistique [Hadjiphani, 2010].

### Sun Tzu et la gestion stratégique

Dans *L'Art de la Guerre*, Sun Tzu explique que l'armée doit établir un plan détaillé avant tout combat [Tung, 1994]. Comme la guerre est le domaine de la vie et de la mort, écrit Sun Tzu, il est impérieux de la régler avec le plus grand soin. La situation doit être analysée en s'appuyant sur une évaluation des forces des différentes parties ainsi que sur cinq critères : le parcours, les conditions climatiques, les conditions géographiques, le commandement et les règles. Ces dernières comprennent l'efficacité organisationnelle, une ligne hiérarchique et une structure logistique efficace [Sun Tzu, 2008]. Ces notions s'appliquent aux stratégies d'entreprise et aux plans de marketing développés par les entreprises pour se mesurer à leurs concurrents. Elles impliquent donc la nécessité, pour l'entreprise, d'évaluer ses capacités et celles des autres et de réfléchir aux changements stratégiques qui devront être opérés en raison de la grande versatilité du marché actuel. En d'autres termes, il s'agit d'utiliser les connaissances et les estimations pour gérer ces changements, que ce soit dans le monde militaire ou dans celui des affaires. Selon Hadjiphani [2010], ce sont ces changements qui lient le management aux principes de Sun Tzu, dans la mesure où les entreprises peuvent périr à cause d'un mauvais management. En temps de guerre, un piètre commandement et une mauvaise planification militaire peuvent entraîner des massacres, des pertes matérielles et finalement la défaite. Dans le monde des entreprises, ce même problème peut mener à la perte de parts de marché, voire à la disparition de l'entreprise.

Selon Wee, Lee et Hidajat [1991], les circonstances qui prévalent en temps de guerre peuvent également s'appliquer au marché actuel et s'avérer capitales dans la conquête d'un avantage concurrentiel. Après avoir analysé les principes de guerre et ceux du management, les chercheurs ont réparti ceux-ci en cinq catégories fondamentales liées au processus de planification

stratégique. Ce processus commence par une analyse situationnelle qui sert de base pour formuler les objectifs et les stratégies. Puis viennent la mise en œuvre, l'évaluation et le suivi de ces stratégies.

Fennely [1998], qui a également développé les principes de Sun Tzu relatifs à l'analyse situationnelle, a relié ces notions à la mise en œuvre stratégique. Citons les analyses internes et externes réalisées par presque toutes les entreprises en vue d'établir une stratégie adéquate, ou encore les processus de contrôle utilisés pour garantir la mise en œuvre des stratégies [Hadjiphani, 2010]. Les dirigeants d'entreprise connaissent très certainement ces analyses situationnelles puisqu'ils tiennent eux-mêmes compte des circonstances internes et externes à leur organisation. L'analyse de l'ennemi, avec l'exploration des opportunités et des menaces, fait en effet fortement penser à des instruments de marketing tels que l'analyse PEST (*Political, Economic, Social and Technological analysis*) et l'analyse SWOT (*Strengths, Weaknesses, Opportunities and Threats*) qui aident les entreprises à analyser leur environnement et à mieux comprendre leurs concurrents [Kotler, 2003]. Une citation couramment utilisée tirée de *L'Art de la Guerre* s'applique bien à cette situation : « *Qui connaît l'autre et se connaît lui-même, peut livrer cent batailles sans jamais être en péril* » [Sun Tzu, 2008, p. 145].

La connaissance préalable est un concept important dans *L'Art de la Guerre*. La « sagesse » du dirigeant militaire réside en partie dans sa capacité à comprendre que chaque série de circonstances est la conséquence d'un processus dynamique de conditions qui se déterminent mutuellement [Sun Tzu, 2008]. Pour ce faire, le dirigeant a besoin d'informations fiables qui doivent être obtenues immédiatement. « *Dans une guerre, l'information est essentielle ; les armées en dépendent à chaque mouvement* » [Ibid., p.123]. Pour chercher la victoire, Sun Tzu privilégie l'obtention d'un avantage stratégique. L'espionnage et le renseignement sont donc d'importance cruciale. C'est grâce à la connaissance préalable qu'un avantage stratégique peut être obtenu et finir par amener la victoire finale [Ibid.]. Des recherches menées par Wan, Chih et Jung [2004] montrent en d'autres termes l'existence d'une parenté forte entre les principes de Sun Tzu relatifs à l'analyse situationnelle et la gestion stratégique. Dans le monde des affaires, les stratégies doivent être établies sur la base d'informations fiables. Cela veut dire que les organisations réalisent des études de marketing visant à analyser leur environnement interne et externe ainsi que leurs concurrents, le but étant au final d'obtenir un avantage concurrentiel. Selon Hadjiphani [2010], c'est précisément là que se situe l'analogie avec la guerre, car les entreprises développent des stratégies susceptibles d'avoir un impact considérable sur la concurrence. Les effets pratiques de

la publicité comparative, par exemple, visent à montrer la concurrence sous un mauvais jour, voire à l'anéantir.

Bien entendu, la connaissance préalable est tout aussi cruciale pour l'ennemi. D'où l'importance du secret soulignée par Sun Tzu. « *L'habileté suprême consiste à disposer ses troupes sans forme apparente. Alors les espions les plus pénétrants ne peuvent fureter et les conseillers les plus sages ne peuvent établir de plans contre vous* » [Sun Tzu, 2008, p. 128]. Pour atteindre l'« absence de forme » voulue, la duperie est une nécessité. Cette nécessité est déjà soulignée au premier chapitre de *L'Art de la Guerre* : « *La guerre est l'art de la duperie. Quand vous êtes capable, feignez l'incapacité ; quand vous agissez, feignez l'inactivité ; quand vous êtes proche, feignez l'éloignement ; et quand vous êtes loin, feignez la proximité. Ne manquez jamais d'offrir un appât à l'ennemi pour le leurrer. Quand il est en proie à la confusion, attaquez-le et saisissez-le. Quand il est effrayant, tenez-vous prêt à y faire face. Quand il est fort, évitez-le. Quand il est flatté, provoquez-le. Quand il est humble, encouragez son arrogance. Quand il est reposé, épuisez-le. Quand il est uni, divisez-le. Attaquez où il n'est pas préparé en surgissant où il ne vous attend pas* » [Sun Tzu, 2008, p. 137].

## L'importance du leadership

Dans *L'Art de la Guerre*, Sun Tzu souligne à gros traits le rôle du dirigeant. Selon lui, le succès ou l'échec d'une stratégie dépend de la qualité du dirigeant ou – par extension – du chef d'entreprise [McComb, 2001]. Il existe une relation forte entre la planification militaire et la planification en entreprise, car toutes deux requièrent un leadership efficace qui, à son tour, repose sur une vision phare. C'est cette vision qui pose les bases des activités et de la croissance de l'organisation dans son environnement. Ces leaders doivent mettre au point des stratégies et une planification permettant de réaliser les objectifs de leur entreprise [Hadjiphanis, 2010].

Comme nous l'avons déjà dit, il existe toutefois une différence non négligeable entre la planification militaire et la planification en entreprise, celle-ci se situant précisément dans l'issue du processus de planification. Selon certains auteurs, cette différence est surtout liée aux divers environnements dans lesquels chacune de ces organisations évolue et elle n'est pas directement liée au processus de leadership utilisé pour mettre les stratégies en œuvre [Popper, Landau *et al.*, 1992].

La première et principale caractéristique du dirigeant militaire idéal est la suivante : il doit être exemplaire et ses compétences militaires doivent être portées par un caractère supérieur [Sun Tzu, 2008]. Ce qui est étonnant,

c'est que Sun Tzu privilégie le caractère du dirigeant plutôt qu'une série de compétences spécifiques.

« *Un commandant qui avance sans songer à obtenir une quelconque gloire personnelle et qui se retire en dépit d'une certaine réprimande, dont le seul souci est de protéger ses hommes et les intérêts de son souverain, ce commandant-là est la richesse de la nation.* » [Sun Tzu, 2008, p. 120]

En d'autres termes, Sun Tzu dit ceci : bien que les compétences et les aptitudes soient nécessaires, c'est surtout le caractère du dirigeant qui est déterminant. Deux éléments clés tirés de cet enseignement sont souvent repris dans la littérature sans mention du caractère. Le premier élément est l'éthique du leader. D'après Hadjiphanis [2010], des valeurs et principes éthiques doivent être pris en compte dans le processus décisionnel pour éviter que certains actes ne mettent les soldats et les collaborateurs en danger. Des dilemmes éthiques peuvent apparaître en temps de guerre comme en entreprise en cas de conflit de valeurs [Morden, 2004]. De toute évidence, les premiers sont différents des seconds ; il n'en reste pas moins que ces dilemmes peuvent avoir un impact sur l'environnement interne et externe entourant l'organisation militaire ou l'entreprise.

Autre composante du leadership : la méthodologie ou structure en processus, qui est liée à la planification visant des fins militaires, mais aussi commerciales. Ainsi, le processus militaire afférent aux fonctions de commandement, de gestion, d'organisation et de leadership est analogue au processus que l'on retrouve dans les entreprises au niveau de la planification, de l'organisation, de la direction et de la gestion des moyens [Daft, 2013]. La fonction de commandement au sein du management militaire est semblable à la fonction de planification du management d'entreprise [Hadjiphanis, 2010]. Les deux fonctions aident les organisations à fixer les objectifs et à établir la manière dont il faut les réaliser [Drucker, 1999]. Par exemple, la formulation d'objectifs clairs permet de guider et de diriger non seulement les organisations (*management by objectives*), mais aussi leurs activités et leurs décisions [Hadjiphanis, 2010]. Visions, objectifs stratégiques et planification à long terme sont autant de concepts qui font partie de la fonction de leadership ; ils permettent un management reposant sur des performances liées à des objectifs partagés [Dahlsten, Styhre *et al.* 2005] et une mise en œuvre du processus de management grâce à un système de récompense et de motivation [Simpson, 1993]. Le dirigeant doit donc aussi développer une série de processus qui renforcent la structure organisationnelle de façon à répartir les responsabilités dans les différents départements, distribuer

les moyens et gérer les processus de travail [Pfeffer and Veiga, 1999]. Outre les volets « éthique » et « processus », la littérature fait souvent référence à un leadership efficace qui réussit à mettre en place un groupe de collaborateurs enthousiastes et dynamiques [Hadjiphanis, 2010].

## Les leçons de Sun Tzu

Comme nous l'avons déjà indiqué dans l'introduction, il existe de très nombreux ouvrages qui tirent les leçons de *L'Art de la Guerre* et qui les appliquent à la vie en entreprise. Nous allons clôturer la présente contribution en citant quelques-uns des principes exposés dans ce traité datant d'il y a 2 500 ans, le but étant d'illustrer la puissance que cet ouvrage peut avoir sur la pensée stratégique dans le monde des entreprises. Les exemples donnés ci-dessous ne sont pas limitatifs ; ils rassemblent une série de principes déjà exposés dans cette contribution, le tout reposant sur une analyse de Marc McNeilly [n.d.].

« *La meilleure politique guerrière est de prendre un État intact ; une politique inférieure à celle-ci consisterait à le ruiner [...]. Être victorieux dans tous les combats n'est pas le fin du fin ; soumettre l'ennemi sans croiser le fer, voilà le fin du fin* » [Sun Tzu, 2008, p.143].

McNeilly y voit la recommandation suivante : il s'agit de conquérir un marché sans le détruire. Comme le but d'une entreprise est de survivre et d'être prospère, il semble tout à fait contre-productif de détruire le marché sur lequel l'entreprise est active. Le marché peut être conquis par des attaques indirectes, subtiles lancées sur un segment qui n'alarmera pas la concurrence [McNeilly, n.d.]. Rappelons ici l'importance de la duperie. Selon McNeilly [n.d.], ce qui doit absolument être évité, c'est de lancer une guerre des prix parce que ce genre d'opération alarme directement la concurrence et que du coup, il n'y a plus rien à tirer du marché concerné.

« *Il en doit être des troupes à peu près comme d'une eau courante : de même que l'eau qui coule évite les hauteurs et se hâte vers le pays plat, de même une armée évite la force et frappe la faiblesse* » [Sun Tzu, 2008, p. 161].

Autrement dit, évitez les points forts de la concurrence et attaquez ses points faibles. Selon McNeilly [n.d.], l'approche militaire occidentale a influencé le monde des affaires. Résultat : beaucoup d'entreprises ont lancé des attaques directes sur les points les plus forts de leurs concurrents. Pensez au cas de Kiwi Air. Ce genre d'approche coûte énormément à toutes les parties. En revanche, attaquer les faiblesses du concurrent permet de maximiser les bénéfices et de minimiser l'utilisation de ses propres ressources [Ibid.].

« *Qui connaît l'autre et se connaît lui-même, peut livrer cent batailles sans jamais être en péril* » [Sun Tzu, 2008, p. 145].

Pour découvrir et exploiter les faiblesses de la concurrence, il faut bien connaître non seulement ses stratégies, ses possibilités et ses souhaits, mais aussi ses propres forces et ses propres faiblesses. Il est également important de bien connaître les tendances générales du marché pour ressentir le futur « champ de bataille ». Afin d'éviter que les concurrents n'emploient ce genre de stratégie contre elle, l'entreprise a par ailleurs tout intérêt à garder ses plans secrets et à utiliser la ruse [McNeilly, n.d.].

« *La rapidité est la sève de la guerre* » [Sun Tzu, 2008, p. 191]. Pour vaincre rapidement la concurrence, McNeilly conseille d'utiliser la vitesse et la préparation. Pour exploiter à fond les connaissances préalables et la duperie, il est nécessaire d'agir au quart de tour. Ce qui ne veut pas dire précipiter les choses. Dans la pratique, la rapidité nécessite beaucoup de préparation. Il est essentiel que l'entreprise réduise le temps dont elle a besoin pour prendre ses décisions, développer ses produits et servir ses clients. Et il est tout aussi nécessaire de réfléchir aux réactions potentielles de la concurrence face à l'attaque lancée [McNeilly, n.d.].

« *Ainsi, l'expert fera vaciller l'ennemi sans vaciller lui-même* » [Sun Tzu, 2008, p. 157].

Utilisez des alliances et des points de contrôle stratégiques sur le marché pour « façonner » vos concurrents et les obliger à se conformer à vos volontés. « Façonner la concurrence » signifie modifier les règles concurrentielles pour qu'elles cadrent dans votre stratégie et dans vos actions, c'est-à-dire prendre le contrôle de la situation. Une manière d'arriver à cet objectif est de conclure et d'utiliser des alliances [McNeilly, n.d.].

« *On rassemble [les troupes] par un traitement humain, on les soude par la discipline militaire. C'est ainsi que leur fidélité sera assurée* » [Sun Tzu, 2008, p. 179].

Sun Tzu décrit les nombreux traits de caractère que doit posséder un dirigeant. Il doit être sage, droit, humain, courageux et rigoureux. Il doit aussi prévoir les besoins de ses troupes.

## Conclusion

Il ressort clairement de la présente contribution que les raisons pour lesquelles les idées militaires semblent souvent inspirer le monde des entreprises se cachent notamment dans le concept de stratégie ainsi que dans la mise en œuvre et la conduite de ces stratégies. La planification d'entreprise est comparée à la planification

militaire, car ces deux concepts ont des processus clés semblables. Ils utilisent la même fonction du management. Ils ont toutefois une vision très différente. Cette différence est liée à l'issue finale de la vision. Celle de l'armée est grosso modo de vaincre l'ennemi [bien qu'il soit possible de citer d'autres objectifs], tandis que celle de l'entreprise est d'assurer sa pérennité et de concurrencer d'autres organisations dans le but d'obtenir un avantage concurrentiel sur le marché.

Des parallèles sont souvent établis à partir de ces similitudes entre les opérations militaires et les opérations en entreprise, le but étant de déceler des stratégies sous-jacentes au sens large du terme et des processus clés qui pourraient éventuellement être mis en œuvre à l'échelle de l'organisation. Le succès de Sun Tzu – et d'autres penseurs militaires – réside précisément dans le fait qu'il communique des idées normatives pour certains processus clés comme la planification, l'exécution et la gestion des stratégies, la communication et le leadership. Des critiques posent toutefois la question de l'interchangeabilité des idées précitées dans la mesure où les objectifs de l'armée ne sont pas les mêmes que ceux d'une entreprise. Il n'en reste pas moins que ces idées peuvent constituer des sources d'inspiration... Ce que le traité *L'Art de la Guerre*, qui a réussi à traverser les affres du temps, a largement prouvé.

*La planification d'entreprise est comparée à la planification militaire, car ces deux concepts ont des processus clés semblables. Ils utilisent la même fonction du management. Ils ont toutefois une vision très différente. Cette différence est liée à l'issue finale de la vision.*

Nous clôturerons cette contribution par une note critique. Bien que les analogies entre la guerre et les affaires semblent interchangeables, on peut se poser une série de questions concernant cette symbiose. L'interchangeabilité du jargon, par exemple, est mise à mal par Talbot [2003] et Keller [2008]. D'une part, l'utilisation du jargon militaire et du concept stratégique dans le monde des affaires peut mener à une forme plus dure et implacable de faire des affaires, ce qui engendre des stratégies « à somme nulle » et des actions où l'on ne parle qu'en termes de gagnant et de perdant. En d'autres termes, cette pratique peut avoir des conséquences sur l'état d'esprit des dirigeants. D'autre part, on observe une influence du jargon des entreprises sur le monde militaire, où l'on parle par exemple de « dommages collatéraux » en cas de victimes civiles et de destruction d'habitations. Les armes nucléaires, biologiques et chimiques sont appelées armes de destruction massive. Le « blanchissage » du jargon militaire peut créer une distance entre la réalité de la guerre et sa planification [Keller, 2008].

Forts de ces mises en garde, les dirigeants d'entreprise sont invités à se plonger dans différents types de littérature, dont la littérature militaire, pour y puiser leur inspiration et frotter les idées et notions qu'ils y trouveront à la réalité quotidienne des affaires. Cet exercice portera ses fruits à court terme, mais aussi à long terme. Et surtout : il s'agit d'apprendre des erreurs du passé ! ■

## Bibliographie

ALBANESE (R.), 1994, «Team-Building Process : Key to Better Project Results», *Journal of Management in Engineering*, 10 (6), 36-44.

