Actes du colloque du CDSE à l'OCDE

Mondialisation, virtualisation, externalisation : l'entreprise peut-elle encore avoir la maîtrise de sa sécurité ?

Jeudi 25 novembre 2010

L'entreprise a-t-elle encore les moyens de sa sûreté dans un contexte où se multiplient prises d'otages et assassinats d'expatriés, conflits sociaux ou encore catastrophes naturelles non prévisibles ? C'est en ces termes que **François Roussely**, Président du CDSE (Club des Directeurs de Sécurité des Entreprises), a introduit le quatrième colloque du CDSE qui se tenait le jeudi 25 novembre à l'OCDE et qui a réuni près de 450 participants (Directeurs de sécurité d'entreprises, hauts fonctionnaires, cabinets de sécurité…).
Le Président a rappelé nombre d'évènements qui ont tristement marqué l'année 2010 : les enlèvements au Niger, le meurtre d'un salarié de Spie au Yémen, la séquestration de patrons ou la prise en otages des actifs d'une société. Dans le domaine financier, la chute de 9 % du Dow Jones le 6 mai 2010, sans savoir si ce trou d'air résulte d'un acte de malveillance, d'une fausse manœuvre informatique ou de la volatilité normale des cours de Bourse a rappelé que notre univers est marqué par les évènements imprévisibles : éruption volcanique en Islande à la suite de laquelle personne ne pouvait envisager la fermeture de 25 aéroports, explosion d'une plate forme pétrolière de BP dans le Golfe du Mexique où la technique comme le management de l'entreprise ont été défaillants.
Pour faire face à ces évènements, il faut commencer par considérer que des évènements réputés imprévisibles peuvent pourtant être anticipés rappelle **François Roussely,** qu'il s'agisse de la structure de financement des *subprimes* ou bien du cyclone Katrina. Le recours aux *scenarii* catastrophes permet notamment de prévoir et de se préparer. Il en est ainsi de la SNCF ou d'EDF qui se préparent, via des installations et des séances de formation pour leurs salariés et leurs cadres, à des situations de crise censées ne jamais survenir. A l'instar des hommes politiques, les managers privés sont jugés sur ce qui est prévisible et courant, mais également sur ce qui est inattendu.

Ce devoir d'anticipation et de préparation à l'inconcevable est rendu plus complexe par les effets simultanés de la mondialisation (implantation dans des pays instables), de l'externalisation (sociétés de sécurité privée, *cloud computing*) et de la virtualisation (cybercriminalité, atteinte à la réputation). Autant de phénomènes qui complexifient l'univers dans lequel opère l'entreprise mais avec lesquels elle n'a d'autre choix que de composer aux yeux d'**Alain Bauer**, Président du CSFRS. Dans ce cadre mondialisé et changeant, il rappelle le rôle primordial du partage du savoir entre experts et ceux qui sont au cœur des opérations dans les secteurs public et prive pour remédier à la crise de la pensée stratégique en France comme dans le reste de l'Occident. **Alain Bauer** pointe alors du doigt les think tanks A l'anglo saxonne qui ne chercheraient pas à donner de la pensée pour permettre aux gouvernements de choisir, mais *« qui agissent simplement en tanks, en justifiant la position du gouvernement en gardant à l'esprit le renouvellement de leurs subventions »*. D'où l'intérêt, selon lui, d'organismes comme le CDSE ou le CSFRS, organe mixte dont le rôle est de mutualiser les savoirs et les financements de la recherche atypique.
Rejoignant les propos de **François Roussely**, il affirme que la surprise stratégique n'existe pas. *« 99 % des désastres militaires du passé ne sont que des effets de notre aveuglement stratégique, par trop de travail, trop de quotidien, de pression, parfois aussi par la réduction absurde des budgets… »*. La surprise est exceptionnelle. En matière policière et militaire, la France possède parmi les meilleurs tacticiens au monde, sans doute les plus compétents en

matière de gestion de crise. Mais en matière de conceptualisation, il qualifie les analyses de « désastreuses » alors que la prévision a le plus souvent été négligée. En la matière, il paraît indispensable de dépasser la production strictement académique pour produire des outils véritablement utiles liés à l'expérience des entreprises afin de répondre au mieux à leurs besoins opérationnels qui sont aussi les intérêts de la Nation.
Il rend hommage au courage et au dynamisme d'une nouvelle dimension des ambassadeurs de France, comme Boris Boillon.

Un avis toutefois nuancé par **Christian Lechervy** *« les prospectivistes sont des gens dangereux car leur statut et leur influence dépendent de leur capacité à dramatiser une situation »*. Si **Jean-Louis Bruguière** s'accorde sur cela, il estime que la sous-évaluation des risques et des signes de basse intensité est tout aussi dangereuse, comme l'absence d'anticipation du 11 septembre l'a révélée. D'où la nécessité d'avoir une stratégie proactive. Selon lui, si la France n'a pas été frappé depuis 1996, ce n'est, selon lui, sans doute pas un hasard. Mais la menace terroriste est encore plus difficile à appréhender : Al Qaïda est de moins en moins centralisée, mais elle conserve une capacité de mobilisation et de recrutement considérable. Internet devient un outil fondamental à ces fins. De surcroît, ces structures sont de plus en plus liées à la criminalité courante, avec des intérêts objectifs à cela : entre le narcotrafic d'Amérique latine et AQMI, le contrôle par AQMI le trafic d'êtres humains et de migrants, ou en Asie du sud-est par une récupération de la contrefaçon médicale dans le registre terroriste. Aujourd'hui on ne peut plus isoler les facteurs.

1. Les effets de la mondialisation sur la sécurité des entreprises

Selon **Alain Bauer** *« nous sommes sortis de l'ordre pour rentrer dans un chaos permanent. Or, nous aimerions que le monde soit tel que nous le voulons et non comme il est. Cette recherche absolue d'un équilibre sans tenir compte de la réalité qui nous entoure est notre drame ».* Nous serions passés d'un monde multiétatique à un monde où les entreprises sont un acteur majeur, et souvent des victimes de premier plan, dès lors qu'elles défendent un brevet, une idée, une invention. Elles deviennent alors un élément majeur de l'activité d'intelligence économique auquel nous sommes peu attentifs, bien que l'arrivée d'**Olivier Buquen** ait quelque peu changé la donne. Ce manque d'attention proviendrait d'une réticence de l'Etat à élargir son monopole naturel (hydrocarbures et télécommunications) pour se soucier de l'économie. Si l'Etat y consent aujourd'hui, ce serait parce que, selon **Alain Bauer**, désormais *« tout est devenu stratégique : finance, emploi, risque, perte, danger, menace… ».*

Dans une optique d'intelligence économique, **Alain Bauer** appelle à dépasser certaines illusions communément entretenues, à l'instar des BRIC : le Brésil, immense Etat économiquement, est l'Etat le plus gangrené par la criminalité, l'Inde est un Etat formidable mais qui n'existe pas encore fédéralement, la Chine a inventé le communisme de marché, mais inquiète par le contrôle de certaines terres rares ou par l'élimination de la concurrence via une baisse des prix comme outil de puissance pour éliminer la concurrence. **Alain Bauer** plaide pour que cette illusion laisse place à la prudence lorsque l'on traite avec ces partenaires, avec lesquels **Alexandra Trzeciak-Duval** chef de la Division de la coordination des politiques à l'OCDE, estime malgré tout important d'envisager des activités économiques triangulaires et des échanges d'expériences.
Alain Bauer poursuit en rappelant que certains de nos partenaires industriels cherchent davantage à piller et restructurer leur industrie éteinte qu'à aider au développement de la nôtre, même au niveau européen. *« Nous faisons semblant de croire que la Grande-Bretagne dispose d'un arsenal nucléaire alors que celui-ci est sous contrôle US depuis les accords Mac Millan. La France reste le seul Etat d'Europe à disposer d'une souveraineté nucléaire ».* Jusqu'à il y a encore deux ans, la France était un des leaders mondiaux de la maîtrise du contrôle et de l'exportation du nucléaire civil, pour devenir aujourd'hui un acteur de seconde zone par la simple indifférence à l'égard des attentes du client. Le rapport Roussely donne un choix entre la disparition d'une industrie majeure, élément de notre indépendance stratégique et de celle de l'Europe, et sa résurrection. Ce choix binaire est à l'image de tous nos secteurs industriels : notre capacité à produire, dans des domaines aussi essentiels que l'aéronautique, l'‘espace, le nucléaire le transport…

A l'‘instar d'**Alain Bauer, Christian Lechervy** juge que la mondialisation engendre de profondes évolutions qu'il faut prendre en considération :

- *« Evolution sur l'identité nationale des entreprises »* : la perception ou l'affichage de leur identité nationale est en bouleversement, ce qui est à la fois une préoccupation des Etats et un facteur de protection pour les entreprises. En effet, celles-ci tendent à être moins liées au territoire, et se soucient de ne pas adosser leur image aux soubresauts des relations bilatérales de leur pays d'origine. Par conséquent, les personnels expatriés sont de plus en plus diversifiés et on est dans une situation où cette dénationalisation est avant tout un avantage en termes de sécurité. Mais l'inconvénient est que les entreprises sont davantage prises pour cible, non en raison leur nationalité mais pour leur symbole occidental. Cette assimilation est croissante.
- *« Changement de la nature des conflits auxquels nous sommes confrontés : de moins en moins politiques et de plus en plus sociaux ».* La lecture des conflits doit se faire, non plus

seulement à travers le prisme de la conquête du pouvoir, mais en termes de distanciation sociale. Le mode de gestion des Etats recourt de plus en plus à la sociologie et à l'anthropologie. Dès lors, selon **Christian Lechervy**, il convient de s'intéresser aux processus d'humiliation périphérique de leurs interlocuteurs politiques.

- *« Désengagement des Etats occidentaux des coopérations de défense et de sécurité »*. Le concours qu'ils pouvaient apporter il y a quelques années fut amoindri par la contrainte budgétaire, la contrainte des opinions (la coopération est faite par des acteurs dont l'image est dégradée) et par un recentrage des priorités vers les puissances émergentes au détriment des autres. La conséquence est une baisse de l'intimité entre leaders, une méconnaissance des chaines hiérarchiques et une méconnaissance des appareils de sécurité des Etats.

- *« L'exigence de sécurité des personnels est croissante et cette contrainte est mal maitrisée parce que l'on sous-estime les contraintes psychologiques individuelles, les risques de judiciarisation »*. Pour se faire, les entreprises et l'Etat sont rentrés en concurrence en cherchant chacun la protection à apporter, leurs approches devenant toujours plus divergentes. **Christian Lechervy** constate par exemple que dans le cas d'évacuation d'urgence, l'Etat a tendance à donner des signaux d'alerte tardifs pour retarder les évacuations, tandis que les entreprises ont plutôt tendance à les accélérer.