ANSOLF (H. I.) (Ed.), 1969, *Business strategy : selected readings*, Baltimore, Md, Penguin Books.

BARTELINK (G. J. M.), 1966, *Grieks-Nederlands Woordenboek*, Utrecht-Antwerpen, Het Spectrum.

BEYER (G.), 2014, «Why business leaders are obsessed with Sun Tzu's ancient military guide, "The Art of War"», *The Huffington Post*.

BRACKER (J.), 1980, «The historical development of the strategic management concept», *The Academy of Management Review*, 5 (2), 219-224.

BRANCH (M. C.), 1957, «Planning and Operations Research», *Journal of the American Institute of Planners*, 23 (4), 168-175.

CANNON-BOWERS (J. A.), SALAS (E.), *et al.*, 1993, «Shared Mental Models in Expert Team Decision Making», *Individual and Group Decision Making : Current Issues*, CASTELLAN (N. J. JR.) (Ed.), Hillsdale, Lawrence Erlbaum Associates, 221-246.

- CANTRELL (R.), 2004, «Sun Tzu and Hollywood : How Sun Tzu's Art of War has appeared on the big and small screen», Retrieved 26 October, 2014, from <http://www.artofwarsuntzu.com/suntzuandhollywood.htm>
- CEO. com, 2013, 7 May, «24 Leadership Books To Read Before You Die», Retrieved 26 October, 2014, from [http://www.ceo.com/leadership\\_and\\_management/the-23-best-leadership-books-of-all-time/](http://www.ceo.com/leadership_and_management/the-23-best-leadership-books-of-all-time/)
- D'AVENI (R.), 1994, *Hypercompetition : Managing the dynamics of strategic maneuvering*, New York, Free Press.
- DAFT (R. L.), 2013, *Management*, 11th edition, Mason, South-Western.
- DAHLSTEN (F.), STYHRE (A.), *et al.*, 2005, «The unintended consequences of management by objectives. The volume growth target at Volvo cars», *Leadership & Organization Development Journal*, 26 (7), 529-541.
- DIXON (N.), 1976, *On the psychology of military incompetence*, London, Random House.
- DRUCKER (P. F.), 1999, *Management. Tasks, responsibilities, practices*, London, Butterworth-Heinemann.
- ECONOMIST (T.), 2013, «Business, politics and war : Why a strategy is not a plan», *The Economist*.
- FARRELL (E.) and DEROSE (R.), 2000, «Restoration Operation», *Best's Review*, 101 (7), 51-62.
- FELD (M. D.), (1959), «Information and authority : The structure of military organization», *American Sociological Review*, XXIV, 15-22.
- FENNELLY (J. P.), 1998, «Seeking strategic advantage through health policy analysis», *Journal of Health Politics*, 23 (5), 867-870.
- FRAZER (W.), 1982, «Milton Friedman and Thatcher's monetarist experience», *Journal of Economic Issues*, 16 (2), 525-533.
- FREEDMAN (L.), 2013, *Strategy : A History*, Oxford, Oxford University Press.
- FRIEDMAN (M.), 1970, «The Social Responsibility of Business is to Increase its Profits», *The New York Times Magazine*, New York, The New York Times Company.
- GHEMAWAT (P.), 2002, «Competition and business strategy in historical perspective», *The Business History Review*, 76 (1), 37-74.
- HADJIPHANIS (L.), 2010, «War and business planning», *Journal of Business Administration Online*, 9 (2), 1-9.
- HEENE (A.), VAN LOOY (B.) *et al.*, 2003, «Defining a service strategy», *Services Management: An integrated Approach*, VAN LOOY (B.), GEMMEL (P.) and VAN DIERDONCK (R.), Essex, Pearson Education Limited, 453-474.
- HONIG (B.), 2004, «Entrepreneurship Education : Toward a Model of Contingency-Based Business Planning», *Academy of Management learning & education*, 3 (3), 258-273.
- JAMES (B.), 1985, «Deterrence - a strategy that pays», *Business Horizons*, 28 (6), 60.
- KELLER (G. F.), 2008, «The influence of military strategies on business planning», *International Journal of Business and Management*, 3 (5), 129-134.
- KOTLER (P.), 2003, *Marketing management*, Upper Saddle River NJ, Prentice Hall.
- LENGNICK-HALL (C. A.), and LENGNICK-HALL (M. L.), 1988, «Strategic Human Resources Management: A Review of the Literature and a Proposed Typology», *The Academy of Management Review*, 13 (3), 454-470.
- Lissack (M.) and Roos (J.), 2001, «Be coherent, not visionary», *Long Range Planning*, 34 (1), 53-70.
- MCCOMB (J. A.), 2001, «Moving from planning to progress», *Credit Union Executive Journal*, 41 (4), 24-27.
- MCNEILLY (M.), [n.d.]. «Six principles of Sun Zzu and the art of business», Retrieved 26 October 2014, from <http://www.suntzustrategies.com/resources/six-principles-of-sun-tzu-the-art-of-business>
- MILLER (D.), 1990, *The Icarus paradox: How exceptional companies bring about their own downfall*, New York, HarperCollins.
- MINTZBERG (H.), 1987, «Crafting Strategy», *Harvard Business Review*, July-August, 66-75.
- MINTZBERG (H.), 1990, «The design school: Reconsidering the basic premises of strategic management», *Strategic Management Journal*, 11 (3), 171-195.

- MINTZBERG (H.), 1994, *The rise and fall of strategic planning*, New York, The Free Press.
- MORDEN (T.), 2004, *Principles of Management*, Ashgate, Aldershot.
- PAYNE (J. H.) and TURNER (J. R.), 1999, «Company-wide project management: the planning and control of programmes of projects of different type», *International journal of project management*, 17 (1), 55-59.
- PECH (R. J.) and DURDEN (G.), 2003, «Manoeuvre warfare: a new military paradigm for business decision making», *Management Decision*, 41 (2), 168-179.
- PFEFFER (J.) and VEIGA (J. F.), 1999, «Putting people first for organizational success», *Academy of Management Executive*, 13 (2), 37-48.
- PING (L. P.) [n.d.], *The Japanese Model and Southeast Asia beyond the Asian Crisis*, Tokyo Global Industrial and Social Progress Research Institute [GISPRI].
- POPPER (M.), LANDAU (O.), *et al.* 1992, «The Israeli defense forces: an example of transformational leadership», *Leadership and Organization Development Journal*, 13 (1), 3-8.
- RUSHIN (G.), 2012, «Strategy : Is war strategy and business strategy similar?», Retrieved 27 September, 2014, from [http://garyrushin.com/my\\_blog/business-strategy-2/strategy-is-war-strategy-and-business-strategy-similar/](http://garyrushin.com/my_blog/business-strategy-2/strategy-is-war-strategy-and-business-strategy-similar/)
- RUTNER (S.), 2012, «Logistics evolution: a comparison of military and commercial logistics thought», *International Journal of Logistics Management*, 23 (1), 96-118.
- SHENHAR (A. J.), 1998, «From theory to practice: toward a typology of project-management styles», *IEEE Transactions on Engineering Management*, 45 (1), 33-48.
- SIMPSON (J. A.), 1993, «Management by objective for appraisal firms», *The Appraisal Journal*, 61 (3), 380-385.
- SUN-TZU, 2008, *De kunst van het oorlogvoeren*, Amsterdam, Muntinga Pockets.
- TALBOT (P.), 2003, «Corporate generals: the military metaphor of strategy», *Irish Journal of Management*, 24 (2), 1-10.
- TEEX, 2013, *Taking Charge-7 Leadership Stories*, Col. John Antal, Texas A & M Engineering Extension Service [TEEX].
- TSANG (A.), 2000, «Military doctrine in crisis management: three beverage contamination cases», *Business Horizons*, 43 (5), 65.
- TUNG (R. L.), 1994, «Strategic management thought in East-Asia», *Organizational Dynamics*, 22 (4), 55-65.
- VON CLAUSEWITZ (C.), 1989, *On War*, Princeton, Princeton University Press.
- WANN (Y. W.), CHIH (H. C.), *et al.*, 2004, «A study of strategy implementation as expressed through Sun Tzu's principles of war», *Industrial Management and Data Systems*, 104 (5), 396-408.
- WEE (C. H.), LEE (K. S.), *et al.*, 1991, *Sun Tzu and management*, Singapore, Addison-Wesley.
- WESLEY (R.), 2004]. «Isabelle Beeton: Management lessons from the kitchen», *Business Strategy Review*, 15 (3) 66-72.
- WONG (L.), BLIESE (P.), *et al.*, 2003, «Military leadership: A context specific review», *The Leadership Quarterly*, 14 (6) 657-692.
- WONG (Y. Y.), MAHER (T. E.), *et al.*, 1998, «The strategy of an ancient warrior. An inspiration for international managers», *Multinational Business Review*, 6 (1) 83-93.

# Les néo-fundamentalistes, version EIL

Hamza SHAREEF HASAN

Les chercheurs et les intellectuels s'accordent à dire que le phénomène salafiste djihadiste découle de la pensée wahhabite de Mohammed ibn Abdelwahhab (1703-1792), fondateur de l'école salafiste qui prône le retour aux pratiques religieuses des pieux prédécesseurs. Ce phénomène a évolué depuis : désormais, la violence est considérée comme le seul moyen de changer radicalement la société en vue de fonder un État islamique. À l'époque de la guerre froide, lorsque l'Union soviétique a envahi l'Afghanistan dans les années 1970, l'Arabie saoudite et d'autres pays du Golfe se sont empressés de soutenir les combattants afghans dans leur résistance face à



l'envahisseur soviétique. Par ailleurs, les jeunes du monde arabe, que l'on appellera par la suite les « djihadistes arabes », ont été encouragés à aller leur prêter main forte. Après la défaite des Soviétiques, les combattants afghans se sont livrés à une guerre sans merci qui s'est soldée par l'arrivée au pouvoir des talibans, soutenus par l'Arabie saoudite et par le Pakistan et qui contrôlaient une grande partie du pays. Contrairement au reste du monde arabo-musulman, l'Arabie saoudite, le Pakistan et les Émirats arabes unis ont reconnu la légitimité du gouvernement taliban. Toutefois, sous l'effet de la pression internationale, l'Arabie saoudite et les Émirats arabes unis ont retiré leur soutien aux talibans le 22 septembre 2001, au lendemain des attentats du 11 septembre.

Les djihadistes arabes se sont réunis sous le commandement de Ben Laden et ont créé une organisation appelée « al-Qaïda ». Cette organisation a développé le concept du djihad et acquis une expérience au combat digne des meilleures unités d'élites, à laquelle s'ajoutent une détermination sans faille et un fort attachement aux

principes qu'elle prône. Après la guerre en Afghanistan, l'invasion de l'Irak, l'assassinat de Ben Laden et l'arrivée d'al-Zawahiri à la tête d'al-Qaïda, une scission au sein des fondamentalistes a provoqué l'apparition de l'État islamique en Irak et au Levant (EIL ou Daech), dirigé par Abou Bakr al-Baghdadi. Celui-ci a d'ailleurs annoncé la fondation d'un État islamique sans frontières géographiques. Par ailleurs, de nombreuses branches d'al-Qaïda à travers le monde ont prêté allégeance à al-Baghdadi.

Depuis leur apparition, ces deux organisations ont fait couler beaucoup d'encre. De nombreux auteurs du monde entier ont tenté de comprendre cette dangereuse tendance qui menace toute l'humanité. Les néo-fundamentalistes (les membres de l'EIL) ont recours à une forme de violence démesurée pour semer la terreur. Persuadés de détenir la vérité et convaincus de l'erreur de l'autre, qu'il soit musulman ou pas, ces individus se prêtent peu au dialogue. Ils ont même accusé al-Qaïda d'hérésie en raison de sa « modération » et de son indifférence vis-à-vis des Frères musulmans qui,

**Hamza SHAREEF HASAN**



Conseiller à l'international pour le gouvernement irakien.

pour leur part, admettent l'existence de plusieurs partis politiques et croient en la démocratie.

L'écrasante majorité des musulmans sait pertinemment que les actions de l'EIIL sont contraires à l'esprit de l'islam, à ses enseignements et aux principes de justice, d'amour, de tolérance et de paix qu'il prêche. Par ailleurs, dans le Coran, Dieu s'adresse à Mahomet en ces termes : « *Et Nous ne t'avons envoyé qu'en miséricorde pour l'univers* ». Mahomet a été envoyé à l'ensemble de l'humanité et pas seulement aux musulmans, avec pour consigne d'appeler les gens « *au sentier* [du] *Seigneur par la sagesse et par la bonne exhortation* » et non par la violence et la contrainte comme le font ces néo-djihadistes. En outre, les actes de ces derniers sont contraires à la nature humaine et leur violence grandissante, à laquelle sont associées des paroles de Mahomet allant en ce sens, devient particulièrement dangereuse.

Ce phénomène nouveau qui sème la terreur et suscite l'aversion en poussant des jeunes à tirer sur les foules ou à faire exploser leurs ceintures au milieu d'innocents dont le seul tort aura été de se trouver au mauvais endroit au mauvais moment, en causant d'importants dégâts, suscite de nombreuses interrogations dans les milieux intellectuel, culturel et social. Par ailleurs, cette organisation s'ingénie à trouver de nouvelles façons de tuer, toujours plus atroces et barbares. Citons l'exemple de ce terroriste qui dévora le cœur de l'une de ses victimes ou du jeune pilote jordanien brûlé vif, ainsi que des décapitations dignes des périodes les plus sombres de l'histoire. Tout en suscitant en nous un sentiment de peine et de tristesse pour les victimes de ces actes barbares, un tel étalage de violence nous pousse à réfléchir sur la manière de protéger ces jeunes recrues contre tout enrôlement comme candidat au suicide ou combattant dans ces organisations terroristes (al-Qaïda et EIIL) qui leur ôtent toute humanité.

Nous tenterons de faire la lumière sur cette tendance, depuis son apparition et jusqu'à son évolution dans sa forme d'État islamique. Dans le cadre de mon exposé, je fournirai, aux nombreuses questions qui se posent, des réponses objectives et rationnelles reposant sur des preuves et des éléments avérés. Les nombreux écrits sur

cette question nous fournissent une importante quantité d'informations, mais ils n'analysent pas toutes les origines du problème et ne proposent aucun moyen de l'aborder et d'y remédier (que ce soit au niveau de la sécurité ou sur les plans économique, culturel, social, religieux et politique) afin d'éradiquer ce phénomène et de protéger l'humanité.

Voici les interrogations que nous posons :

L'ÉCRASANTE MAJORITÉ  
DES MUSULMANS SAIT  
PERTINEMMENT QUE LES  
ACTIONS DE L'EIIL SONT  
CONTRAIRES À L'ESPRIT DE  
L'ISLAM, À SES ENSEIGNEMENTS  
ET AUX PRINCIPES DE JUSTICE,  
D'AMOUR, DE TOLÉRANCE ET  
DE PAIX QU'IL PRÊCHE. PAR  
AILLEURS, DANS LE CORAN, DIEU  
S'ADRESSE À MAHOMET EN CES  
TERMES : « *ET NOUS NE T'AVONS  
ENVOYÉ QU'EN MISÉRICORDE POUR  
L'UNIVERS* ».

1. Le développement du fondamentalisme violent est-il dû à l'existence de dictatures répressives dans le monde arabe et dans certains pays musulmans ? Dans ce cas, que dire des personnes qui sont nées et ont grandi dans des pays démocratiques, mais qui se laissent malgré tout influencer par les idées de ces organisations et qui les rejoignent ?
2. La marginalisation et le racisme au sein d'une société démocratique (notamment en Occident) sont-elles les raisons qui poussent ces jeunes à rejoindre ces organisations terroristes ou bien leur décision est-elle due à leur échec personnel et à leur incapacité à accéder à de meilleures conditions de vie matérielle et culturelle ? Les raisons seraient-elles d'ordre psychologique ? Ces personnes seraient-elles en quête de fortune et d'aventures ? Bien que leur nombre soit limité, leur pouvoir dévastateur reste considérable ;
3. Quelles sont les raisons qui incitent de jeunes femmes nées et éduquées dans des sociétés civilisées à rejoindre ces organisations barbares et à prendre part à ces actes inhumains ?
4. Les mosquées, les écoles et les institutions religieuses financées par l'Arabie saoudite dans le but de propager la pensée wahhabite à travers le monde sont-elles responsables de la propagation des idées d'al-Qaïda et de l'EIIL ?
5. Ces jeunes fuient-ils la situation économique et la pauvreté en s'enrôlant ? Que dire alors des personnes des classes moyennes et des milieux aisés qui rejoignent elles aussi ces organisations ? Si la pauvreté, le sous-développement et la dictature ne sont pas les seules causes d'un tel comportement, comment pourrions-nous protéger les prochaines générations ?

6. L'ignorance et le sous-développement forment-ils un contexte propice à l'assimilation de telles idées ? Dans ce cas, pour quelles raisons des personnes éduquées et compétentes dans divers domaines ont-elles rejoint les rangs de ces organisations ? Ont-elles tiré profit de ces compétences pour obtenir un rôle clé au sein de ces organisations ou bien sont-elles persuadées de la légitimité des principes salafistes ?
7. La promesse du paradis et des houris parvient-elle à attirer de jeunes personnes frustrées, démunies, opprimées et n'ayant plus rien à perdre ou bien sont-elles victimes d'un « lavage de cerveau » ?
8. Le conflit israélo-arabe, la cause palestinienne et la politique répressive d'Israël expliquent-ils cette réaction violente de jeunes musulmans et le désespoir et la frustration les incitent-ils à adhérer à cette idéologie destructrice ?
9. Les divergences politiques et les conflits ethniques en Irak et en Égypte forment-ils un contexte propice à l'apparition de groupuscules terroristes et au renforcement du fondamentalisme ?
10. L'invasion du Koweït par l'Irak en 1990, sa libération en 1991 accompagnée de l'intervention américaine et occidentale en Arabie saoudite explique-t-il en partie l'augmentation du radicalisme ?
11. La stratégie mise en place par le président américain après l'invasion de l'Irak en 2003, qui a permis l'entrée de nombreux combattants étrangers sur le territoire irakien dans l'espoir de mieux les maîtriser, a-t-elle provoqué un accroissement de la violence et la création de l'EIL ?
12. L'augmentation de la violence et du terrorisme résulte-t-elle de la dégradation des conditions de sécurité après l'invasion de l'Irak et du retrait des troupes américaines avant même que la situation politique ne soit stabilisée et la sécurité rétablie ?
13. Les diverses interventions régionales et internationales dans les pays du Printemps arabe, leurs conséquences négatives et la dégradation des conditions de sécurité expliquent-elles l'augmentation du radicalisme et de la violence ?
14. Dans quelle mesure la guerre au Yémen va-t-elle entraîner plus de violence ? (Rappelons que les Houthis combattent al-Qaïda au Yémen depuis longtemps). Comment interpréter les frappes saoudiennes contre les Houthis, qui ont contribué à renforcer al-Qaïda ?
15. La politique du deux poids et deux mesures appliquée par les grandes puissances mondiales en matière de relations internationales, notamment sur la question du Proche-Orient, est-elle l'une des raisons de la recrudescence de la violence ?
16. La résistance à l'occupation est perçue comme un acte de terrorisme par certains acteurs de la politique internationale. Cette perception aurait-elle contribué à renforcer le terrorisme ?
17. Ces organisations terroristes rejettent le chiïsme, les chrétiens et bien d'autres groupes. Il y a très peu de temps encore, l'imam de la Mecque maudissait les chrétiens et les juifs lors du prêche du vendredi et suppliait Dieu d'accorder la victoire aux musulmans. Toutefois, est-ce pour des raisons religieuses, politiques ou autres que ces organisations rejettent également d'autres groupes de musulmans sunnites ?
18. De quelle manière le recrutement incite-t-il ces nouveaux venus à adopter les idées de ces organisations et à considérer leurs actes barbares comme un combat au nom de l'islam et à penser que leurs morts sont des martyrs destinés au paradis ? Quel dieu et quelle religion autoriseraient de tels actes ? Comment ces organisations parviennent-elles à convaincre les jeunes recrues de la légitimité de leurs actions ?
19. Les prisons comme le camp de Guantanamo et le Camp Bucca en Irak ont-elles contribué à renforcer le radicalisme violent et à faciliter le recrutement de nouveaux membres ?
20. De quelle manière cette idéologie s'est-elle développée pour devenir de plus en plus cruelle et malveillante ?
21. Pourquoi l'islam a-t-il été associé au terrorisme ? Sans l'existence du wahhabisme, une telle violence aurait-elle été possible ?
22. Ces organisations envisagent-elles de remettre en question leurs méthodes ou sont-elles déterminées à continuer sur cette voie ? Certaines réformes ont été constatées mais elles n'ont abouti qu'à davantage de radicalisme, pourquoi ?
23. Est-il possible de réformer leurs membres et de les réhabiliter ? La méthode de réhabilitation saoudienne a-t-elle porté ses fruits ? Ou bien les personnes « réhabilitées » sont-elles revenues au terrorisme ? Faut-il condamner les membres de ces organisations à la prison à perpétuité ?

24. Comment traiter les personnes qui, dupées par le discours de ces organisations, se sont rétractées après avoir constaté la réalité des faits ? Comment les aider à se réformer ?

25. Existe-t-il un inventaire précis et des informations fiables sur les différentes organisations djihadistes existantes comme leur répartition géographique et le nombre de leurs membres et ce, quels que soient leur appellation et leur emplacement, tant que leur idéologie et leur mode d'action criminel sont le même ? Savons-nous combien de personnes soutiennent de telles organisations (des milliers ? des centaines de milliers ? des millions ?) ?

26. Lors de l'invasion de Ninive (Irak) et d'autres villes du pays par l'EIIL, les hommes de religion et les médias d'Arabie saoudite et d'autres pays du Golfe ont affirmé qu'il ne s'agissait là que d'une révolte populaire sunnite. Ces propos étaient-ils dus à l'ignorance ou bien à un sectarisme excessif ?

27. Pourquoi certains gouvernements, organisations et individus financent-ils al-Qaïda ou l'EIIL ? Les raisons sont-elles politiques, sectaires ou même les deux ? S'agit-il d'une lutte d'influence ou pour la domination d'un pays ?

28. Les États qui, jusqu'à une période récente, étaient accusés de soutenir et de financer le terrorisme, sont-ils désormais réellement déterminés à le combattre ou bien leur engagement dans cette lutte n'est-il qu'un leurre ?

29. Pourquoi certains pays échappent-ils aux attaques terroristes ? Est-ce parce qu'ils financent ces organisations ou bien leurs mesures de sécurité sont-elles plus efficaces que celles d'autres pays ?

30. Supposons que 15 Saoudiens parmi ceux qui ont pris part aux attentats du 11 septembre aient été originaires d'un pays différent, que se serait-il passé ? Quelle est la raison du silence des États-Unis sur cette question ? Ces derniers se sont-ils abstenus de tout commentaire afin de préserver la durabilité de leurs importations de pétrole ou des relations personnelles ?

31. Pourquoi l'Arabie saoudite est-elle considérée comme un État modéré, selon les critères occidentaux, alors que l'Iran fait partie de l'axe du mal ? Est-ce parce que l'Iran a abrité des chefs d'al-Qaïda ou pour une autre raison ?

32. Comment Abou Moussab al-Zarqaoui est-il parvenu à s'enfuir de Jordanie après sa remise en liberté et à atteindre l'Afghanistan avant de se rendre en Irak en traversant l'Iran ? Qui l'a aidé dans cette entreprise ?

33. Existait-t-il réellement une relation entre le parti Baath et al-Qaïda ? Puis entre le parti Baath et l'EIIL ? De nombreux Irakiens et moi-même considérons cette hypothèse comme plausible en raison de notre connaissance des méthodes employées par le parti Baath ainsi que de la manière dont il est arrivé au pouvoir. En décembre 2010, j'ai pris la parole sur la question lors d'une conférence sur le terrorisme organisée à Washington par la fondation Jamestown. À cette époque, très peu de personnes avaient prêté attention à mes paroles. Néanmoins, le *Washington Post* a publié il y a quelques semaines un article sur les liens existants entre le parti Baath et l'État islamique ;

34. Les décisions du Conseil de sécurité de l'ONU sur la lutte contre le terrorisme, à savoir les résolutions 1373 de 2001, 2175 de 2014 et enfin, 2199 de 2015, ont-elles permis de réduire le financement et le soutien aux organisations terroristes ou bien ont-elles été insuffisamment efficaces et doivent-elles être revues ?

35. Est-il vrai que la Turquie, membre de l'OTAN qui lutte contre le terrorisme, entraîne et finance des centaines de nouvelles recrues et leur permet de se rendre en Syrie ? Pour quelle raison le ferait-elle ? Serait-ce dans le simple but de faire tomber Bachar al-Assad ? Est-ce qu'un tel objectif justifierait que l'on sacrifie pour lui des centaines de vies innocentes et que l'on détruise des villes et des monuments du patrimoine archéologique et humain ? S'agit-il alors d'une erreur de jugement aux conséquences désastreuses ?

36. Le monde aurait-il soudain découvert que le gouvernement de Bachar al-Assad était en fait une dictature dont la suppression serait si indispensable qu'elle justifierait le soutien apporté au front al-Nosra (lui aussi affilié à al-Qaïda) et à l'EIIL ? Il convient d'abord de redéfinir les priorités dans le cadre de la lutte contre le terrorisme avant d'aider le peuple syrien à se libérer d'un régime totalitaire ;

37. La politique d'armement de l'opposition syrienne modérée s'est-elle révélée utile ou bien a-t-elle, au

COMMENT TRAITER LES  
PERSONNES QUI, DUPÉES  
PAR LE DISCOURS DE CES  
ORGANISATIONS, SE SONT  
RÉTRACTÉES APRÈS AVOIR  
CONSTATÉ LA RÉALITÉ DES  
FAITS ? COMMENT LES AIDER  
À SE RÉFORMER ?

contraire, permis de fournir des armes aux terroristes par divers canaux ?

38. Quelles raisons poussent ces organisations à détruire le patrimoine culturel (dans l'Afghanistan des talibans d'abord, puis à Ninive et en Syrie) et les hommes religieux saoudiens à cautionner cette entreprise ? Nous devons protéger l'histoire et le patrimoine de l'humanité ;

39. La supervision de la préparation des armes et du matériel conformément à la convention sur la lutte contre le commerce d'armes légères et de petit calibre est-elle efficace ou doit-elle être revue ?

40. L'État islamique a dérobé une quantité importante d'armes et de matériel aux armées syrienne et irakienne : comment expliquer qu'il ne manque jamais de munitions et de matériel, ni de pièces détachées pour le réparer ?

41. Pourquoi la communauté internationale est-elle incapable de mettre un terme aux activités des trafiquants d'armes et de pétrole ?

42. L'alliance internationale actuelle et sa stratégie parviennent-elles à lutter contre le terrorisme ou un remaniement total s'impose-t-il ?

43. Est-il possible d'interdire à ces organisations l'accès à tous les moyens de communication y compris les réseaux sociaux ? Quelles en seraient les conséquences ?

44. Cette décennie de lutte contre le terrorisme a-t-elle été productive ou, au contraire, a-t-elle provoqué l'apparition de nouvelles générations de terroristes encore plus cruels ? Dans ce cas, il convient de revoir les modalités de la lutte contre le terrorisme ;

45. Le « conflit entre les civilisations » est-il la raison de la recrudescence des actes de violence et de terrorisme ou en est-il la conséquence ?

Il existe de nombreuses réponses à ces questions, certaines exprimant des opinions personnelles et d'autres se fondant sur des analyses. J'estime qu'il revient aux centres de réflexions et aux spécialistes de différents domaines, ainsi qu'aux savants musulmans et aux services de renseignement de pays du monde entier, de répondre à ces questions. Il est nécessaire de créer un réseau d'études destiné à analyser les racines du problème de manière approfondie, réfléchie, scientifique et professionnelle. Pour obtenir des réponses fondées sur des preuves et proposer des instructions et des stratégies efficaces et applicables avec la coopération de la communauté internationale, il nous faut analyser l'idéologie des organisations comme al-Qaïda et l'État islamique.

La mise en œuvre de ces propositions nécessite un temps considérable, probablement des dizaines d'années. Par conséquent, il est nécessaire de proposer des stratégies par étapes incluant des priorités hiérarchisées et d'instaurer un dispositif de supervision permanente. Par ailleurs, les solutions isolées et régionales ne seront jamais efficaces. En outre, elles nécessiteront plus de temps, seront plus coûteuses et provoqueront l'apparition d'une génération de terroristes encore plus cruels que les membres actuels de l'État islamique, et nous ne saurons ni où ni quand cette barbarie se manifesterà. Nous devons nous unir pour lutter contre ce fléau ■

# Salafisme (s) et violence. La construction historique d'une axiomatique de la violence

## *Des frères musulmans à Al-Qaïda : d'une conception utilitaire de la violence à une vision organique ?*

Mohamed-Ali ADRAOUI

L'objet de cet article est de faire la lumière sur les différentes éthiques de la violence observables au sein des mouvements revivalistes et fondamentalistes se réclamant du salafisme. Depuis, en effet, plusieurs décennies, ce terme a été utilisé (souvent de manière abusive) pour décrire l'idéologie religieuse à partir de laquelle des partis politiques organisés, des groupes militaires (faisant parfois usage de méthodes qualifiées de terroristes) ou encore des communautés puritaines déployaient une vision du monde centrée sur la nécessité de remettre au goût du jour l'islam « original ». En raison de la légitimité historique accordée à la velléité de revenir aux sources de la religion musulmane afin de donner l'impulsion à une réforme spirituelle, morale et parfois juridique et politique censée revigorer la *oumma* (« matrice des croyants »), nombreux ont été clercs, décideurs et croyants « du commun » à réclamer de mettre leurs pas dans ceux des « Sages Anciens » (*Salaf Salih*<sup>1</sup>).

**Mohamed-Ali ADRAOUI**



Visiting Senior Research Fellow au Middle East Institute de l'Université nationale de Singapour.



À l'époque contemporaine, les chercheurs ont pris l'habitude de distinguer les courants salafis en trois catégories<sup>2</sup> (bien que les évolutions récentes dans le monde arabe ainsi que les phénomènes d'hybridation et de passage d'une conception à une autre incitent à garder à l'esprit qu'il

(1) Cette expression désigne dans la tradition musulmane telle qu'elle a été construite et codifiée au fil des siècles, depuis l'apostolat de Muhammad (571-632), les générations de fidèles ayant vécu à l'époque de ce dernier, puis celles qui leur ont immédiatement succédé et celles qui sont venues après celles-ci. Plus généralement, est « salafie » toute personne choisissant de s'inspirer et de reproduire la foi et la pratique des fidèles étant censés avoir puisé à la source paradigmatique qui est celle du Prophète, incarnation des vertus islamiques faites homme. Il est donc question d'une éthique fondamentaliste, au sens premier du terme, en ce que la norme la plus ancienne est présentée comme la plus « pure ». La racine *s-l-f* en arabe est celle de l'antériorité par opposition à *kh-l-f* qui est celle de la postériorité (et qui, à titre d'exemple, donne le terme « calife » (*khalif*) qui désigne celui qui vient après (le Prophète)). Lire Haykel (B.), 2009, «On the Nature of Salafi Thought and Action», in Meijer (R.) (ed.), *Global Salafism. Islam's New Religious Movement*, London, Hust & Company, p.33-57, p.38.

(2) Lire Wiktorowicz (Q.), 2006, «Anatomy of the Salafi Movement», *Studies in Conflict & Terrorism*, vol.29, n°3, April-May, p.207-239; Amghar (S.), 2011, *Le salafisme d'aujourd'hui. Mouvements sectaires en Occident*, Paris, Michalon ; Rougier (B.) (dir.), 2008, *Qu'est-ce que le salafisme ?*, Paris, PUF, Proche-Orient ; Adraoui (M.-A.), 2013, *Du Golfe aux banlieues. Le salafisme mondialisé*, Paris, PUF, Proche-Orient.

s'agit d'abord d'idéaux types). Il existe une compréhension du salafisme principalement animée du désir de réformer, sur une base d'abord individuelle puis communautaire, les mœurs supposées « déviantes » des musulmans. Sur un plan politique, cela engendre une défiance fondatrice de l'anarchie et des phénomènes de contestation de l'ordre gouvernant en place. Quand bien même le « détenteur de l'autorité » (*wali al-amr*) serait défaillant au point de vue religieux, il est de fait légitime tant qu'il ne franchit pas ostensiblement les limites de l'injonction religieuse. Les adeptes ont la violence en horreur en ce qu'elle incarne la sédition contre laquelle tout croyant doit s'ériger puisque son déchaînement va jusqu'à menacer l'ordre social et la possibilité de déployer au quotidien son « orthodoxie ». Une autre conception du salafisme est synonyme d'une nouvelle génération d'islamistes<sup>3</sup> dans la mesure où, en vertu d'un projet également « orthodoxe » pour la société, les outils modernes du militantisme politique (partis organisés, manifestations, participation aux élections, animation de journaux...) sont légitimés<sup>4</sup>. Enfin, une dernière acception du salafisme voit ses thuriféraires se projeter au niveau transnational en raison d'un projet politique, à vocation révolutionnaire<sup>5</sup> et visant l'instauration d'une autorité politique et religieuse (le califat) régentant le destin de tous les musulmans de par le monde. La principale conséquence en termes de légitimation et d'usage de la violence est non seulement l'agrégation de celle-ci, mais également sa place centrale dans la politisation de ces groupes pour qui le concept de « jihad » (entendu comme la dynamique de mise en conformité aux valeurs et aux injonctions de l'islam) doit s'entendre de manière véhémement et, dès lors, se déployer sans concessions contre les acteurs considérés comme « les ennemis de l'islam » (régimes « apostats », pays occidentaux leur apportant leur soutien...).

Si les justifications religieuses de la violence au cœur de la socialisation salafie jihadiste puisent incontestablement dans une vision sacrale du monde en vertu de laquelle certains musulmans, incarnant une avant-garde capable de porter le fer chez les adversaires de la religion, mènent un combat de nature cosmique, l'émergence de ce

courant convient néanmoins d'être historicisée. En effet, s'intéresser à la problématisation de la violence au sein des mouvements d'inspiration « jihadiste » revient à poser deux questions fondamentales. Tout d'abord, celle-ci présente la particularité d'être inspirée religieusement avant de se décliner au point de vue strictement politique. La raison d'être de l'orthodoxie étant de « rappeler à l'ordre » les coreligionnaires s'éloignant du viatique « authentique », l'usage de violence peut se concevoir comme une déclinaison de la prédication qui peut devenir, dans cette acception, armée. Le droit de mener la « révolution islamique » par ce moyen fait ainsi partie de l'éventail des virtualités, considérées comme légales et légitimes par les clercs, références de ces mouvements, que les croyants peuvent chercher à inscrire dans le réel. D'autre part, il est essentiel de s'intéresser aux différentes temporalités de l'émergence et la consolidation des courants jihadistes à l'âge contemporain. Quels sont, à ce titre, les ressorts de la pensée et de l'action jihadiste à notre époque, plus précisément eu égard aux logiques et aux ruptures dans le déploiement de l'islam politique depuis près d'un siècle ? La déconstruction de la mobilisation à la violence et à la guerre qui est au fondement de l'éthique jihadiste oblige, en effet, de resituer les débats et les évolutions au sein de la sociologie des mouvements influencés par cette matrice idéologique dans le contexte plus vaste des interactions entre les tenants de l'islam fondamentaliste et militant depuis près d'un siècle et leur environnement politique national et international. Cette dimension nous autorise alors à voir dans la socialisation jihadiste avant tout un langage social au travers duquel certaines dynamiques et problématiques centrales des sociétés musulmanes sont révélées<sup>6</sup>.

## Le salafisme jihadiste comme fruit de la réhabilitation d'une acception guerrière et violente du jihad au XX<sup>e</sup> siècle

L'émergence d'une conception potentiellement martiale de l'impératif de corriger spiritualité et pratique, morale

(3) Par opposition notamment aux acteurs historiques de l'islam politique que sont les mouvements héritiers de l'association des Frères musulmans née à la fin des années 1920 en Égypte sous l'influence de Hassan Al-Banna (1906-1949) et qui essaimera dans tout le monde musulman et même au-delà dans le but de réorienter les sociétés majoritairement musulmanes vers davantage de conformité aux normes morales, mais également juridiques et politiques présentées comme constitutives de l'éthos islamique. C'est ainsi que les croyants choisissant d'opérer une telle rupture se feront appelés *islamawiyoun* (« islamistes » soit des fidèles lucides et conscients des implications autres que simplement morales de la religion). Lire Carré (O.) et Seurat (M.), 2001, *Les Frères musulmans : 1928-1982*, Paris, L'Harmattan, Comprendre le Moyen-Orient.