2 - Pourquoi et comment investir en zone instable ?

- L'instabilité de certaines zones empêche-t-elle les entreprises d'opérer ?

A cette question particulièrement d'actualité, l'Ambassadeur de France en Irak, **Boris Boillon**, répond sans hésitation « Non ». A condition toutefois que la sécurité soit possible et que le coût de la sécurité soit inférieur aux marges de bénéfice réalisées. L'Ambassadeur ne nie pas l'insécurité irakienne mais entend rappeler certaines réalités *« Al Qaïda est une organisation habile qui parvient toutes les six semaines à donner l'impression au monde entier que l'Irak est une poudrière ».*
Boris Boillon évoque deux principaux risques en Irak. Le risque d'enlèvement est très élevé dans certains quartiers, et notamment à Saadr City où des enfants sont enlevés quotidiennement de manière extrêmement brutale par d'anciens gangs terroristes reconvertis dans la criminalité, qui donnent deux jours aux parents pour payer la rançon. Pour lutter contre ce risque, l'escorte par des hommes armés en voiture est le plus efficace. L'Ambassadeur rappelle le cas d'un journaliste sur le point d'être enlevé à un feu rouge, avant que la simple présence d'hommes armés derrière lui suffise à dissuader les preneurs d'otage.
Le second risque est celui de se trouver à proximité d'une explosion. L'Ambassadeur recense dix évènements à caractère terroriste chaque jour et observe une recrudescence d'IED (bombes artisanales) posées sous les véhicules ou sur des vélos. Pour se prémunir contre ce risque ou limiter les effets de projection, il est préférable de circuler en voiture blindée.

La France demeure *« une marque de qualité en Irak »* et l'expertise des entreprises françaises est très demandée selon **Boris Boillon**. Il reste par exemple des quartiers et un aéroport construits par les français. Evoquant les récents marchés obtenus par Alstom (20 millions d'€ pour rénover une station électrique), Saint-Gobain (marché de canalisation de 60 millions d'€ à Bagdad) et Suez-Degrémont (station de potabilisation pour 200 millions d'€), il estime que l'Irak est une terre d'opportunités pour nombres d'entreprises françaises en dépit des conditions sécuritaires fragiles. Une conviction partagée par **Christian Valéry** (Bureau des Opérations Internationales) qui relate l'organisation d'une délégation de cinquante entreprises françaises à la Foire de Bagdad, qui ont pour une grande partie d'entre eux signé des contrats. Cela n'aurait pas été rendu possible pour des raisons de coût sans l'appui de l'Ambassade et du Service Economique.
Les autres intervenants dressent un constat similaire. Dans certains secteurs, à l'instar du pétrole, les entreprises n'ont pas d'autre choix que d'aller dans les pays où se trouvent les réserves selon **Jérôme Ferrier**, Directeur de la Sécurité Générale de Total. Celui-ci rappelle que plus de la moitié des réserves pétrolières et gazières se trouvent en Irak, en Arabie Saoudite ou encore au Yémen, pays à hauts risques. De surcroît, l'implantation dans ces pays doit se faire dans des conditions de concurrence qui ont sensiblement évolué, puisque les compagnies pétrolières internationales sont concurrencées par les compagnies nationales, notamment chinoises mais également brésilienne (Petrobras), ou malaisienne (Petronas). Ces compagnies ont l'ambition de se développer sur les mêmes terrains que les compagnies internationales, mais sans avoir dans le même temps les mêmes critères en termes de sécurité et de sûreté. Concernant l'Irak, **Jérôme Ferrier** explique que Total dispose d'une précieuse expérience de plus de cinquante ans dans le pays, héritée d'Elf Aquitaine et de la Compagnie Française du Pétrole.

Pascal Junghans, médiateur de cette première table-ronde, introduit ensuite la question de la méthodologie déployée par les entreprises pour choisir ou non d'opérer dans les pays instables. Un souci permanent pour Total qui opère dans plus de 130 pays, parmi lesquels une quarantaine présente des risques plus ou moins importants. L'approche de Total, présentée par

Jérôme Ferrier, est fondée sur trois critères : la criminalité (criminalité courante, enlèvements, piraterie maritime, cybercriminalité), le risque politique (risque politico-social, risques liés aux élections, soulèvements populaires) et le risque terroriste. Pour chacun de ces critères, une cellule d'analyse et de veille a pour mission d'anticiper les risques et se nourrit d'informations fournies par les services de la République, les Ambassades et des consultants. In fine, ces critères sont pondérés et donnent un coefficient représentatif du niveau d'insécurité du pays dans lequel l'entreprise est appelée à travailler. Ce coefficient sera associé à un certain nombre de conditions et de mesures à mettre en place. A titre d'exemple, le Nigeria est un pays-clé parce qu'il compte pour 12 % de la production de Total et la compagnie compte 550 expatriés sur place. Cela nécessite donc pour le groupe pétrolier de développer un tissu de mesures de protection pour faire face à la criminalité, aux enlèvements, à la piraterie maritime. Si le Nigeria a pour l'instant été épargné par la menace terroriste, les récents attentats d'Abuja alertent sur le fait que la menace peut venir aussi du Sahel et descendre vers le Nigeria. Ce tissu sécuritaire est composé de personnels statutaires, à savoir des officiers et des managers de sécurité (salariés du Groupe ou contractés), qui s'appuient sur les forces armées locales (militaires, marins, policiers).