(4) Ces partis salafis ont notamment tiré profit de l'ouverture de l'espace politique consécutive aux dynamiques révolutionnaires dans certains pays arabes depuis 2010 (Tunisie et Égypte notamment).

(5) Lire Amghar (S.), 2006, « Le salafisme en Europe : la mouvance polymorphe d'une radicalisation », *Politique étrangère*, N° 1, printemps, p. 65-78.

(6) Nous retrouvons ici la vision de la socialisation qui est celle de George Simmel : « *Tout ce qui se manifeste dans les individus, lieux immédiats et concrets de toute réalité historique, sous forme de tendances, intérêts, fins, inclinations, conformité et mobilité psychique, à partir de quoi ou à propos de quoi ils exercent une influence sur autrui ou bien en subissent un, tout cela je le désigne comme le contenu, en quelque sorte la matière, de la socialisation* », *Sociologie et épistémologie*, Paris, PUF, 1981.

et action, conception nommée jihad, fait écho à deux formes concrètes de déclinaison de l'identité musulmane au XX<sup>e</sup> siècle. Les deux représentent indéniablement une rupture en matière de compréhension des normes religieuses contenues dans le sunnisme jusqu'à l'époque contemporaine. En réactivant un droit à la guerre théorisé au cours des siècles par certains docteurs de la foi, les théoriciens, cadres et militants jihadistes entendent s'inscrire au sein de deux temporalités structurantes.

### **Le salafisme jihadiste s'inscrit, pour partie, dans la lignée de l'islam politique**

Le premier ressort de cette éthique de la violence est la croyance sociale d'une décadence de l'islam, entendu comme fait civilisationnel, contre laquelle seul un activisme conscientisé comme tel permet de s'ériger. En cela, le jihadisme, tel qu'il est compris, s'inscrit clairement dans l'histoire de l'islamisme tel que ce mouvement de pensée et d'action se dessine à partir de 1928 en Égypte. La crise caractérisant « la conscience musulmane » est mise au passif des musulmans eux-mêmes qui ont délaissé les enseignements censément « authentiques » de leur religion. Posé comme l'infrastructure de l'évolution historique, l'islam, en tant que dogme, pratique culturelle et norme comportementale, est le facteur qui, en dernière instance, décide de l'atonie ou de l'avancée civilisationnelle des sociétés cultivant son héritage. Ainsi, la compréhension « orthodoxe » du corpus religieux constitue le moteur du « réveil » des peuples musulmans, majoritairement placés sous la domination européenne à l'époque, celle-ci pouvant, si les circonstances l'imposent, prendre la forme d'un combat contre les acteurs présentés comme co-responsables de l'abaissement des musulmans de par le monde. Le recours à une forme politisée et potentiellement violente est d'ailleurs mis en avant comme envisageable, si les circonstances l'imposent, dans les écrits du fondateur du mouvement des Frères musulmans et la charte du mouvement : « *Dieu est notre but, le Prophète notre chef, le Coran notre constitution, le jihad notre martyr notre plus grande espérance* ».

### **Le salafisme jihadiste s'est nourri de la confrontation avec les États en place**

Néanmoins, ce n'est pas tant l'idéologie originale des Frères musulmans qui explique la systématisation intellectuelle du recours au jihad comme manière de redresser le corps musulman à une époque où nombre de ses parties sont sous contrôle étranger. La théorisation d'une forme, autrement plus fonctionnelle et, d'une certaine manière, utilitaire, réaliste et acrimonieuse du combat pour l'islam doit, en effet, se comprendre à la lumière d'une dynamique double. La première, comme nous venons de le voir, est celle de l'islam politique, chargé dès l'origine de « rétablir l'islam dans ses droits ». Cependant, ce qui, après la mort du Guide (assassiné en 1949) et la crise d'identité et de leadership, va caractériser l'organisation (passée, entre-temps, d'acteur caritatif à mouvement politique de masse puissant tourné vers la conquête du pouvoir en vue d'instaurer un État régi par les injonctions de la religion (*chari'a*)), instaure le jihad comme paradigme de l'action politique et religieuse est le retour fait par certains théoriciens « fréristes » sur ce qui passe pour un échec du « mouvement islamique<sup>7</sup> ». Le rôle de celui qui se propose alors d'axiomatiser l'agenda de ce dernier, Sayyed Qotb (1906-1966<sup>8</sup>), est central dans l'apparition d'un appareil conceptuel dont le principe fondamental tient au couplage des notions religieuses d'anathème et de jihad légitime et quasi obligatoire.

La rupture induite par l'œuvre et la pensée de Qotb est souvent présentée comme l'événement à partir duquel les courants islamistes, désireux de réfléchir aux raisons de leur incapacité à prendre le pouvoir<sup>9</sup>, vont se doter d'une armature idéologique faisant muter une partie de l'islam politique vers une radicalisation plus prononcée, prélude à l'apparition d'une offre exclusivement « jihadiste<sup>10</sup> ». Écrivain jadis proche des mouvements de gauche égyptiens, Qotb entreprend d'expliquer à une génération d'islamistes orpheline depuis la mort de Hassan Al-Banna les raisons de l'incapacité à transformer la société et l'État (dans la conception islamiste qui prévaut à l'époque, en réalité la société par l'État). Sa réflexion l'amène à constater « la trahison » des dirigeants à la tête des pays musulmans, au premier rang desquels l'Égypte nassérienne. Bien

(7) Nom donné par les *ikhwan* (« Frères ») à leur association prédicatrice, sociale et politique.

(8) Lire Carré (O.), 2004, *Mystique et politique. Le Coran des islamistes*, Paris, Cerf ; Carré (O.) et Seurat (M.), *Les Frères Musulmans*, op.cit. ; Kepel (G.), 2012, *Le Prophète et Pharaon. Les mouvements islamistes dans l'Égypte contemporaine*, Paris, Folio ; Elshobaki (A.), 2009, *Les Frères Musulmans Des origines à nos jours*, Paris, Karthala.

(9) Notamment dans les années 1950 en Égypte lorsque, après avoir appuyé le coup d'État militaire des Officiers libres (dirigé notamment par Nasser) contre la monarchie, les Frères, espérant l'avènement d'un État conforme à leurs vues ont apporté leur soutien à ce changement de régime. Lire Aclimandos (T.), 2001, « Regard rétrospectif sur la Révolution égyptienne ou le 23 juillet 1952 », *Égypte-Monde arabe*, Alléaume (G.) (dir.), n° 4-5, p.15-39.

(10) Bozarslan (H.), 2008, *Une histoire de la violence au Moyen-Orient*, Paris, La découverte.

que ceux-ci se disent « princes musulmans », tirant leur légitimité et leur assise populaire de leur service de la religion, les croyants « lucides » ne peuvent les prendre au mot et sont obligés de constater leur « forfaiture ». Parmi les nombreux « chefs d'inculpation » retenus par

LA MAJORITÉ DES ISLAMISTES  
SE TROMPE EN POSTULANT  
QUE LA PRÉDICATION,  
LE TRAVAIL SOCIAL ET  
L'ACTIVISME POLITIQUE  
MÈNERONT VERS UNE SOCIÉTÉ  
ET UN ÉTAT CONFORMES  
À LEURS OPINIONS. DANS  
L'ÉPREUVE DE FORCE, LE  
POUVOIR EST SOUVENT PLUS  
FORT COMME LE MONTRENT  
L'INCARCÉRATION ET LA  
CONDAMNATION À MORT DE  
NOMBREUX IKHWAN APRÈS  
LE COUP D'ÉTAT, UNE FOIS  
QU'ILS S'ÉTAIENT RETOURNÉS  
CONTRE LES MILITAIRES.

le théoricien frériste contre Nasser et son régime, le fait d'arbore l'idéologie panarabiste (là où la finalité du mouvement islamique est l'unification des peuples d'islam de par le monde), au demeurant séculière, et de se revendiquer d'une vision politique de gauche (bien que non communiste) figurent en si bonne place qu'il les érige en « idoles modernes » dont une « avant-garde » (*tali'a*) doit viser la destruction pour bâtir sur ses décombres un État régi par les règles exclusives de l'islam. En prêtant, à ses yeux, allégeance à des principes non islamiques, « le prince pervers » a fait retomber l'Égypte dans le paganisme (*jabiliyya*) contre lequel l'islam est né. Décrétant l'expulsion de la société et de l'État en dehors de la sphère de l'islam (*takfir*), Qotb induit bon an mal an une révolution conceptuelle et symbolique qui ne va pas tarder à se traduire

politiquement. Pour avoir, selon lui, entrepris d'exercer le pouvoir sans tenir compte des préceptes sacrés (et pris en chasse volontairement les représentants, à ses yeux, de l'islam « authentique » que sont les Frères musulmans), Nasser a commis une faute impardonnable qui est celle d'avoir retiré à Dieu Sa souveraineté sur le monde terrestre (*hakimiyya*). Dès lors, il revient à une génération de fidèles conscients de leur tâche de lutter contre ce nouveau « paganisme » en ayant recours à une compréhension politisée, violente et révolutionnaire du

jihad. Cette « avant-garde » doit, afin de réussir, suivre les jalons posés sur sa route par le penseur ayant compris le sens de l'histoire des États (à ses yeux faussement) musulmans à son époque<sup>11</sup>.

La violence qu'il inspire alors doit se comprendre, dans son esprit, comme la réaction légitime et, d'une certaine façon utilitaire, pour restaurer sa religion dans ses droits inaliénables. En feignant de servir l'islam pour mieux se tourner vers « les idoles » de l'époque, les princes musulmans ont mené non seulement les peuples qu'ils étaient censés servir « islamiquement » à leur perte, mais ont surtout « trahi » Dieu. La majorité des islamistes se trompe en postulant que la prédication, le travail social et l'activisme politique mèneront vers une société et un État conformes à leurs opinions. Dans l'épreuve de force, le pouvoir est souvent plus fort comme le montrent l'incarcération et la condamnation à mort de nombreux *ikhwan* après le coup d'État, une fois qu'ils s'étaient retournés contre les militaires. Le recours à la violence a donc ici une triple fonction : épargner au mouvement islamique des épreuves dont il n'est pas certain de sortir vainqueur, punir des dirigeants que les musulmans sincères n'ont plus d'autre choix que d'excommunier et hâter la construction d'un État islamique dont la législation serait dérivée directement du corpus religieux.

**La temporalité géopolitique :  
la matrice afghane.**

**La gestation d'une idéologie  
violente et transnationale**

En théorisant le droit à une insurrection contre les régimes « fausement » islamiques, Qotb axiomatise un projet, lequel nécessite d'être porté des groupes organisés, qui, minoritaires dans un premier temps dans l'Égypte des années 1970, vont tenter de renverser ce qu'ils appréhendent comme des structures iniques de domination se couvrant de rhétorique religieuse pour mieux tromper le peuple. C'est ainsi que certains mouvements tel que *Tanzim al-Jihad* (« L'organisation du jihad ») vont voir le jour de manière à drainer les générations de « qotbistes<sup>12</sup> » (souvent des jeunes éduqués enfants par l'exode rural massif que connaît le pays à cette époque) vers une violence programmatique supposée rétablir l'islam dans ses droits, une fois que les potentats

(11) Qotb est notamment l'auteur d'un ouvrage présenté comme le *vade-mecum* des islamistes et qui lui vaudra non seulement l'emprisonnement, mais surtout la mort par pendaison en 1966 pour le caractère subversif de son œuvre : *Jalons sur la route (Ma'alim fil-Tariq)*, dont l'influence est immense sur les courants jihadistes jusqu'à aujourd'hui.

(12) Carré (O.) et Seurat (M.), *Les Frères Musulmans*, op.cit.

« traîtres à la religion ») auront été éliminés. Jusqu'au début des années 1980 et l'assassinat du successeur de Nasser, Anouar Al-Sadate (en 1981), la société égyptienne va expérimenter les prémices du jihad violent mené contre les « faux représentants de l'islam ». Un membre de cette organisation, Adessalam Farag (mort exécuté en 1982) ira même jusqu'à écrire un texte devenu central dans la littérature jihadiste qu'il nomme *Al-Farida al-Ghaïba* (« L'impératif occulté<sup>13</sup> ») faisant par-là référence au jihad compris comme une lutte armée et structurante de la société musulmane qu'il théorise comme le sixième pilier de la religion musulmane (avec l'attestation de foi, la prière rituelle, le jeûne lors du mois de Ramadan, l'aumône purificatrice et le pèlerinage à La Mecque), à ceci près que, d'après lui, ce dernier est tombé en déshérence, les croyants ayant oublié sa centralité, ce qui constitue l'une des raisons de leur déchéance.

La géopolitique mondiale va alors rencontrer l'histoire de l'islam politique égyptien pour voir certains de ses cadres et militants rejoindre au tournant de la décennie 1980 la lutte contre l'URSS sur le théâtre afghan. C'est ainsi que certains islamistes radicaux socialisés dans un contexte de lutte acharnée contre l'ennemi « proche » (le régime abusant son islamité et menant une politique contraire à l'islam) vont se retrouver à défier « l'ennemi lointain » (la puissance non musulmane prenant pour cible des coreligionnaires ainsi qu'une « terre d'islam », ce qui constitue une autre cause de jihad<sup>14</sup>). La temporalité égyptienne va alors être mise en lien avec une demande sociale de radicalité transnationale puisque émanant de groupes sociaux différents (Arabie saoudite, Algérie...) déclenchant ainsi une hybridation entre le militantisme frériste et une acception également rigoureuse et clivante de l'islam trouvant son origine dans le contrat social saoudien depuis la décennie 1920. Appelée, par certains « wahabisme », construction religieuse s'inscrivant dans l'histoire pluriséculaire du salafisme<sup>15</sup>, cette école va renforcer la propension à l'excommunication déjà présente dans l'idéologie des *jama'at islamiyya* (« associations islamiques » se réclamant de l'héritage de Qotb) égyptiennes ayant vu le jour lors de la décennie 1970. La radicalité accrue contenue dans cette hybridation va alors viser le monde comme champ d'expérimentation,

l'une des manifestations les plus frappantes étant sans contester la création d'une organisation déterritorialisée visant l'établissement d'un régime islamique transnational et légitimant, pour ce faire, le jihad véhément (Al-Qaïda autour du Saoudien Oussama Ben Laden, de l'Égyptien Ayman Al-Zawahiri (proche de Farag) et du Palestinien Abdallah Azzam<sup>16</sup>).

## La temporalité sociale : un besoin organique de violence ?

Les mouvements jihadistes contemporains, y compris ceux qui, aujourd'hui, recherchent une forme de territorialisation par le biais de la création étatique *ex nibilo* au sein d'une société fortement éprouvée et traumatisée par l'instrumentalisation de la diversité ethnique et confessionnelle (Syrie, Irak, Yémen, Mali...) n'en restent pas moins des producteurs de sens religieux, à travers lesquels une demande sociale de violence est canalisée et cadrée religieusement. Si les débats sur la nature de l'ennemi, la meilleure manière de s'y opposer et de le vaincre sont légion au sein des communautés jihadistes<sup>17</sup>, l'analyse sociologique permet d'historiciser les recours à ce registre à la fois symbolique et politique par des groupes choisissant de transformer des conditions sociales préexistantes en motifs de révolte en mobilisant l'idiome sacré.

L'aspect relationnel des phénomènes de théorisation et de recours à la violence, y compris la plus exacerbée, à tout le moins lorsque celle-ci concerne « l'ennemi proche », fait écho au lien, mis en évidence par Georg Simmel, entre une éthique comportementale (et la morale à laquelle elle fait écho) et les structures de la société dans laquelle celle-ci s'insère. Selon ce dernier, toute forme de socialisation (jihadiste ici pour ce qui nous concerne) renvoie au processus qu'il définit comme la « structuration de la juxtaposition solitaire des individus par des forces d'existence commune et solidaire<sup>18</sup> ». La principale incidence d'un éloignement des justifications religieuses des acteurs est la restitution du phénomène jihadiste dans un cadre analytique plus large. Le cloisonnement des champs politiques nationaux, pour des générations en

(13) Kepel (G.), *Le Prophète et Pharaon*, op.cit.

(14) Pour une analyse approfondie de la dialectique ennemi proche/ennemi lointain, lire Kepel (G.), 2004, *Fitna. Guerre au cœur de l'islam*, Paris, Gallimard.

(15) Lire Mouline (N.), 2011, *Les clercs de l'islam. Autorité religieuse et pouvoir politique en Arabie saoudite (XVIII-XXIe siècles)*, Paris, PUF, Proche-Orient.

(16) Lire Filiu (J.-P.), 2001, *La véritable histoire d'Al-Qaïda*, Paris, Fayard ; Kepel (G.) et Milelli (J.-P.) (dir.), 2008, *Al-Qaïda dans le texte*, Paris, PUF, Proche-Orient.

(17) Lire Lohker (R.) and Abu-Hamedh (T.) (eds), 2014, *Jihadist Thought and Ideology*, Berlin, Logos verlag Berlin GmbH.

(18) Simmel (G.), *Sociologie et épistémologie*, op.cit.

nombre croissant de personnes recherchant l'amélioration de leurs conditions de vie et une forme d'absolutisme religieux présenté comme le fruit du combat éternel entre le bien et le mal, explique sans conteste la genèse de l'idéologie jihadiste au XX<sup>e</sup> siècle. Le changement de dimension observé dans la décennie 1980 et l'avènement d'une conception dénationalisée, transnationale et déterritorialisée après le départ des troupes soviétiques d'Afghanistan et le retournement des groupes jihadistes contre l'Arabie saoudite au moment de la guerre du Golfe (ce pays ayant choisi de renforcer l'alliance avec les États-Unis alors que Ben Laden et ses combattants se proposaient d'assurer eux-mêmes la défense du territoire), peut ainsi se voir comme l'agrégation de différentes générations de jeunes gens ayant convergé vers l'Afghanistan pour réactualiser le pacte originel de l'islamisme et, ce faisant, abandonner toute référence à la construction d'une société islamique dans un pays précis. Faisant évoluer l'utopie fondatrice vers un désir de révolution mondiale par la violence, le jihadisme s'est retrouvé à coïncider avec l'aspiration massive de certaines générations issues du monde musulman à faire de la politique alors même que le théâtre national leur était interdit. Interprétant le départ soviétique comme l'illustration de la justesse de leur combat et la résultante de l'agrément divin, la décennie 1990 verra ce camp se tourner plus énergiquement vers de nouveaux ennemis, à commencer par les États-Unis, « ennemi lointain » sans l'aide duquel, d'après leur conception politique, les régimes « apostats » n'auraient pu rester en place. Les attaques contre New York et Washington le 11 septembre 2001 s'inscrivent ainsi dans la transnationalité du combat correspondant à la déterritorialisation de l'idéologie<sup>19</sup>.

La temporalité immédiatement contemporaine, qui est celle de groupes jihadistes concourant pour la conquête du pouvoir là où des régimes établis vacillent les uns après les autres, met également en lumière le caractère organique, voire consubstantiel, de la demande de violence qui est celle de sociétés engagées dans un processus de recherche d'ouverture politique (censée pour les jihadistes mener vers l'avènement d'un État répondant à leurs vues religieuses) au sein de systèmes de pouvoirs structurellement réfractaires à sa prise en considération. Outre, dès lors, l'emploi du langage politique de l'islam comme ressource symbolique et pratique pour contester un ordre largement disqualifié (et qui en retour, comme en Syrie et en Irak aujourd'hui n'hésite pas à désigner le jihadisme comme ennemi commun dans une logique de stratégie de survie), celui d'une violence à la fois rédemptrice et fonctionnelle ne peut se comprendre en dehors de l'étude de l'interaction problématique entre groupes religieux interdits de parole<sup>20</sup> et régimes incapables d'entendre sous peine d'être emportés par le flot de protestations. En cela, le passage d'une dimension utilitaire de la violence, au sein des communautés jihadites, à un aspect organique (« la violence pour la violence ») restera sans doute comme l'un des résultats les plus frappants de plusieurs décennies d'autocratie et de prohibition du pluralisme dans de nombreux pays du monde musulman contemporain ■

(19) Roy (O.), 2004, *L'islam mondialisé*, Seuil.

(20) L'une des illustrations les plus marquantes de cette dialectique est sans doute, au moment de la chute du Président Moubarak en 2011, la décision de l'un des dirigeants historiques de l'Organisation du jihad en Égypte, Abbud Al-Zumar, d'abandonner toute stratégie politique fondée sur l'emploi de la violence dès lors que l'État pouvait être conquis par d'autres voies.

# L'apport de la psychologie et de la psychiatrie dans la connaissance des phénomènes de radicalisation et de terrorisme

Michel BÉNÉZECH, Nicolas ESTANO

## Introduction

Les récents attentats et tentatives d'attentats, liés à la mouvance islamiste commis sur le sol français, font ressortir des questionnements sur ce qui pousse un individu à choisir le chemin de la lutte armée dans le cadre de croyances religieuses détournées. Le fanatisme dans les religions monothéistes a en effet toujours existé [Diderot, D'Alembert, 1751]. Nous tenterons dans cet article de présenter brièvement ce que la psychologie et la psychiatrie médico-légale peuvent nous apporter dans la compréhension de ces mouvements et sur les processus sous-tendant le basculement d'individus dans le terrorisme<sup>1</sup>.

## Considérations générales

Le terrorisme se caractérise par le fait de mener des actions violentes et intimidatoires afin d'instaurer un climat

de peur, de panique, permettant de modifier rapidement la conscience des populations dans le but d'aboutir à un changement de société. Il s'agit d'une violence idéologiquement motivée (politique, religieuse), commise par des individus, des groupes d'individus ou des agents missionnés ou soutenus par un État dans le but de transformer ou d'altérer en profondeur un système politique. Hoffman [2006] fait d'emblée la distinction entre le véritable terroriste et l'assassin dément, lunatique (*lunatic*), qui peuvent tous deux utiliser des tactiques identiques (bombes, tirs) et parfois avoir le même objectif (la mort d'un leader politique), mais le premier cherche à modifier un système social alors que le but du second est intrinsèquement idiosyncrasique, égocentré et personnel [Hoffman, 2006].

Malgré la variété des profils des auteurs et des organisations terroristes (extrémismes de droite ou de gauche, mouvements séparatistes, islam avec Al Qaïda, Jemaah Islamiyah Group, etc.), quelques mécanismes psychologiques individuels ou collectifs paraissent être communs et se retrouver fréquemment. Certains auteurs ont tenté de détecter dans le discours tenu par Mohamed

### Michel BÉNÉZECH



Médecin-chef honoraire des hôpitaux psychiatriques, expert judiciaire honoraire et conseiller scientifique de la Gendarmerie nationale. Il a enseigné la médecine légale et le droit privé à l'Université de Bordeaux et dirigé le service médico-psychologique régional des prisons de Bordeaux.

### Nicolas ESTANO



Psychologue clinicien, titulaire d'un Master Professionnel et d'un Master Recherche de l'université Paris 7, complété par un échange universitaire aux USA (UMass Boston). Psychologue Expert Près la Cour d'Appel de Versailles, il a publié plusieurs articles portant sur le thème du passage à l'acte criminel.

(1) Le lecteur pourra se procurer l'intégralité de ce document de travail par mail : [michel.benezech@gmail.com](mailto:michel.benezech@gmail.com) ; [nicolas.estano@gmail.com](mailto:nicolas.estano@gmail.com)



Merah, durant les négociations, des axes d'analyses. Il en ressort que 17 % du temps de négociation portait sur les justifications religieuses, 13 % sur le parcours initiatique [Marchand, 2014]. Cela met l'accent sur la dimension idéologique et l'apprentissage nécessaire à un jeune homme pour basculer et adhérer à l'action violente. Le terrorisme a par ailleurs des conséquences négatives sur la santé mentale des populations ciblées et des victimes civiles, celles possédant des croyances religieuses ou une spiritualité forte étant mieux protégées contre les conséquences psychotraumatiques des attentats [Fisher, 2008].

Dans son étude, Loza [2007] constate que les auteurs d'actes terroristes sont majoritairement des hommes qui entrent jeunes, entre 17 et 26 ans, dans le djihadisme. Ils sont souvent issus de familles appartenant aux classes moyennes et ils ont obtenu de bons résultats scolaires ou professionnels. Citant Hudson, cet auteur note que

ceux qui agissent criminellement dans leur propre pays sont fréquemment d'un niveau éducatif et professionnel médiocre, voire sans emploi et éloignés des interactions sociales. Concernant les terroristes qui voyagent en occident, 70 % se sont ralliés au djihad dans un pays étranger et étaient fortement idéalistes. Les leaders de ces groupes sont souvent plus âgés d'une quinzaine d'années et possèdent un charisme qui entraîne un grand respect de la part de leurs disciples et exécutants. Ils sont considérés comme ayant une grande connaissance de l'islam et très influents.

Notons que la recherche de Corner et Gill [2015], contrairement à l'étude de Loza, ne relève pas chez les auteurs d'actes terroristes un isolement social prédominant. On peut penser que l'adhésion des étrangers à une idéologie religieuse se produirait au moment où ces expatriés chercheraient à retrouver des éléments culturels de leurs racines

et qu'ils se verraient proposer à cette occasion une mystique radicale et extrémiste [Corner, Gill, 2015].

## Psychopathologie et fanatisme

### La psychose

La conviction délirante signe le degré d'attachement d'un psychotique à son délire alors que la croyance religieuse, de par l'impossibilité d'établir la réalité ontologique, induit cette « conviction » nécessaire à tout croyant pour adhérer au dogme. Pour autant, peut-on considérer le croyant comme un « délirant »? Sprinzak [2001] insiste sur la mégalomanie de certains dirigeants extrémistes qui veulent changer l'histoire : « megalomaniacal hyper-terrorists » [Kruglansky, Bélanger, Gelfand *et al.*, 2013]. Les profils de personnalité des dictateurs correspondent

fréquemment à celui d'une personnalité de fonctionnement paranoïaque et de dimension mégalomane (de Staline à Hitler, aux gourous de groupes sectaires), mais les suiveurs ? Les personnes qui adhèrent à l'idéologie paranoïaque du « nous contre eux » sont-elles des malades psychotiques par contagion ?

Pour des raisons évidentes, liées au secret relatif à des opérations terroristes « majeures », type 11 septembre, les personnes présentant une pathologie schizophrénique active se voient souvent « évincées » du processus de « recrutement ». Ce n'est pas du fait d'une prétendue impossibilité à accomplir des actes rationnels, qui n'est pas vérifiée empiriquement, mais plutôt dans un risque sur le long terme quant au manque de discrétion indispensable pour des attentats de vaste ampleur. Fein et Vossekul [1999] soulignent « le cas d'individus atteints de troubles mentaux et tout aussi capables de planifier et d'exécuter efficacement des comportements que ceux sans diagnostic psychiatrique » [Corner, Gill, 2015].

Le cas d'A. Breivik illustrera cette intrication entre un acte méticuleusement préparé, planifié et exécuté et pourtant sous-tendu par des croyances pour le moins paranoïques. La justice norvégienne s'est longuement interrogée sur la responsabilité pénale de ce criminel de masse initialement diagnostiqué comme schizophrène délirant. Il importe de ne pas céder à la tentation d'établir des typologies rigides, perdant de vue la singularité essentielle à toute analyse psychocriminologique : « On ne saurait en effet confondre la folie d'un crime avec la folie de son auteur, le crime "fou" ne renvoyant pas forcément à un malade mental grave, et le crime prémédité n'excluant pas obligatoirement une pathologie psychiatrique sévère chez celui qui l'a commis. Il en résulte que l'évaluation du degré de responsabilité pénale des terroristes doit se faire au cas

*Tous ces volontaires de la mort sont animés par une conviction inhumaine, un processus d'exaltation intellectuelle qui fait changer d'échelle de valeurs, une chosification (« réification ») de lui-même et de l'adversaire, une transgression du respect de sa propre vie et de la vie d'autrui*

*par cas, selon des pratiques médico-légales pertinentes, sans se laisser déterminer par la gravité de l'acte criminel ou par l'idéologie fanatique et apocalyptique du groupe auquel le sujet appartient »* [Bénézech, Toutin, 2015].

Concernant les terroristes djihadistes, si l'idéologie à laquelle ils adhèrent possède cette tonalité paranoïaque du « nous contre eux », sont-ils pour autant tous atteints d'un délire passionnel schizophrénique ou paranoïaque ? Les recherches tendent à montrer que les profils des individus recouvrent un spectre large de la « maladie mentale » incluant davantage d'individus « normaux », de personnes atteintes de troubles de la personnalité et du narcissisme que de psychoses décompensées. La plupart des études s'accordent sur l'absence de pathologie mentale invalidante et sur le fait qu'il n'existe pas de trait de personnalité spécifique associé [Bell, 2005 ; Kruglansky *et al.*, 2013 ; Silke, 1998].

### Fanatisme et système paranoïaque

S'il n'existe pas de portrait-robot du terroriste, certains auteurs s'accordent à leur reconnaître quelques caractéristiques communes de personnalité correspondant à la constellation propre du sujet « luttreur fanatique », selon l'expression d'Alonso-Fernández [1997]. Pour cet auteur, les principales caractéristiques du combattant intégriste sont les suivantes : absolutisme d'un système d'idées dans les domaines religieux, sociopolitique et/ou

nationaliste ; surcharge d'affectivité prenant la forme d'une passion absolue installée au centre de la vie psychique du sujet et qui gouverne sa pensée et ses actes (prosélytisme, bellicisme, criminalité) ; possession de la vérité totale ; refus de toute contradiction ; sentiments négatifs de colère, haine, hostilité, vengeance et autres contre ceux qui s'opposent au développement de ses idées ; comportement extrapunitif flagrant ; absence de culpabilité ou de remords ; distorsion de la réalité ; faiblesse du moi manipulé par le self en complicité avec le surmoi et le ça ; narcissisme idéologique non pathologique soit primaire (enfance avec privation affective ou violence familiale) soit secondaire (cohabitation avec un groupe de fanatiques).

Traitant de la psychologie du terroriste volontaire de la mort, Géré [2003] note la fierté du sacrifice, l'absence de délire, la dichotomie de la personnalité avec d'un côté un comportement normal et sensible à la vie et de l'autre un monde intérieur différent au service du devoir sacrificiel, un calme tragique de surface (exaltation et colère contenues) avant l'attentat suicidaire. Tous ces volontaires de la mort sont animés par une conviction inhumaine, un processus d'exaltation intellectuelle qui fait changer d'échelle de valeurs, une chosification (« réification ») de lui-même et de l'adversaire, une transgression du respect de sa propre vie et de la vie d'autrui [Géré, 2003].

Se penchant à son tour sur la question, Squerverer [2007] étudie

en particulier les relations cliniques entre fanatisme et passion amoureuse (exclusivité de l'objet, idéalisation, surestimation, fausseté du jugement, absence de critique et de remords), l'ivresse idéologique et la sensation de triomphe qui en fait « *une manie de l'idéal* », la jouissance qui le rapproche du pervers, le remodelage « *déliquant* » de la réalité qui peut se socialiser en un « *délire de masse* » des groupes terroristes, l'importance et l'intensité des liens maternels (fascination par la figure de la mère castrée que le terroriste veut rendre intègre), le défaut de transmission symbolique et la haine du père qui poussent le sujet à la conversion, la perte des limites dans la foule, l'insensibilité du corps qui ne ressent pas la douleur.

Pour Bouzar [2014], les activistes violents utilisent aussi le thème de la persécution et du complot : « *Il est intéressant de remarquer que les activistes juifs et chrétiens, même s'ils apparaissent actuellement beaucoup moins nombreux que les musulmans, ont les mêmes modes opératoires : c'est le sentiment de persécution qui justifie à leurs yeux leur passage à l'acte, qu'ils ne qualifient jamais d'acte terroriste, mais de "résistance", "d'opération juste", de "manœuvre défensive", de "stratégie rendant nécessaire l'usage de la force"... ils sont dans une lecture paranoïaque de la réalité* ».

Les liens entre la personnalité fanatique et la personnalité paranoïaque sont plus particulièrement étudiés par Litinetskaia et Guelfi [2015]. Ces auteurs soulignent qu'il n'est pas toujours aisé de distinguer entre les deux (« *zone grise* ») et que l'on doit évaluer l'individu sans l'assimiler à son acte, aussi « *fou* » que ce dernier puisse paraître. Ils constatent que la sémiologie fanatique coïncide sur plusieurs points avec celle d'une passion amoureuse exclusive et idolâtrée et que l'« *idée fixe* » est commune aux personnalités fanatiques et paranoïaques. L'idée qui guide un fanatique vient

de l'extérieur, du leader, sans interprétation, adoptée « *à l'emporte-pièce* » ; en revanche, le délire paranoïaque, qui reste habituellement individuel contrairement aux idées fanatiques, naît à l'intérieur de la sphère psychique du sujet avec pour mécanisme l'interprétation.

Ainsi, de nombreux points rapprochent le fanatique du paranoïaque passionnel : fonctionnement en secteur du psychisme ; moment identique de « *révélation* » et de « *vérité* » unique et absolue ; orgueil et certitude d'avoir raison ; exaltation idéologique avec idée fixe prépondérante (idéologie radicale) ; sentiment de supériorité ; fausseté du jugement ; psychorigidité ; méfiance ; intransigeance ; fidélité aveugle à la cause et à un chef charismatique ; obstination ; vécu de conspiration de l'entourage social ; intolérance envers l'opinion d'autrui ; querulence jusqu'au-boutiste ; désignation de boucs émissaires (personnes ou groupes de personnes perçus comme différents, hostiles ou de moindre valeur) ; actes antisociaux ; prosélytisme ; absence d'auto-critique et de remords ; résistance au changement.

## Le terrain psychologique favorable

### La stigmatisation

La théorie criminologique du stigma social, c'est-à-dire de l'étiquetage (*labelling approach*), stipule que l'auteur d'un comportement déviant est blâmé par son entourage social et qu'il s'identifie profondément à la puissance et à la nature de ce marquage, de l'image négative qui lui est imposée. Cette identification mimétique à l'étiquette stigmatisante fait que le sujet adhère et intériorise le rôle social qu'elle implique et qu'il peut devenir un délinquant récidiviste [Addad, Bénézech, 1982]. Selon nous, il existe donc un « *terrain préparatoire* » à la délinquance

d'habitude, un soubassement psychologique qui permet au déviant discriminé d'accepter l'étiquetage négatif ainsi que la fonction qui en découle, faire une carrière criminelle soit individuelle soit au sein d'un groupe marginal (gangs, mafias, organisations terroristes, sectes fondamentalistes).

Ce terrain préparatoire, résultat de base du processus d'internalisation et d'identification de la petite enfance, paraît constitué de divers éléments dont les trois principaux sont les suivants : 1) Sentiment oedipien de culpabilité à l'origine de souffrances, de conduites d'échec et de recherche inconsciente de la punition ; 2) Faille narcissique avec insécurité primitive provoquée par une privation affective maternelle de la première enfance (« *enfants mal aimés* ») et se traduisant par une altération du lien interhumain, de la relation intersubjective ; 3) Carence éducative (« *enfants mal éduqués* ») associée à la carence affective et aux problèmes culturels et confessionnels chez les immigrés (déracinement, écart et choc culturel).

Il résulte de tout ceci un « *contentieux* » de déplaisir, d'agressivité revendicatrice, de culpabilité et d'infériorité avec désir de se venger d'autrui et de retrouver magiquement un paradis perdu resté jusqu'à alors inaccessible [Addad, Bénézech, 1982]. L'adolescent ou la personne vulnérable pourra alors s'identifier de façon durable à des modèles antisociaux et s'intégrer dans une idéologie ou une sous-culture criminelle qui le comprendra, l'acceptera sans le rejeter et donnera un but apparent à sa vie.

### La fragilité existentielle

Nous arrivons ici à un point essentiel, celui du niveau de signification de la vie (*meaning of life*) chez les délinquants par rapport aux personnes de

la population générale. Nous envisageons l'hypothèse que les individus en risque de radicalisation et de terrorisme présentent un niveau abaissé de signification de la vie (carence existentielle) comme chez certains criminels récidivistes [Addad, Bénézech, 1986 ; 1987].