- Comment se protéger ?

L'appréhension des risques tient en permanence compte des obligations opérationnelles du Groupe et est indissociable du business. *« Il faut être moins exposé que les autres, mais il y a un moment où on va aller tellement loin dans la protection qu'on ne pourra plus travailler, au point de pénaliser l'activité de l'entreprise »*. C'est d'abord le business qui décide et la sécurité générale, sans formuler d'interdiction, va ensuite recommander si oui ou non il est possible de travailler et dans quelles conditions. *« La rentabilité du business doit être à la hauteur des risques que l'entreprise encourt »*. Par conséquent, précise-t-il, *« toute décision [quant aux moyens et au coût de la protection] doit s'appuyer sur l'évaluation des risques »*, laquelle doit être la plus fiable possible. Le Directeur met toutefois en garde : « *il y a certaines circonstances ou situations particulières qui peuvent nous amener à déconseiller de développer une activité dans des régions où la gestion des risques devient trop compliquée »*.
Les évaluations de risques ne pèsent pas la même chose selon l'intérêt stratégique des pays visés. Dans le cas de Total, les risques évalués au Pakistan où l'entreprise est présente dans une activité de marketing, et au Yémen, où elle opère dans l'E&P, diffèrent sensiblement. *« Si nous avions une explosion sur une station service par exemple au Pakistan et sous réserve qu'il n'y ait pas de victime, cela ne fera une minute au 20H. Mais en revanche, si nous sommes victimes d'un attentat sur une usine de raffinage ou de liquéfaction de gaz naturel représentant un investissement significatif pour le Groupe, il est certain que cela aura un impact majeur »*.

Selon **Bernard Frahi,** l'obligation de résultat en matière de sûreté contraint à l'adoption de mesures préventives sous peine de mise en cause civile et pénale. Mais le coût de cette protection doit être en adéquation avec la richesse de l'entreprise, à savoir les ressources humaines. A l'instar de l'Ambassadeur, **Bernard Frahi** défend l'idée que les entreprises doivent intégrer les coûts de sécurité dans les projets. Une escorte de 1000 € depuis l'aéroport jusqu'au Centre des Affaires à Bagdad est un coût, mais il est justifié au regard des besoins imposés par la réalité sécuritaire du pays. Sanofi Aventis compte plus de 100 000 employés répartis dans plus de 60 pays et un dispositif destiné à la protection des collaborateurs et expatriés a été évalué à 500 000 € répartis sur la sûreté des voyageurs d'affaires, sur la formation et la sensibilisation des expatriés, et sur la mise en place d'une cellule de gestion de risques et de crise, largement imposés par la jurisprudence Karachi.

Selon **Bernard Frahi,** l'obligation de résultat en matière de sûreté contraint à l'adoption de

mesures préventives sous peine de mise en cause civile et pénale. Mais le coût de cette protection doit être en adéquation avec la richesse de l'entreprise, à savoir les ressources humaines. A l'instar de l'Ambassadeur, **Bernard Frahi** défend l'idée que les entreprises doivent intégrer les coûts de sécurité dans les projets. Une escorte de 1000 € depuis l'aéroport jusqu'au Centre des Affaires à Bagdad est un coût, mais il est justifié au regard des besoins imposés par la réalité sécuritaire du pays. Sanofi Aventis compte plus de 100 000 employés répartis dans plus de 60 pays et a alloué un montant substantiel de ressources distribué sur la sûreté des voyageurs d'affaires, sur la formation et la sensibilisation des expatriés, et sur la mise en place d'une cellule de gestion de risques et de crise, largement imposés par la jurisprudence Karachi

Bernard Frahi défend l'idée de « sécurité compétitive ». La sécurité accompagne l'entreprise dans son développement dans des pays instables où l'évaluation des risques est fondamentale. Mais encore faut-il s'entendre sur cette évaluation qui doit être pour lui le produit des « menaces et des vulnérabilités ». Dans l'appréciation des différentes menaces, **Bernard Frahi** rappelle qu'il faut prendre en compte la gravité et la fréquence de celles-ci. Quant à l'évaluation des vulnérabilités, il distingue cinq éléments :

- *« Vulnérabilité de la filiale par rapport à sa localisation »* : la situation dans certains endroits est évolutive. Ainsi, une filiale implantée à Port-Harcourt dans le Delta du Niger sera bien plus exposée aux dangers (enlèvements) qu'à Lagos ou Abuja. Des critères et des signaux d'alerte sont mis en place pour apprécier cette vulnérabilité.
- *« Vulnérabilité du personnel »,* qui s'apprécie à travers le nombre et la qualité des collaborateurs, qui ont tous la même valeur qu'ils soient locaux ou expatriés, ainsi que l'exprime également **Jérôme Ferrier.** Toutefois, ce denier précise que les conditions de protection peuvent varier entre des expatriés que l'entreprise oblige à résider dans des camps protégés, comme par exemple à Port Harcourt, et des salariés nigérians qui n'accepteraient pas de vivre dans ces camps et qui résident bien souvent dans la ville. Leur plus grande exposition aux dangers oblige l'entreprise à étendre le périmètre de sécurité.
- *« Vulnérabilité du patrimoine »,* a fortiori dans l'industrie pharmaceutique où les produits sont au cœur de la richesse du groupe.
- *« La filiale a-t-elle les moyens internes de sa protection ? »* Il faut déployer une cellule de gestion de risques, de gestion de crise, afin de faire face aux situations de crise de manière coordonnée et structurée.
- *« La filiale dispose-t-elle des moyens de protection externes suffisants ? »* Dispose-t-elle de l'appui diplomatique ? **Bernard Frahi** précise que l'entreprise se doit de travailler *« avec les services de renseignements officiels et non en parallèle de ceux-là ».* Témoignant de sa propre expérience passée, il explique que les relations tissées avec les services de renseignement pakistanais (ISI) ont été des plus efficaces afin d'anticiper ou de régler certains problèmes.

Concernant ce dernier point, **Boris Boillon** a tenu a rappelé que l'Etat et les Ambassades ont une mission générale de renforcement des relations de confiance avec les autorités locales et les forces de sécurité locales. *« Sans ce cadre général essentiel, on ne peut pas parler de sécurité »* affirme-t-il. Cela passe par le dialogue politique au niveau intermédiaire comme au plus haut niveau (visites de ministres…), par l'identification des véritables circuits d'influence (identifier qui compte et qui a les moyens de passer à l'acte), et par un réengagement sur le terrain pour mieux connaître et appréhender le pays (en Irak, inauguration d'un Consulat honoraire dans le sud, construction de deux écoles françaises au nord).

Parallèlement à cette mission de protection générale, toute Ambassade doit aider les entreprises à renforcer leur sécurité commerciale et juridique. La France a ainsi été le premier pays à signer un accord de protection des investissements avec l'Irak. De nombreux outils

généraux existent permettant aux entreprises d'investir en confiance, à l'instar du retour de la Coface, du lancement d'un Fonds d'amorçage de dix millions € pour financer des opérations de formation, et la création d'outils innovants. En la présence de son Directeur **Jean-Pierre Vuillerme**, **Boris Boillon** évoque la création du CFA en Irak (Centre Français des Affaires). Ce centre est le fruit d'un partenariat public-privé financé ex nihilo par l'ADIT sans que cela ne coûte d'argent au contribuable. Situé dans le périmètre de sécurité de l'Ambassade, il est composé de deux bâtiments : un bâtiment hôtelier d'une dizaine de chambres et une vingtaine de bureaux pour accueillir ou domicilier les entreprises ponctuellement ou à l'année. Ce centre a désormais un bras armé à l'issue d'un appel d'offre lancé par l'ADIT et remporté par une société française de sécurité. Elle permettra au centre d'offrir la panoplie complète que peut attendre une entreprise lorsqu'elle arrive en Irak : une veille stratégique pour 2000 €/ an avec un domicile (le CFA) et des informations régulières selon le champ de compétences de l'entreprise. Par le biais de ce CFA, les différentes entreprises françaises de sécurité peuvent répondre à une variété de solutions de sécurité selon les besoins des entreprises. A ce titre, **Boris Boillon** distingue schématiquement deux visions de la sécurité : une sécurité visible et une sécurité furtive. La première, davantage anglo-saxonne, est faite d'imposants 4X4 avec des hommes armés et visibles, qui s'avère être assez coûteuse (6000 $ par jour) tandis que la seconde, davantage « low profile » pour un niveau de sécurité très élevé, peut descendre aux alentours de 1000 $ par jour. Le CFA offre ce panel de solutions. Il semble malheureusement que cette initiative demeure isolée à ce jour et sa réalisation est en grande partie due à l'engagement de l'Ambassadeur précise **Jean-Pierre Vuillerme.**

Reste enfin, le partage d'expériences entre entreprises. Mais la coopération dans le domaine de la sécurité entre entreprises travaillant dans les mêmes zones d'opération trouve ses limites, notamment avec les entreprises internationales. Ainsi, dans le domaine pétrolier, **Jérôme Ferrier** explique que si les échanges d'expérience existent, une certaine réserve s'impose également avec certaines compagnies dont les liens avec leurs services de renseignement d'origine restent très forts. Quant au domaine des systèmes d'information, il y a des *« zones sensibles »* avec lesquelles les coopérations sont minimes : l'Asie et surtout la Chine, ou la Russie, qui recèlent des risques. Le partage se fait davantage en sous-groupes, comme ce qui se fait avec l'ANSSI ou au sein du CDSE. Le partenariat demeure toutefois une obligation pour **Bernard Frahi**, notamment dans la contrefaçon des médicaments puisque les autres entreprises du secteur sont confrontées aux mêmes problématiques que Sanofi-Aventis. La mutualisation des moyens et la collecte d'informations sont indispensables à l'endiguement des trafics.

- Les Sociétés Militaire Privées (SMP) sont-elles une solution ?

Ce délicat équilibre entre nécessité d'opérer et besoin de se protéger ouvre-t-il la voix à l'externalisation de la sécurité aux fameuses SMP (Sociétés Militaires Privées) ? *« Débat qui peut vite déraper »* confie en coulisse un participant. **Jérôme Ferrier** rappelle qu'il peut arriver, dans certains pays comme l'Irak, où l'entreprise ne peut pas être correctement protégée sans soutien de forces internationales, c'est-à-dire qui ne soit pas exclusivement irakiennes. Toutefois, l'entreprise tend à privilégier la protection par les forces armées nationales du pays d'implantation mais *« par le biais d'accords (Memorandum Of Understanding) permettant à Total de poser des conditions relatives au respect des droits de l'homme par les forces armées »*. Le Directeur explique que ces forces armées sont rémunérées par la compagnie puisqu'elles sont dédiées à sa protection et à aucune autre mission, mais cette rémunération s'inscrit dans le cadre d'un accord permettant à l'entreprise de fixer ses exigences (notamment en matière humanitaire). Pour s'assurer du respect de ces règles par l'armée, Total a recours à du personnel contractant spécifiquement dédié à cette tache. Cette solution permet de ne pas faire appel aux Sociétés Militaires Privées (SMP), ou

selon **Jérôme Ferrier,** ce que l'on pourrait appeler « *entreprises militaires de défense et de sécurité* » afin de se démarquer du concept très connoté de SMP.