La criminalité active de ces personnes remplit, semble-t-il, leur pauvreté existentielle de base et renforce leur moi en leur permettant de surmonter le handicap de l'anxiété névrosique. L'aspiration pour, d'un côté, la maîtrise, le pouvoir, la capacité et, d'un autre côté, la recherche du plaisir, paraît trouver une réalisation dans le comportement criminel durable qui devient un substitut à l'absence de signification profonde de la vie et donne une vraie raison d'exister à ces personnes profondément enfoncées dans la déviance antisociale [Addad, Bénézech, 1986].

L'idéologie radicale, qui justifie l'action violente comme moyen d'atteindre un but (défense d'un groupe présenté comme menacé ou humilié par la majorité ; faire évoluer les lignes sociales pour favoriser l'accès à un statut meilleur ; reconnaissance d'un État indépendant...), s'ancrerait plus facilement chez des individus traversant une période où ils auraient éprouvé un sentiment de perte de repères : perte du sens à donner à leur vie, de leur importance dans la société, de deuils difficilement vécus, etc. Il s'agirait ici non d'une fragilité narcissique causée par des carences dans le développement psycho-affectif de l'enfant, mais d'un moment de fragilité narcissique pouvant survenir aux différentes étapes de la vie. Ce sont dans ces moments de flottements existentiels, de perte des repères que les sujets seraient les plus à même de se radicaliser.

Cela implique donc soit des adultes confrontés à des échecs, des discriminations, des humiliations répétées ou graves, des souffrances, des pertes (au plan social, affectif, professionnel, voire de foi) soit également des jeunes adultes ou adolescents, à un âge où le sens à donner à sa vie est souvent source d'anxiété. La séduction médiatique (journaux, télévision, Internet) et l'influence par autrui qu'exerce une idéologie religieuse ou politique fanatique sont d'autant plus efficaces qu'elles portent sur une personne jeune, réceptive, au moi fragilisé, au « terrain préparatoire » fait de failles narcissiques et existentielles (colère, honte, humiliation, sentiment d'insignifiance).

Il s'agit ici d'un essai de renarcissisation par un processus psychodynamique antisocial. Notons que pour certains individus, l'incarcération constitue une expérience particulièrement humiliante et réductrice de leur sentiment de valeur existentielle. Elle rend ces personnes hautement vulnérables aux arguments de la radicalisation. Comme le souligne Sageman [2004], la plupart des personnes embrassant la radicalisation n'avaient pas initialement de solides bases religieuses et n'adoptèrent le salafisme qu'à l'entrée dans l'âge adulte [*idem*].

Les travaux récents menés par Kruglanski *et al.* [2013] soulignent que la recherche d'un sens à donner à la vie (*significance*) peut immédiatement faire écho à un besoin d'appartenance dans un groupe. L'appartenance permet un sentiment d'importance ou d'un « sens à travers le dévouement à une cause importante. Cette bascule collectiviste engendrée par cet objectif d'importance à atteindre a deux conséquences immédiates : (a) l'effet d'habilitation

(*empowerment effect*)<sup>2</sup> (d'où l'obtention d'un sentiment d'importance !) en se voyant soi-même comme une part d'une entité plus large et puissante et (b) l'effet de sacrifice, l'inclination à suivre les normes du groupe et/ou agir en son nom quel qu'en soit le prix. En conséquence, lorsque l'idéologie du groupe justifie le terrorisme, elle peut promouvoir le martyr, la violence au nom du groupe ». Le groupe, au sens large, est dans ce cas celui de la minorité se sentant discriminée négativement et qui s'identifie à l'agresseur pour défendre ce qu'elle croit être ses droits légitimes.

## La psychologie des groupes et des foules

En sus d'une centration sur la psychologie individuelle, la psychologie des groupes serait donc pertinente pour comprendre les processus de radicalisation [Moghaddam, 2005]. L'organisation actuelle des cellules terroristes serait de plus en plus décentralisée, loin de ressembler à une structure hiérarchisée avec un commandement central. À défaut de pouvoir centralisateur, ce sont très souvent des liens de parenté ou d'amitié qui cimentent ces groupes [Magouirk, Sageman, Atran, 2008]. Ces cellules comptent habituellement au maximum huit personnes qui obéissent cependant aux « lois » de la psychologie des foules : suggestion, fascination, idéalisation, identification, imitation, soumission, dévotion.

On observe une fusion de l'individu dans le groupe, dans un esprit et un sentiment collectif (« *âme des foules* ») qui estompent les différences de personnalité et l'esprit critique quels que soient la classe sociale d'origine, le niveau d'éducation ou de culture. Cette dissolution de la conscience et

(2) L'effet d'habilitation implique quatre notions : compétence, estime de soi, conscience critique, participation. Cela définit l'acquisition de nouvelles compétences en lien avec des jeux de pouvoirs dans les relations interpersonnelles.

des caractères individuels au profit d'une pensée commune permet l'« unité mentale » de tous et est le résultat de l'effet de masse, du charisme des meneurs, de la toute-puissance de leurs croyances, de leurs personnalités paranoïaques, mégalomaniaques, manipulatrices et haineuses [Moscovici, 1991].

Pour Freud, la foule permet la régression psychique des individus dans la masse, diminue la répression des tendances inconscientes, fait disparaître les inhibitions morales, l'instinct et l'affectivité s'exprimant alors plus intensément. Les valeurs archaïques et les traditions remplacent la raison pour déterminer la conduite de chacun. Les individus agissent uniformément sans même se concerter, comme des automates dépourvus de volonté propre, régressant de plusieurs degrés dans l'échelle de la civilisation [Freud, 2012].

## Typologies et psychiatrie

### Classifications

Pour mémoire, rappelons que le psychiatre américain Hacker reconnaissait trois catégories de terroristes : les idéalistes ou « croisés », les criminels, les fous (anormaux et malades mentaux) [Hacker, 1976].

D. Bouzar, anthropologue, responsable du Centre de prévention contre les dérives sectaires islamiques (CPDSI) et C. Caupenne, ancien négociateur au RAID, décrivent en 2014 cinq catégories de profils :

- « Call of duty » : ou celui qui recherche le combat entre hommes. Le *call of duty* (l'appel du devoir) est le profil type de l'aventurier. Pour le CPDSI, il s'agit d'un jeune qui a cherché à entrer dans l'armée ou dans la police et qui a été refusé. Pour compenser la frustration du rejet de l'institution et avoir sa dose d'adrénaline et de violence,

il choisira sa propre guerre, à la recherche du contact avec les armes et du combat. On peut rapprocher de ce profil celui dépeint par Trévidic [2013] de la « *bête de guerre* » ;

- « Zeus » : ou celui qui recherche la toute-puissance et le pouvoir. Le CPDSI constate qu'il s'agit d'individus « no limit », à la recherche de conduites à risques. Leur maxime principale serait la suivante : « *Ça passe ou ça casse* ». Si « *ça passe* » c'est qu'ils sont immortels et dominants, élevés au niveau de Dieu ;

- « Lancelot » : ou celui qui cherche l'idéal chevaleresque. Dans ce type d'identification, l'individu fanatique ressentirait un fort besoin d'offrir le sacrifice de sa vie pour l'histoire, la postérité et le triomphe de la vérité. Son état d'esprit de missionnaire, obsédé par la théorie du complot contre sa vérité, correspond à : « Je vais vous sauver malgré vous, vous ne comprenez pas mais en fait, je veux votre bien... » ;

- Le « porteur d'eau » : ou celui qui cherche un groupe d'appartenance. Cette catégorie concernerait les individus en quête d'identité, qui ont besoin d'appartenir à un groupe, même s'ils n'ont qu'un rôle d'exécutant de second plan. Lors du retour en France, certains individus ont évoqué des tâches ménagères, la surveillance de prisonniers, voire un rôle de fossoyeur pendant plusieurs semaines ;

- « Sœur Thérèse » : ou celui (celle) qui part pour la cause humanitaire. Il s'agit le plus souvent de jeunes femmes européennes, fréquemment mineures, croyant partir en Syrie pour le « bien » des autres. Mais au lieu d'agir pour l'humanitaire, le but espéré, via les réseaux sociaux, se transforme à l'arrivée en tâches domestiques et en agence matrimoniale qui permet à des hommes de se marier rapidement

avec de jeunes occidentales qu'ils ne connaissent quasiment pas. En Tchétchénie et en Irak, les pertes importantes de terroristes combattants ont été compensées par le recrutement de femmes, alors uniquement pour des missions kamikazes.

### Corrélations médico-psychologiques

Certains professionnels de sécurité s'interrogent sur la qualification de « terroriste » : « *Parfois, on se retrouve face à un terrorisme que je qualifierais presque de pulsionnel* », estime le juge d'instruction Trévidic [2013]. Un spécialiste de l'islamisme radical au ministère de l'Intérieur va plus loin : « *On a de plus en plus affaire à des individus déséquilibrés. Pour moi, on est à la limite du terrorisme et de la pathologie mentale* ».

Pour Bouzar [2014], le discours sur l'exclusion n'expliquerait pas suffisamment le processus de radicalisation. Selon cette personne, il s'agit souvent de jeunes gens « *présentant des personnalités "borderline", qui seraient en recherche de limites, d'où leur extrême violence* ». La plupart d'entre eux ont versé dans la délinquance avant de se tourner vers le djihad : « *C'est la même violence, mais mise au service d'une autre cause. Une cause soi-disant plus pure et donc plus valorisante à leurs yeux* ». Pour Khosrokhavar [2014], l'attrait du fondamentalisme musulman s'explique aussi par son corpus de valeurs simplistes : « *Pour un jeune sans repères, la vision du monde véhiculée par l'intégrisme musulman a ceci de rassurant qu'il est très binaire : un monde divisé entre le bien et le mal, entre les musulmans et les impies, c'est très rassurant* ».

On trouvera sur le tableau 1 les rapprochements possibles entre les profils du CPDSI et certains troubles psychiatriques.

Victoroff [2005], dans une large revue de la littérature, confirme

Tableau 1 - Rapprochements possibles entre les profils du CPDSI et les troubles mentaux [Bénézech et Toutin, 2015]

CPDSI	Pathologies psychiatriques	Motivations, revendications, tempérament
Call of duty	Personnalité psychopathique Personnalité antisociale	Agressivité, utilitarisme, égocentrisme, criminalité, recherche de sensations
Zeus	Personnalité narcissique, antisociale, borderline Personnalité paranoïaque Délire de grandeur	Mégalomanie, toute-puissance, orgueil, dogmatisme, réformisme
Lancelot	Personnalité paranoïaque Délire passionnel	Redresser les torts, récrimination, altruisme morbide, idéalisme passionné
Porteur d'eau	Personnalité dépendante ?	Quête d'identité, sentiments d'infériorité, besoin grégaire et d'être apprécié, réassurance, demande d'aide, éviter la critique
Sœur Thérèse	Idéalisme passionné de la bonté ? Personnalité histrionique ?	Altruisme, amour des autres, dévouement, sympathie, quête d'identité

l'hétérogénéité des « profils » parmi les auteurs d'actes terroristes. Il isolerait toutefois quatre caractéristiques chez le « terroriste », qu'il soit un suiveur ou un leader : « (a) une valence affective élevée concernant une question idéologique ; (b) : un enjeu personnel – tel qu'une forte oppression, une humiliation perçue, ou de la persécution, un irrésistible besoin de gloire, de vengeance ou d'identité, un moteur pour exprimer une agressivité intrinsèque – qui le (la) distingueront de la grande majorité de ceux répondant aux points présents dans le (a) ; (c) : une faible flexibilité cognitive, une faible tolérance pour l'ambiguïté, une forte tendance à l'erreur d'attribution ; (d) la capacité à supprimer les contraintes morales, instinctives et sociales quant au fait de blesser des innocents, que cela soit dû à des facteurs intrinsèques ou acquis et certainement influencés par les trois points précédents ».

Une approche synthétique de l'état d'esprit des militants extrémistes nous est donnée par Stankov *et al.* [2010] : violence, monde méprisable et pouvoir divin. C'est d'abord l'adhésion très forte à la croyance que la violence est un moyen utile

d'atteindre des objectifs personnels et sociaux. C'est ensuite l'identification et la désignation d'un ennemi (politique, économique, religieux) ou la croyance qu'un monde corrompu et vil est la source de la souffrance d'un groupe auquel le sujet appartient. C'est enfin la nécessité que la violence soit positivement appuyée, cautionnée par une autorité supérieure (Dieu/pouvoir divin) ou par une force considérée comme inévitable dans l'histoire de l'humanité (révolutionnaires athées ou communistes). Les auteurs constatent que ces trois composantes psychologiques fondamentales sont communes à l'ensemble des extrémistes, mais que leurs valeurs diffèrent sensiblement selon les pays et les cultures auxquels ils appartiennent [Stankov, Saucier, Knežević, 2010].

## L'auteur solitaire

Si les auteurs d'attentats symboliques et spectaculaires (New York, 2001 ; Londres, 2005) étaient semble-t-il

quasi normaux, mais déterminés, méticuleux et prêts à se sacrifier, les terroristes actuels dans notre pays paraissent privilégier des actes de moindre valeur symbolique, nécessitant une logistique réduite, moins coûteux en temps et en argent et donc moins repérables par les services de renseignements. Dans cette catégorie d'attentat « acte isolé », est-il possible d'identifier les signes indicateurs d'un comportement préparatoire chez des individus qui agissent seuls, ou avec l'aide *a minima* d'un ou deux complices, ayant décidé de finir leurs jours en « martyr » ? La figure du loup solitaire, parfois dénommé sous l'acronyme SIMAD (*Single Individual Massively Destructive*), pose un défi majeur à la sécurité publique par sa dimension imprévisible et l'impossibilité de déjouer le complot à temps. Dans les deux exemples les plus récents, Ghlam et El Khazzani, des circonstances extérieures imprévisibles ont empêché l'exécution des actes, le premier djihadiste présumé s'étant tiré accidentellement une balle dans le pied, tandis que le second a été maîtrisé par l'intervention courageuse de plusieurs passagers.

C'est parmi les auteurs solitaires que l'on a la probabilité de trouver la plus grande variété psychopathologique, allant de la normalité à des troubles schizophréniques ou de l'humeur. Les faits commis à Dijon le 22 décembre 2014 et à Joué-Les-Tours deux jours plus tôt, furent présentés dans les médias comme des attentats djihadistes, mais le premier auteur, bien qu'il ait crié « Dieu est grand », était un homme aux antécédents psychiatriques anciens et graves, et il est possible que l'acte n'ait été qu'une violence pathologique se greffant sur le contexte particulier du moment. Quant au second, si son acte survint quelques jours après des appels de Daech à mettre à mort des policiers ou des non-croyants par tous les

C'est parmi les auteurs solitaires que l'on a la probabilité de trouver la plus grande variété psychopathologique, allant de la normalité à des troubles schizophréniques ou de l'humeur.

moyens possibles, il sera tué dans le commissariat où il était entré armé d'un simple couteau, laissant ses motivations indéterminées.

L'impulsivité, le manque évident de préparation (cibles désignées au hasard, moyen du crime hasardeux, non professionnel) pourraient orienter vers des auteurs présentant des troubles psychiatriques importants. Selon Corner et Gill [2015], c'est chez les auteurs solitaires qu'il existe le plus de malades mentaux au sens large (troubles de la personnalité ou de l'humeur, psychoses, autres) : « La probabilité d'avoir un acteur solitaire avec une maladie mentale est 13,49 fois (intervalle de confiance à 95 % : 4,630-40) supérieure à celle d'avoir un acteur en groupe atteint de maladie mentale... Ceux qui avaient une épouse ou un partenaire qui était impliqué dans un vaste mouvement terroriste avaient 18,07 fois (intervalle de confiance à 95 % : 2,134-152,914) plus de probabilité d'être malades mentaux (test de Fisher ;  $p = .001$ ). Ceux avec des liens de commandement et de contrôle avec les autres avaient moins de probabilité (OR 0,32, intervalle de confiance à 95 % : 0,880-1,178) d'avoir un trouble mental... ».

Ces mêmes auteurs citent les rares études antérieures concernant la fréquence des troubles psychiatriques chez les terroristes : 61 % des « assassins » solitaires ont eu des contacts antérieurs avec les services de santé mentale ; 22 % des solitaires américains sont psychologiquement perturbés contre

8,1 % de ceux appartenant à un groupe ; 31 % des solitaires ont un passé de trouble mental ; 40,4 % des solitaires d'extrême droite souffrent de maladie mentale contre 7,6 % chez les auteurs en groupe. Toujours selon les recherches de Corner et Gill sur 119 terroristes loups solitaires condamnés ou morts comparés à un échantillon représentatif de terroristes opérant en groupe, l'acteur solitaire ayant une épouse ou un partenaire impliqué dans des mouvements terroristes ont 22,2 fois plus de probabilité d'avoir un diagnostic de schizophrénie et 250 fois plus de probabilité de souffrir d'un trouble de l'humeur. Ceux blessant au cours d'un attentat sont 11,3 fois plus à même d'être atteints de schizophrénie et 41,6 fois plus d'être atteints d'un trouble de l'humeur. Par rapport à des auteurs en groupe possédant une forme d'entraînement « paramilitaire », les auteurs solitaires sont enclins à se radicaliser et à passer à l'acte beaucoup plus rapidement, certains évoquant un délai parfois inférieur à 48 heures [Corner, Gill, 2015].

Il n'est pas sans intérêt de noter que parmi les « loups solitaires » auteurs d'attentats dans le monde, les plus nombreux (40 %) sont sans « aucune idéologie précise » [Okomba-Debarice, 2015]. Ce résultat plaide en faveur de la fréquence des troubles mentaux dans cette population.

## Le processus de radicalisation

Selon Moghaddam [2005], l'ensemble de l'opération de recrutement, entraînement et mise en œuvre de l'action terroriste peut prendre moins de 24 heures : « Durant celles-ci, la recrue se voit fournir un ensemble d'attentions

positives, est traitée comme une sorte de célébrité, notamment par le recruteur (qui restera à ses côtés constamment) et par une figure charismatique de la cellule ». Ce sont les « fantassins », choisis uniquement pour mener des opérations violentes ou des opérations suicides. Cette rapidité d'action met en évidence l'importance de la cellule qui fournit un appui logistique (armes, choix de cibles...) à des personnes embrigadées pour passer à l'action et pouvant avoir été séduites par des rhétoriques bien ciblées.

Ainsi, à l'exception d'actes isolés et peu planifiés, quoique « spectaculaires », commis par des individus souffrant de troubles de l'humeur ou d'un délire mystique s'inspirant volontiers des discours diffusés par Daech, la plupart des auteurs d'actes solitaires sont le bras armé d'une cellule organisationnelle pluridisciplinaire et/ou d'un donneur d'ordre éloigné. Par exemple, la filière des Buttes-Chaumont se composait d'individus en interrelations depuis des années, à savoir des djihadistes « historiques » et des criminels de droit commun ayant adopté le choix du terrorisme au nom d'un « islam radical » et recrutés pour leurs connaissances des réseaux d'armements et de flux financiers parallèles. Ces activités illégales (trafics, braquages, etc.) sont souvent source de financement des actions terroristes<sup>3</sup>.

Des études récentes [Crenshaw, 1988, 2006 ; Kruglanski, Bélanger, Gelfand *et al.*, 2013 ; Moghaddam, 2005] portent sur les processus à l'œuvre lors de la radicalisation d'un individu. Nous les résumons ici. Ces mécanismes quasi sectaires sont fondés sur des rencontres virtuelles répétées (Internet, appels téléphoniques, réseaux sociaux) précédant des rencontres physiques. Parfois l'initiation au djihad armé

(3) <http://www.nytimes.com/interactive/2015/01/09/world/europe/links-between-the-charlie-hebdo-suspects.html>

se fait au sein de la famille ou par un groupe d'amis issus du même quartier. À noter que les études psychologiques comparant l'intensité des émotions éprouvées dans les relations en ligne contre celles hors-ligne, montrent que les sentiments « en ligne » sont plus intenses que ceux hors-ligne. Sageman [2008] développa l'importance d'Internet dans le processus de recrutement, notamment la place prépondérante tenue par les forums de discussions « actifs », en comparaison avec les sites « passifs » d'informations.

Les divers processus utilisés établissent une réelle pression des néo « pairs » sur l'individu, l'incitant à des règles de conduite en accord avec l'idéologie présentée. Faraj (1954-1982), l'un des idéologues salafistes « historiques », membre de l'organisation ayant perpétré l'assassinat du président El-Sadate, écrira dans un pamphlet *The neglected duty* : « *Le djihad est un devoir personnel, il n'y a pas besoin de demander la permission à vos parents pour mener le djihad, comme l'ont écrit les juristes ; c'est ainsi similaire à la prière et au jeûne* » [Sageman, 2004]. Il est ainsi fort probable que ce type de rhétorique soit utilisé très fréquemment dans les processus d'endoctrinement d'adolescents ou de jeunes adultes.

La définition ci-dessous de la secte correspond à ce qui est décrit par des personnes ayant abandonné les groupes radicaux auxquels elles appartenaient, ce qui permet de se faire une idée précise des mécanismes utilisés dans l'endoctrinement : « *Une secte c'est : un gourou, leader incontesté, incontestable, aimé et craint, une doctrine de message unique et ultime de salut, un groupe chaleureux et hiérarchisé, qui vont accomplir un conditionnement en plusieurs étapes. La première consistant à séduire et survaloriser. En proposant des réponses simples sur tous*

*les grands thèmes de l'époque. En valorisant le futur adepte et en lui garantissant la connaissance, la liberté, le bonheur. La seconde vise à anesthésier l'esprit critique et la personnalité. Par un état de fatigue provoqué par des activités incessantes comme le démarchage, la formation, la méditation ou la prière. En modifiant les habitudes alimentaires (régime, jeûne), en créant des conditions de vie qui empêchent le futur adepte de prendre le recul nécessaire qui l'autoriserait à réfléchir à ce qu'il fait ou à ce qu'il vit, en réduisant l'intimité jusqu'à la rendre dérisoire comme l'impossibilité d'être seul, l'obligation de se raconter... en modifiant le vocabulaire par un langage scientifique ou religieux qui sonne bien mais n'a de sens qu'à l'intérieur du groupe...<sup>4</sup> ».*

Le processus de radicalisation a été comparé par Moghaddam [2005] à l'ascension d'un « escalier » de cinq étages se rétrécissant jusqu'à l'acte terroriste à son sommet (Figure 1). L'accession à un étage supérieur dépend des places disponibles à ce niveau. Il y aurait tout d'abord, au rez-de-chaussée, la perception d'une équité toute relative et la prédominance de sentiments subjectifs de spoliation, de manque, de dénuement, de frustration, de colère, quelles que soient les conditions matérielles de la vie. Dans le monde, c'est le cas de millions de personnes qui éprouvent des idées d'injustice et de privation et qui remettent plus ou moins en cause le vivre ensemble. Certains, parmi ces mécontents insatisfaits, vont alors monter au premier étage à la recherche de solutions. S'ils n'y trouvent pas la possibilité d'obtenir un changement social et qu'ils estiment qu'ils ne peuvent pas participer aux processus décisionnels, ils seront enclins à continuer l'ascension.

Les individus accédant au deuxième étage, ceux qui perçoivent toujours des injustices et inégalités graves,

ressentent encore de la frustration, du dépit et, sous certaines conditions, sont influencés par des leaders pour déplacer leur agressivité sur un « ennemi » désigné comme le responsable des « blocages ». Les recherches menées en psychologie insistent sur l'importance du rôle de l'impression subjective sur le sentiment de dénuement. « *Runciman (1966) fait la distinction entre la déprivation égoïste, où un individu se sent dépossédé en raison de sa position au sein d'un groupe, et la déprivation fraternelle impliquant des sentiments de dénuement qui émergent en raison de la position d'un groupe d'individus par rapport à celle d'autres groupes. La recherche suggère que la déprivation fraternelle est, sous certaines conditions, un meilleur prédicteur de sentiments de mécontentement parmi les minorités que ne l'est la déprivation égoïste... La déprivation fraternelle peut émerger plus aisément lorsque des membres d'un groupe ont l'impression que le chemin a été bloqué vers un objectif désiré, que leur groupe mériterait ce que d'autres groupes possèdent* » [Moghaddam, 2005].

Les sujets prêts à déplacer leur agressivité physique sur des ennemis et qui recherchent des possibilités de le faire, accèdent au troisième étage. La transformation essentielle est alors un engagement progressif vers la moralité collective des organisations terroristes : rigidification idéologique, rupture psychologique et/ou physique avec l'environnement familial ou social. C'est le début de la radicalisation grâce à l'utilisation d'un ensemble de techniques qui s'exercent à leur encontre : isolation, affiliation, secret, peur. Ces personnes commencent à envisager le terrorisme comme une stratégie justifiée et certaines, qui s'engagent moralement dans cette idéologie, continuent à monter et sont désormais prêtes à être recrutées comme terroristes. Au quatrième étage, maintenant admises

[4] « Les sectes : la définition de l'ADFI », *Bulletin du Syndicat national des psychologues*, avril 1993, 112, p. 3.

dans le secret de l'organisation, on consolide leur radicalisation et on leur apprend à percevoir le monde sur une modalité rigide, teintée d'une vision binaire, « nous contre eux », et à considérer l'action terroriste comme un moyen légitime.

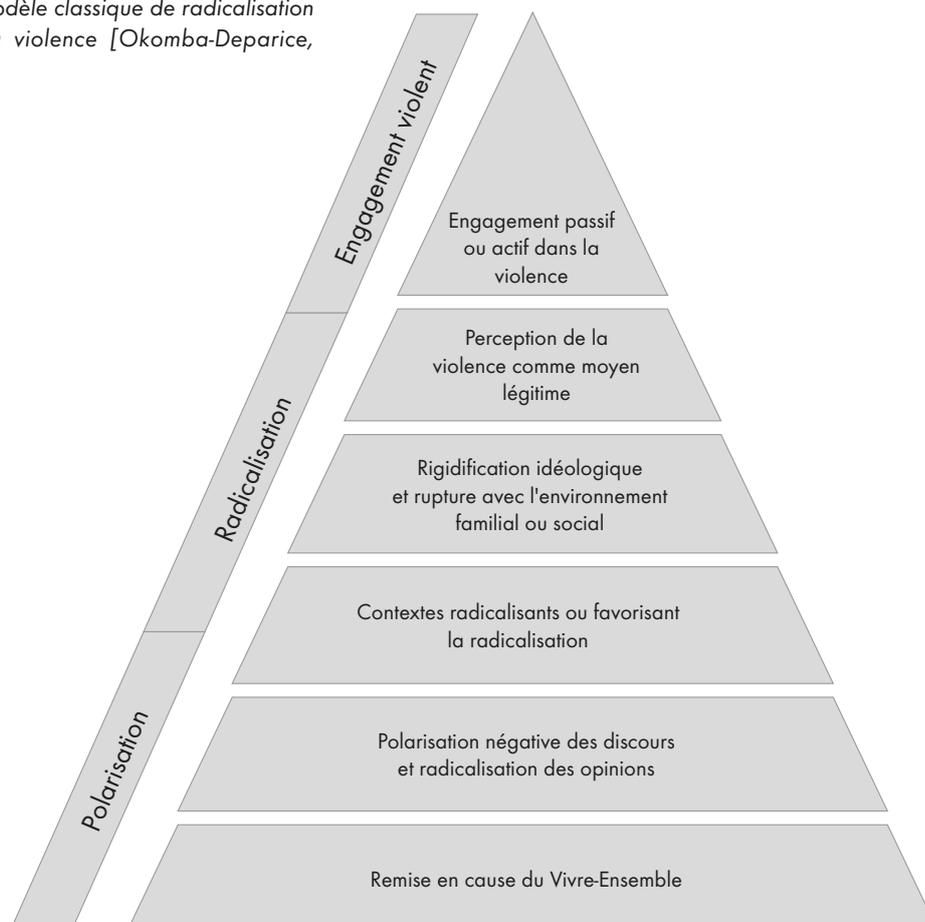
Le leader de la cellule exerce une forte autorité et exige conformité et obéissance. Le groupe comprend généralement quatre à cinq personnes se répartissant en membres à long terme (premiers recrutés) et en « *fantassins* » admis pour mener uniquement des opérations violentes ou suicides. Au cinquième et dernier niveau, quelques rares individus sont choisis et entraînés à mettre de côté les mécanismes inhibiteurs qui pourraient les empêcher d'infliger

des blessures ou tuer autrui, voire eux-mêmes (distanciation psychique). Ils sont prêts à tuer ceux hors de leur groupe (catégorisation). Ils sont maintenant formés et missionnés pour conduire des actions terroristes, n'attendant plus que l'ordre d'agir. C'est l'engagement passif ou actif dans la violence [Moghaddam, 2005].

Pour en arriver à franchir les deux dernières étapes, les personnes sélectionnées sont amenées à adopter de nouveaux cadres de références : abandon des anciennes normes et codes socialement admis auparavant, adoption d'une morale « parallèle » et d'une idéologie légitimant le terrorisme. Leistedt [2013] rappelle les huit procédés fondamentaux préconisés dans les milieux totalitaires,

y compris dans les organisations terroristes, pour modifier les attitudes et comportements : 1) Contrôle du milieu (contrôle total des communications) ; 2) Utilisation d'une rhétorique collectiviste (jargon du groupe) ; 3) Recherche d'une pureté (système de croyance en tout ou rien) ; 4) Confession (les membres doivent révéler leur histoire et leur comportement passé et présent) ; 5) Manipulation mystique (« tu as été choisi pour être là ») ; 6) Prépondérance de la doctrine sur l'individu (syndrome des faux souvenirs) ; 7) Science « sacrée » avec des leaders historiques respectés ; 8) Fournir une réponse existentielle (appartenance du membre à une élite) [Leistedt, 2013].

Figure 1 - Modèle classique de radicalisation menant à la violence [Okomba-Debarice, 2015]



Meloy et Yakeley [2014] proposent une lecture psychodynamique des évolutions émotionnelles présentes aux différentes étapes de la radicalisation vis-à-vis de l'altérité. Là où la colère renvoie à la prise en compte de l'altérité et à ses opinions divergentes, on observerait chez les auteurs isolés radicalisés un passage de la colère vers le mépris puis le dégoût à l'encontre des croyances autres que les leurs. La place de la valeur accordée à autrui est progressivement éliminée. Dans le mépris, il y a condamnation de l'autre, qui apparaît dévalué, puis à mesure de la radicalisation un dégoût profond s'installe. Ces auteurs suggèrent d'observer sur les réseaux sociaux l'évolution séquentielle : colère -> mépris -> dégoût comme pouvant être des signaux émotionnels précurseurs d'actes violents.

On relèvera que l'idéologie terroriste va utiliser des méthodes rhétoriques et sémantiques qui vont délégitimer les cibles des violences en les présentant souvent comme infra-humaines : « *porcs* », « *vermines* », « *infidèles* » qui ne méritent pas la considération dévolue aux personnes [Bandura, 1999 ; Bar-Tal, 1990]. Sageman [2004], dans son étude sur le djihadisme, permet de comprendre la logique (auto) destructrice observée lors des tentatives de négociations : « *le mouvement [...] ne doit jamais déposer les armes peu importe les pertes. Si la retraite est coupée, et que la chute est imminente, le mujahid (combattant du djihad) doit combattre "de telle sorte que personne n'est capturé ou tué pour rien"* ».

Il apparaît, comme le souligne Leistedt [2013], que les leaders observent dans les groupes ceux partageant leurs idées et leurs idéaux les plus à même de franchir les deux derniers paliers menant à l'action violente. Ces individus sont ensuite subdivisés en cellules réduites « *où ils pourront s'auto-alimenter de leur radicalisation* ». La recrue fait face à deux forces contraires : à

l'intérieur de la cellule où elle doit suivre des règles et conditionnements menant à la mort de civils, et souvent d'elle-même, et à l'extérieur de la cellule, notamment dans les pays du Maghreb ou du Moyen-Orient, où la moindre voix discordante est réprimée [Moghaddam, 2005]. Le recours aux concepts développés par Asch et Lewin, en psychologie sociale, sur la pensée de groupe, l'autocatégorisation et la polarisation dans les processus décisionnels pourrait éclairer ce qui se joue au sein de ces cellules, où chacun se perçoit comme part d'une entité qui le dépasse. Notons encore que, parmi les recruteurs, certaines femmes sont particulièrement actives sur Internet en véhiculant un discours radical. Elles cimentent encore les alliances entre différents groupes (Rabiyah Huntchinson, Emilie König...). Le recours aux sites de rencontres communautaires apparaît également comme une des cibles privilégiées des recruteurs.

## Prévention du risque violent

Les signes de basculement vers une radicalisation ont donné lieu à des campagnes de prévention de la part du ministère de l'Intérieur (<http://www.stopdjihadisme.fr>) avec la publication de différents marqueurs comportementaux (plaquette du ministère avec les idéogrammes). Toutefois, ces signes ne décrivent que le choix d'une idéologie radicale et non l'imminence d'un passage à l'acte. Cette décision est le plus souvent « compartimentée » dans l'esprit des fanatiques, qui ont appris à ne la dévoiler à personne à l'exception de ceux appartenant au « groupe des choisis ». Concernant les facteurs pouvant avoir une utilité pratique pour les enquêteurs de terrain, nous avons vu que les auteurs d'attentats terroristes n'ont pas un profil de personnalité unique. Parfois même,

comme dans une carrière criminelle, un individu peut traverser différentes typologies (Tableau 1) à mesure de son avancement idéologique, de son habitude et de ses capacités.

Malgré l'extrême difficulté à prévenir un acte terroriste perpétré par un acteur solitaire connu, nous pensons cependant que quelques indices doivent particulièrement alerter les autorités afin de les aider à cibler les individus à haut risque :

- toute modification récente de situation susceptible d'affecter l'individu et d'augmenter ses sentiments de frustration, de colère, de honte, d'hostilité contre les « autres » et la société : divorce des parents, changement de vie actuel, préjudice subi, conflits divers. Ces « stressés » sont souvent par ailleurs des signes annonciateurs de criminalité violente générale ;
- les antécédents de violence physique ;
- les antécédents criminels et les incarcérations ;
- les antécédents psychiatriques quels qu'ils soient (retard mental, troubles de l'enfance et de l'adolescence, usage de substances illicites, troubles de la personnalité, psychose, troubles de l'humeur...) ;
- la présence d'un partenaire ou d'un conjoint impliqué dans une organisation terroriste ;
- la fréquentation de membres de la criminalité organisée ou de personnes liées au fanatisme idéologique ;
- le retour de Syrie d'un « déserteur » radicalisé qui peut être un porteur missionné de projets terroristes.

Si possible, on pourra encore attacher de l'importance aux comportements

préparatoires et de prédispositions qui, pour le sujet, ont pour fonction d'acquiescer une technique opératoire et de s'habituer à l'idée du passage à l'acte par une mise en condition psychologique (baisse de la peur, abolition des freins moraux). Ces comportements se présentent sous diverses formes :

- par stimulation mentale (entraînement psychologique) : rêverie sur l'action, jeu de rôle personnel et vision de vidéos sur la violence, le scénario criminel, les techniques de combat, le contact avec les victimes, etc. ;
- par comportement préparatoire direct : acquisition de matériel paramilitaire, maniement des armes, évaluation des capacités personnelles, simulation et entraînement sur d'autres personnes, moyens de transport, location de véhicules, surveillance, repérage, modifications des habitudes, etc. ;
- par comportement préparatoire indirect : collecte de fonds par des moyens légaux ou illégaux, entraînement physique, conditions favorisées, expérimentation de la prise d'alcool et de drogue sur le comportement, promenade sur le futur lieu des attentats afin de se rendre le terrain familier, etc. [Vandevoorde, Estano, 2015].

## Audition des suspects

Lorsqu'ils sont appréhendés, les auteurs ou futurs auteurs possibles d'attentats utilisent diverses tactiques de « contre-interrogatoire » face au questionnement des enquêteurs. La 17<sup>e</sup> règle du manuel d'Al Qaïda est claire sur la conduite à tenir en cas d'arrestation : « *Les membres ne doivent pas révéler une quelconque information,*

*peu importe s'ils pensent qu'elle soit insignifiante, afin de ne pas ouvrir des portes qui ne pourront plus se refermer jusqu'à ce qu'ils se soient incriminés ou n'exposent l'organisation* » [Alison *et al.*, 2014].