Jean-Louis Bruguière, ancien juge antiterroriste, et **Christian Lechervy**, Directeur adjoint de la Direction Prospective au ministère des Affaires Etrangères y sont résolument opposés. Ce que les entreprises gagneraient en sécurité, elles le perdraient en image, résume en substance **Christian Lechervy**, pour qui ces SMP sont difficilement contrôlables. Tout dépend de la fragilité dans laquelle se trouve le groupe. Tout d'abord, l'image de la société et de ses personnels : il faut faire un travail de compréhension de l'insertion de l'entreprise dans son milieu. Quelles sont les perturbations qu'elle crée dans le champ politique et les fragilités que suscitent les employés ? Dans certains pays, le risque est proportionnel au comportement des employés, a fortiori sur des théâtres instables où l'entreprise est quasiment seule. Dans ce contexte, poursuit **Christian Lechervy,** l'exemplarité des comportements des employés doit davantage retenir notre attention. Avant de s'interroger sur l'opportunité de recourir un SMP, il faut avant tout un bon DRH, qui connaisse intimement ses personnels, leurs modes d'insertion dans l'espace, ce qui suppose une présence physique et du temps. Il faut avant tout connaître le caractère perturbateur de ces SMP, et notamment le profil tribal ou clanique des hommes qui les composent par rapport à l'ordonnancement général de la zone ou de l'Etat central. A partir de ce constat, **Christian Lechervy** estime *« qu'à cette heure, les SMP ne servent pas à grand chose et s'avèrent finalement être davantage un problème pour les Etats que pour les entreprises »*. L'entreprise, qui est également un acteur politique, a davantage intérêt à recourir à l'Etat local, en l'aidant à sortir de ses fragilités, que de se substituer à celui-ci via les SMP, à l'instar de ce que **Jérôme Ferrier** laissait entendre. Dans un certain nombre de cas, les entreprises n'ont pas le choix et sont contraintes de contracter avec l'Etat ou des épigones privatisées de l'Etat, mais les SMP s'apparentent surtout aujourd'hui à des sociétés de sécurité et de gardiennage pour réaliser des activités de convoyage ou protéger des installations. Selon lui, *« même si l'Etat a la volonté de construire ces sociétés nationales en matière militaire privée, je pense qu'elles ne naitront pas du jour au lendemain »*. En d'autres termes, selon **Christian Lechervy,** si certaines entreprises seront tentées de recourir à des SMP françaises, la plupart d'entre elles iront vers ce qu'offre le marché, en fonction de la disponibilité immédiate et du coût.

Christian Lechervy rappelle qu'une bonne partie du débat ne concerne pas la France, puisque le Livre Blanc de la Défense rappelle son opposition à l'externalisation de fonctions de combat à des entreprises privées. Par ailleurs, il n'y a pas nécessité de transformer les lois actuelles parce que les besoins des entreprises ne l'imposent pas. **Christian Lechervy** concède quelques exceptions, notamment l'armement des bâtiments exposés à la piraterie maritime. Il y a un *« risque légal »* ajoute **Jean-Louis Bruguière**, que les entreprises comme les Etats s'exposent à d'éventuelles poursuites judiciaires en cas d'exactions commises par les SMP, jusqu'à la Cour Pénale Internationale en cas d'évolution de sa jurisprudence. *« Une entreprise qui n'aurait pas fait l'audit suffisant sur la SMP avec laquelle elle travaille pourrait être civilement responsable des exactions commises par celle-ci »* précise-t-il. En outre les SMP sont soumises à la juridiction des pays dans lesquels elles évoluent et non de la juridiction de l'entreprise qui va les embaucher, ce qui engendre un certain risque légal. **Christian Lechervy** partage ce sentiment : *« il faut également voir comment ces sociétés peuvent exporter des équipements de défense d'un pays tiers vers un pays tiers. La réforme des intermédiaires d'armement est sur la table depuis une dizaine d'années mais il faut en faire le choix politique »*.
Selon **Jean-Louis Bruguière** la problématique des SMP cache une question beaucoup plus générale : *« tout est un problème d'équilibre entre la protection des libertés individuelles et la sécurité collective. Force est de constater que dans le cadre de la politique européenne, le curseur est très proche de la protection des libertés individuelles »*. L'ancien juge

antiterroriste rappelle à cet égard la réticence du Parlement européen à fournir des données personnelles aux Etats-Unis dans le cadre la signature de SWIFT (accord TPTP).

La question de pose également de la protection par ces SMP des postes diplomatiques français, voire européens. Sans se prononcer sur la question durant son allocution, **Boris Boillon** a rappelé qu'il était l'un des seuls Ambassadeurs en Irak a bénéficie encore de la protection nationale, tandis que les autres s'appuient sur des sociétés de sécurité privée. L'occasion pour l'Ambassadeur de salué le professionnalisme et la flexibilité du GIGN, chargé de sa protection lors de ses déplacements, des gendarmes mobiles, qui s'occupent de la protection passive de l'Ambassade et de la Résidence, ainsi que des OPEX chargés de protéger les diplomates en mobilité. Témoignant de cette efficacité, l'Ambassadeur a relaté le rôle joué par le GIGN qui a tenu informé en continu l'Ambassadeur lors de l'attentat contre les chrétiens à Bagdad.

3 - Le développement durable peut-il contribuer à la sécurité de l'entreprise ?

Alexandra Trzeciak-Duval (OCDE) rappelle qu'aujourd'hui la croissance économique se situe majoritairement dans des pays qualifiés « d'instable » (entre 40 et 50) où les entreprises sont amenées à tenir compte de facteurs sociopolitiques pouvant avoir des conséquences sur leur activité. D'après elle, ces pays comptent une population dont la majorité a entre 15 et 25 ans, ce qui nous place devant l'obligation de leur assurer un emploi et un avenir économique sous peine de créer de l'instabilité de plus en plus en grave. Ainsi par exemple du Mozambique, qui connait une croissance de 10 % par an. Il existe souvent dans ces pays une classe de consommateurs émergents, comme au Burundi où la première entreprise est Heineken. Ces Etats recèlent également beaucoup de ressources naturelles, dont l'exploitation est à la fois insuffisante et mal encadrée. Le manque d'opportunités incite ces populations à se tourner vers des activités illicites et favorise le retour des conflits. Ainsi de l'Afghanistan d'où provient 90 % de l'offre mondiale d'héroïne, ce qui représente 2 milliards de $ de revenus pour le pays et compte pour 20 % de son PNB. Les conséquences sont également néfastes pour les pays environnants et à un niveau global, qu'il s'agisse des pressions migratoires dans les pays du Nord mais également au sein des pays du Sud eux-mêmes, notamment en Afrique, qui alimentent les trafics de drogue en développement.

Dans ce contexte d'instabilité, généralement alimenté par des inégalités sociales et un manque d'infrastructures, le développement durable joue un rôle fondamental. **Clara Gaymard**, PDG de General Electric France, début la seconde table-ronde en exposant sa vision du monde de demain, *« un monde où les valeurs d'éthique et d'environnement seront clé ».*
Comme **Dominique Lamoureux,** Directeur Ethique et Responsabilité d'Entreprise de Thales, le précise, il faut en premier lieu s'accorder sur une définition commune des mots morale et éthique : la morale relève de l'individu et contient les valeurs universelles et dogmatiques qui disent le bien et le mal, alors que l'éthique s'applique à l'entreprise comme ce qui est bon ou mauvais dans un contexte particulier. Les deux intervenants considèrent que le monde de demain façonnera l'univers d'action de l'entreprise duquel elle ne pourra se départir. Les condamnations ne sont plus seulement juridiques mais peuvent tout autant être morales. « *Ce qui est légal n'est pas toujours moral* » défend **Clara Gaymard.** En témoigne l'affaire du Sida, où les industries pharmaceutiques respectaient la loi mais étaient condamnées moralement car elles ne distribuaient pas gratuitement les rétroviraux ; ou la condamnation morale de l'attitude des Banques durant la crise financière. L'urbanisation galopante (80 % de la population sera urbaine en 2020) et la multiplication de pôles urbains (15 villes dépasseront les 15 millions d'habitants en Chine en 2015) obligent à une forme de sobriété tant la fabrication que dans la consommation d'énergie sous peine de ne pas pouvoir satisfaire tout le

monde. La croissance de demain sera faite d'innovations pour tous, c'est-à-dire de produits hautement technologiques mais accessibles à tous. A titre d'illustration, General Electric a créé un ultrason de la taille d'un *smartphone* permettant de faire de l'imagerie médicale à distance. Le monde de demain connaîtra une accélération des crises, et la responsabilité des élites s'en trouvera fortement appréciée. En effet, selon elle, le comportement du dirigeant est essentiel pour assurer la stabilité de l'entreprise en période de crise, et la première des qualités d'un dirigeant est sa capacité à naviguer dans l'incertitude. Enfin, **Clara Gaymard** estime que la croissance de demain ne se fera pas sans partage. Elle relève que les entreprises qui ont connu le plus fort taux de croissance sont celles qui ont su installer le partage de la connaissance dans leur croissance (Apple, Google). Toutes les entreprises devront se plier à cette logique pour être performantes. Il en est de même pour la question de la diversité. Si certaines entreprises la considèrent comme une menace, **Clara Gaymard** y voit un moteur de la réussite bien que ce ne soit pas facile à gérer lorsque plusieurs cultures et langues se mélangent. La Présidente de General Electric France suggère donc que l'évolution naturelle de la technologie comme du management de l'entreprise conduira celle-ci à faire de l'éthique une priorité.