Alison *et al.* [2014] identifient cinq catégories de tactiques dilatoires utilisées par les suspects : 1) Verbale : discuter de sujets sans rapport avec l'enquête, donner des informations déjà bien connues, fournir des réponses impromptues ; 2) Verbale-passive : fournir des réponses monosyllabiques, exprimer une perte de mémoire ; 3) Passive : refuser d'engager un contact oculaire, adopter un mutisme total (se distancier psychologiquement du contexte d'interrogatoire en n'interagissant ni physiquement ni verbalement) ; 4) « Pas de commentaires » : le suspect répond systématiquement « pas de commentaires », « je n'ai rien à dire » ; 5) Rétractation : le suspect se rétracte par rapport à des déclarations précédentes.

Toujours selon Alison *et al.*, c'est la méthode de rétractation qui paraît spécifique des terroristes internationaux, ce type de comportement n'étant guère utilisé par les terroristes d'extrême droite et ceux appartenant à des organisations paramilitaires. Chez les terroristes paramilitaires et internationaux, type Al Qaïda, on observe souvent l'adoption de tactiques passives en accord avec la règle écrite du manuel. Ils privilégient donc la méthode de « désengagement » verbal ou physique du cadre de l'audition [Alison *et al.*, 2014].

Dans la quatrième édition de son ouvrage, Turvey [2014] consacre le chapitre 23 à l'étude du terrorisme international et notamment des djihadistes opérant en Asie du Sud-Est (Jemaah Islamiyah Group). Il rappelle à son tour la variété des types de personnalité et l'absence de

troubles mentaux décompensés parmi les terroristes. Citant Gunaratna, il remarque qu'Al Qaïda recrute ses membres dans 74 pays parmi une quarantaine de nationalités, ce qui rend difficile l'identification par groupe ethnique ou national, mais qui n'empêche pas qu'un profil opérationnel ou organisationnel d'un terroriste soit réalisable. Le recrutement international et les observations des convertis en Occident (Emilie König, Maxime Dauchard...) montrent que c'est bien l'idéologie et la structure organisationnelle qui doivent être profilées et non pas le physique et l'ethnie des suspects [Turvey, 2014].

Au préalable à tout entretien avec un suspect, il convient de définir la nature et les origines de ses croyances idéologiques. Au cours de l'audition, l'interrogateur doit parvenir à comprendre les caractéristiques psychosociales et les besoins personnels de l'interrogé, par opposition à la logique collectiviste et la dynamique groupale utilisées dans le processus de radicalisation. Turvey insiste également sur la notion de respect vis-à-vis de l'interrogé et préconise d'éviter les attitudes suivantes : dénigrer, se montrer dominateur, humilier, crier, s'emporter, insulter, utiliser des arguments enflammés. Entrer dans une logique confrontationnelle n'est à moyen terme que contre-productif. Il est nécessaire de réagir le plus sereinement possible à la frustration que les auditions engendrent par moments et, si l'interrogateur ne peut contrôler ses émotions, il doit savoir se retirer de la procédure [Turvey, 2014]. En somme, en matière de terrorisme comme ailleurs, il faut appliquer les bonnes règles psychologiques et criminologiques de conduite d'un interrogatoire [Bénézech, St-Yves, 2011].

## Prise en charge

### Déradicalisation et désengagement

Certains auteurs, comme Horgan et Braddock [2010], font une distinction entre déradicalisation et désengagement. La déradicalisation ne peut en effet être considérée simplement comme l'inverse de la radicalisation, la distinction portant principalement sur les composantes cognitives et les composantes comportementales. Ces auteurs utilisent le terme « *désengagement comportemental* » pour désigner le fait de cesser ou réduire les implications physiques dans des activités violentes et/ou radicales, et le terme « *désengagement psychologique* » pour désigner un retournement attitudinal ou de croyances.

Quatre types de « désillusionnement » se retrouvent régulièrement dans les processus de déradicalisation : 1) Une dissonance entre les idéaux des volontaires et la réalité éprouvée au sein du groupe ou de l'État islamique (corruption, injustice). Ceci ressort des discours de 58 déserteurs revenant de Syrie, Daech combattant et tuant davantage de musulmans que de « croisés » [Neuman, 2015]. Des désaccords tactiques et stratégiques internes et des luttes intestines au sein de la mouvance islamique ; 2) Une forme d'épuisement type « burn-out » et un changement dans les priorités personnelles ; 3) La mauvaise qualité de la vie sur place [Barrelle, 2010 ; Horgan, Braddock, 2010].

### Quête d'importance et comportements pro-sociaux

Il s'agit de faire évoluer les néo-codes moraux adoptés par l'individu lors du processus de radicalisation,

l'amener à se confronter à la morale et à l'idéologie justifiant la violence auxquelles il a souscrit et pour lesquelles il s'est totalement effacé en tant que sujet individuel. L'aide de personnalités religieuses, qui ouvriront un dialogue avec les sujets à risque et les détenus pendant plusieurs mois, voire des années, est fondamentale et reposera sur les interdits quant aux violences commises sur des civils [Young, Rooze, Holsappel, 2015]. Lorsque la quête de signification existentielle est éveillée, des comportements pro-sociaux peuvent être activés selon l'idéologie [Kruglanski, Bélanger, Gelfand *et al.*, 2013].

### Renverser la quête pour l'importance existentielle

Parvenir à réinstaurer l'argument moral selon lequel la violence n'est pas acceptable du point de vue religieux peut délégitimer ce moyen criminel d'obtenir un niveau satisfaisant de signification existentielle, d'amour-propre. Il faut signaler cependant que si les suiveurs sont généralement plus facilement « retournables » que les leaders, leurs « conversions » peuvent être par opposition superficielles et moins durables, ce qui soulève la question de la récidive. Il se peut, à la faveur de contextes spécifiques, que la recherche d'une signification existentielle puissante pousse à nouveau les sujets provisoirement déradicalisés à adopter une idéologie extrémiste et il convient donc d'être attentif à leur suivi à long terme.

### La déradicalisation via un changement d'objectifs

Les préoccupations familiales peuvent se trouver au centre de la désistance observée par exemple chez certains terroristes de l'ETA ayant obtenu un statut autonome et atteint

*L'aide de personnalités religieuses, qui ouvriront un dialogue avec les sujets à risque et les détenus pendant plusieurs mois, voire des années, est fondamentale et reposera sur les interdits quant aux violences commises sur des civils.*

leur but. Les proches, le conjoint, les enfants, le sentiment d'avoir « fait sa part » comme révolutionnaire rendaient moins justifiable la question de la lutte armée. Meloy *et al.* [2014] décrivent la place essentielle que joue la famille dans le processus de déradicalisation [Meloy, Yakeley, 2014]. C'est donc en parvenant à restaurer des préoccupations individuelles et personnelles que le sujet pourrait commencer à critiquer une logique de groupe qui l'avait effacé subjectivement pour lui faire embrasser un but plus élevé que son existence antérieure.

### Modification du système de pensée paranoïaque

Nous avons déjà signalé que le mode de pensée du fanatique religieux ou politique avait de nombreux points communs avec celui du paranoïaque passionnel. Comme chez le paranoïaque, le système de pensée du « terroriste » se caractérise par la rigidité des schémas mentaux, les distorsions cognitives et les pensées automatiques. Les objectifs à long terme du traitement pour le sujet (thérapie psychodynamique, comportementale et cognitive) pourraient être de reconnaître et accepter ses sentiments de vulnérabilité, augmenter son sentiment de valeur personnelle, développer une vision plus positive d'autrui, accepter des points de vue alternatifs plutôt que de recourir à des stratégies contre-productives

comme l'isolement, le terrorisme et la guerre [Le Bihan, Brulin-Solignac, Bénézech, 2015]. La connaissance et la modification des structures cognitives des terroristes sont en effet nécessaires [Canter, Sarangi, Youngs, 2014].

## Conclusion

Nous avons tenté de définir très brièvement les bases psychodynamiques qui rendent un individu sensible au discours extrémiste, à une problématique fanatique, ainsi que les processus en œuvre dans le parcours individuel et collectif (groupe, foule) du futur terroriste. Nous pensons en

effet qu'une personne qui adopte une idéologie intégriste utilise un mécanisme psychologique de protection, de défense, de nature passionnelle et de mécanisme paranoïaque, pour trouver ou retrouver de l'amour-propre, surcompenser la faiblesse de son moi, se rassurer, se valoriser, se donner de l'importance, du pouvoir, du plaisir. La maladie mentale déclarée ne joue dans tout ceci qu'un rôle de second plan. Seule la population des auteurs solitaires présente une fréquence élevée (20 à 60 % ?) de troubles mentaux sévères (psychoses, troubles de l'humeur et de la personnalité...) alors que le reste de la population globale des terroristes ne se singularise pas dans ce domaine particulier.

Pour terminer, soulignons l'importance d'un projet social collectif impliquant de manière concertée et intégrée l'ensemble des acteurs de la communauté : familles, proches, enseignants, intervenants divers [Okomba-Debarice, 2015]. Parvenir à adresser une contre-rhétorique parlante, à se montrer le plus transparent possible pour lutter contre la théorie du complot et de l'oppression, terreau dans lequel l'idéologie extrémiste prend racine, pourrait permettre une avancée plus importante en sapant les bases d'une croyance répandue parmi un large panel d'individus qui remettent en cause le vivre ensemble [Demant, de Graaf, 2010] ■

## Bibliographie (...)

ADDAD (M.), BÉNÉZECH (M.), 1982, «New approach to the process of stigmatization in criminology: the preparatory ground», *International Criminal Police Review*, 37, 356, 66-72.

ADDAD (M.), BÉNÉZECH (M.), 1986, «Névrosisme, signification existentielle et auto-renforcement du moi. Enquête comparative entre délinquants et non-délinquants », *Annales Médico-Psychologiques*, 144, 8, 777-789.

ADDAD (M.), BÉNÉZECH (M.), 1987, «Jugement moral, extraversion, névrosisme et délinquance », *L'Évolution Psychiatrique*, 52, 3, 703-727.

ALISON (L.) *et al.*, 2014, «Whatever you say, say nothing: individual differences in counter interrogation tactics amongst a field of right wing, A.Q. inspired and paramilitary terrorists», *Personality and individual differences*, 68, 170-175.

ALONSO-FERNÁNDEZ (F.), 1997, « Aspects psycho-sociologiques et psychopathologiques du terrorisme », in Albernhe (T.) (ed), *Criminologie et psychiatrie*, Paris, Ellipses, p. 135-140.

BANDURA (A.), 1999, «Moral disengagement in the perpetration of inhumanities», *Personality and social psychology review*, Special Issue on Evil and Violence, 3, 193-209.

BAR-TAL (D.), 1990, «Causes and consequences of delegitimization: models of conflict and ethnocentrism», *Journal of Social Issues*, 46, 65-81. doi : 10.1111/j.1540-4560.1990.tb00272.x

BARRELLE (K.), 2010, «Disengagement from violent extremism», Conférence, Global terrorism centre and politics department, Monasch university.

BELL (S.), 2005, «The martyr's oath», *The apprenticeship of a homegrown terrorism*, Canada, John Wiley and Sons.

BÉNÉZECH (M.), ST-YVES (M.), 2011, « Méthode d'aide à l'audition d'un suspect : la MAAS-8M », *Revue internationale de criminologie et de police technique et scientifique*, 1, 63-82.

BÉNÉZECH (M.), TOUTIN (T.), 2015, « Radicalisation, terrorisme et psychiatrie », *Journal de Médecine Légale-Droit Médical-Victimologie-Dommage corporel*, série F, Médecine Légale du Vivant, 58, 4, 231-238.

BOUZAR (D.), 2014, *Désamorcer l'islam radical. Ces dérives sectaires qui défigurent l'islam*, Paris, L'Atelier.

BOUZAR (D.), CAUPENNE (C.), 2014, « Une nouvelle forme d'embrigadement des mineurs et des jeunes majeurs dans le terrorisme », Rapport du CPDSI Recherche

- action « Indicateurs de prévention », première étape.
- CANTER (D.), SARANGI (S.), YOUNGS (D.), 2014, « Terrorists' personal constructs and their roles: a comparison of three Islamic terrorists », *Legal and Criminological Psychology*, 19, 160-178.
- CORNER (E.), GILL (P.), 2015, « A false dichotomy? Mental illness and lone actor terrorism », *Law and Human Behavior*, 39, 1, 23-34.
- CRENSHAW (M.), 1988, « The subjective reality of the terrorist: ideological and psychological factors in terrorism », in SLATER (R.O.), STOHL (M.) (eds), *Current perspectives on international terrorism*, London, Macmillan Press, p. 12-46.
- CRENSHAW (M.), 2006, « Have motivations for terrorism changed? », in VICTOROFF (J.) (ed), *Tangled roots: social and psychological factors in the genesis of terrorism*, Oxford, ISO Press, p. 51-61.
- DEMANT (F.), GRAAF (B. DE), 2010, « How to counter radical narratives: Dutch deradicalization policy in the case of Moluccan and Islamic radicals », *Studies in Conflict and Terrorism*, 33, 408-428.
- DIDEROT (D.), ALEMBERT (J. D.), 1751, *Encyclopédie ou dictionnaire raisonné des sciences, des arts et des métiers*, Paris, Briasson/David/Le Breton/Durand, Article : « Fanatisme », volume 1, tome 6, p. 393-401.
- FISCHER (P.), AI (A.L.), 2008, « International terrorism and mental health, Recent research and future directions », *Journal of Interpersonal Violence*, 23, 3, 339-361.
- FREUD (S.), 2012, *Psychologie des foules et analyse du moi*, Paris, Petite Bibliothèque Payot.
- GÉRÉ (F.), 2003, *Les volontaires de la mort. L'arme du suicide*. Paris, Bayard.
- HACKER (F.), 1976, *Crazies, criminals and crusaders*, New York, Norton.
- HOFFMAN (B.), 2006, *Inside Terrorism*, New York, Columbia University Press.
- HORGAN (J.), BRADDOCK (K.), 2010, « Rehabilitating the terrorists? Challenges in assessing the effectiveness of de-radicalization programs », *Terrorism and Political Violence*, 22, 24.
- KHOSROKHAVAR (F.), 2014, *Radicalisation*, Paris, Éditions de la maison des sciences de l'homme.
- KRUGLANSKI (A.W.), BÉLANGER (J.J.), GELFAND (M.) et al, 2013, « Terrorism, A (self) love story. Redirecting the significance quest can end violence », *American Psychologist*, 68, 7, 559-575.
- LE BIHAN (P.), BRULIN-SOLIGNAC (A.), BÉNÉZECH (M.), 2015, « Personnalité paranoïaque et changement », in Coutanceau (R.), Smith (J.) (eds), *Psychothérapie et éducation. La question du changement*, Paris, Dunod, p. 117-128.
- LEISTEDT (S.J.), 2013, *Behavioural aspects of terrorism*, Forensic Science International, 228, 21-27.
- LITINETSKAIA (M.), GUELFY (J.D.), 2015, « Fanatisme et délire : les frontières psychiques », *Annales Médico-Psychologiques*, 173, 7, 618-622.
- LOZA (W.), 2007, « The psychology of extremism and terrorism: a middle eastern perspective », *Aggression and Violent Behavior*, 12, 141-155.
- MAGOURIK (J.), SAGEMAN (M.), ATRAN (S.), 2008, « Connecting terrorist networks », *Studies in Conflict and Terrorism*, 31, 1-16.
- MARCHAND (P.), 2014, « Analyse avec Iramuteq de dialogues en négociations de crise : le cas Mohamed Merah », 12<sup>e</sup> Journées internationales d'analyse des données textuelles.
- MELOY (J.R.), YAKELEY (J.), 2014, « The violent true believer as a "lone wolf": psychoanalytic perspectives on terrorism », *Behav Sci Law*, 32, 347-365.
- MOGHADDAM (F.M.), 2005, « The staircase to terrorism. A psychological exploration », *American Psychologist*, 60, 2, 161-169.
- MOSCOVICI (S.), 1991, *L'âge des foules. Un traité historique de psychologie des masses*, Bruxelles, Complexe.
- NEUMAN (P.), 2015, International Centre for the Study of Radicalization and Political Violence (ICSR), *Victims, perpetrators, assets : the narratives of Islamic state defectors*.
- OKOMBA-DEPARICE (H.), 2015, *Prévenir de la radicalisation menant à la violence. Les contours d'une « approche québécoise »*, Centre de prévention de la radicalisation menant à la violence (CPRMV), Paris, 21 octobre.
- SAGEMAN (M.), 2004, *Understanding terror networks*, Philadelphia, University of Pennsylvania press.
- SAGEMAN (M.), 2008, *Leaderless Jihad*, Philadelphia, University of Pennsylvania Press.
- SILKE (A.), 1998, « Cheshire-cat logic. The recurring theme of terrorist abnormality in psychological research », *Psychology, Crime and Law*, 4, 51-69.
- SQUVERER (A.), 2007, « Figure clinique du fanatisme », *Synapse*, 230, 20-26.

- STANKOV (L.), SAUCIER (G.), KNEŽEVIĆ (G.), 2010, «Militant extremist mind-set: proviolence, vile world, and divine power», *Psychological Assessment*, 22, 1, 70-86.
- TRÉVIDIC (M.), 2013, *Terroristes. Les 7 piliers de la déraison*, Paris, JC Lattès.
- TURVEY (B.E.), 2014, *Criminal profiling. An introduction to behavioral evidence analysis* (4<sup>th</sup> ed), London, Academic Press, p.570-581.
- VANDEVOORDE (J.), ESTANO (N.), 2015, « Contexte préparatoire et comportement de prédisposition dans les gestes violents d'apparence impulsive: évaluation des éléments de planification et de préméditation », *La revue de médecine légale*, 6, 1, 11-19.
- VICTOROFF (J.), 2005, «The mind of terrorist, a review and critique of psychological approaches», *Journal of Conflict Resolution*, 49(1), 3-42.
- YOUNG (H.), ROOZE (M.), HOLSAPPEL (J.), 2015, «Translating conceptualizations into practical suggestions. What the literature on radicalizations can offer to practioners», *Peace and Conflict: Journal of Peace Psychology*, 21(2), 212-225.