Cécile Renouard (ESSEC) se démarque légèrement de cette vision. Elle se montre pour sa part assez pessimiste à l'égard d'une perspective instrumentale de l'éthique (win-win perspective) mais considère davantage l'éthique comme un aiguillon critique pour faire émerger les contradictions qui traversent les activités de l'entreprise, dans ses dimensions économiques et financières (répartition des bénéfices), sociales (à l'égard des salariés), sociétales (à l'égard des parties prenante), et politiques (effets sur l'organisation culturelle, économique, sociale et politique de la Cité). Selon elle, une bonne politique de développement durable est au service de meilleures relations entre l'entreprise et ses parties prenantes et accroit les chances d'une stabilité du tissu social.
L'entreprise ne peut pas s'implanter dans un pays sans connaître *« la société, les populations et leurs cultures »* précise **Bernard Frahi**, Directeur Sécurité de Sanofi-Aventis. Un constat que défend ardemment **Alexandra Trzeciak-DuvaL** pour qui la connaissance du contexte est le point de départ pour toute entreprise, qui se doit de connaître la culture, la composition ethnique, la religion, les intérêts des élites, les dynamiques sociales, et pour ce faire, entretenir un tissu relationnel est une priorité. Ces pays sont traversés par des interactions entre élites et non pas par un contrat social qui lie ces élites et leurs citoyens. **Jérôme Ferrier** va plus loin et défend que *« le développement durable est souvent étroitement lié à la sûreté. Pour bien sécuriser nos installations et nos personnels, il faut un bon relationnel avec les communautés locales et cela doit s'appuyer sur des activités de développement durable qui s'inscrivent dans le long terme »*. Ces relations de bonne composition permettent selon lui d'être mieux protégés, et notamment de recevoir les bonnes informations permettant de prendre connaissance d'évènements survenus au sein de la communauté ou bien d'être informé d'une éventuelle dérive permettant à la compagnie de faire savoir aux forces armées nationales qu'elles ont contrevenu aux règles décidées en commun. L'Ambassadeur **Boris Boillon** évoque quant à lui des raisons géopolitiques, voire civilisationnelles, devant inciter les entreprises à investir en Irak : *« une entreprise n'est pas seulement un compte bancaire, mais un projet structurant, des compétences, une potentialité de transfert de compétences, c'est-à-dire exactement ce dont les pays instables ont besoin pour traiter la cause de leur instabilité »*. Un moyen pour les entreprises, selon lui, de réaliser la main invisible d'Adam Smith, à savoir de servir leurs intérêts commerciaux tout en contribuant à l'intérêt général. Cela est d'autant plus pertinent à en croire **Alexandra Trzeciak-Duval**, qui rappelle que cette catégorie de pays instables est en majorité composée d'Etats qui ne pourront remplir les OMD (Objectifs du Millénaire pour le Développement), ce qui justifie d'autant plus une démarche éthique de la part des entreprises qui y investissent.

A la lecture de son expérience dans le Delta du Niger, **Cécile Renouard** nuance quelque peu ces propos et décèle plusieurs limites à l'engagement éthique des entreprises. Elle constate ainsi que le poids du passé rend les efforts pour changer les choses très compliqués. Deux grandes tensions demeurent : une contradiction entre une logique financière à court terme, et le principe du développement durable, tant dans le monde financier que dans le monde de l'industrie. Le souci d'un retour sur investissement à très court terme nuira toujours au développement durable. Un constat que partage **Bertrand Perrin,** professeur à la HEG (Haute Ecole de Gestion Arc), qui évoque *« la contrainte de l'immédiat »* qui s'impose à l'agent économique dans chacune de ses actions**.** Pour ce même motif, **Dominique Lamoureux** va même jusqu'à dire que les entreprises spéculatives ne sont aucunement concernées par l'éthique. La seconde tension relevée par **Cécile Renouard** procède des entreprises occidentales qui arrivent pour mettre en place des projets de développement durable, et qui abandonnent un système paternaliste pour devenir partenaire dans un projet dont elles n'ont pas la maîtrise. Elle a pu constater dans le Delta du Niger que les entreprises ne parvenaient pas à se défaire de ce paternalisme par contrainte, à la fois parce qu'elles doivent suppléer des pouvoirs publics déficients et corrompus, et également parce que les projets de développement durable sont devenus un moyen d'étouffer la contestation sociale. Il est difficile de changer les choses dans ce contexte. En outre, les actions menées par les entreprises s'inscrivent dans des ordres sociaux où les élites captent la rente sans une redistribution équitable. Les entreprises doivent donc jouer avec cette organisation sociale et ne parviennent pas à favoriser un développement équilibré qui profite à tous. Leurs politiques ont donc pour effet indirect et involontaire de renforcer les réseaux clientélistes, ce qui est en contradiction avec la volonté de l'entreprise. Cela pose donc la question de la revitalisation de la société civile, problème que soulève également **Alexandra Trzeciak-DuvaL.**
Des enquêtes sociologiques au Nigeria ont tenté de mesurer la contribution des entreprises à l'amélioration des conditions de vie matérielles des populations (« indicateur de sorite de pauvreté ») et sa contribution à l'amélioration du tissu social (« indicateur de capacité relationnelle »). On voit que les entreprises améliorent les conditions de vie matérielles des « host communities », dans son périmètre d'action, mais la qualité du tissu social s'est dégradée. La question de l'après pétrole se pose également et oblige l'entreprise à penser la gestion des infrastructures (électricité notamment) une fois qu'elle sera partie. L'enjeu déterminant c'est l'augmentation des inégalités, y compris à l'intérieur des villages, entre ceux qui ont accès à la rente et ceux qui vivent dans une grande misère. Aucun programme ne sera efficace tant que cette question essentielle ne sera pas réglée, a fortiori dans un contexte d'augmentation démographique et de faible niveau d'éducation. Les entreprises n'ont pas la solution à elles-seules, mais elles font partie de la solution.

Gérard Kuster, Directeur Ethique de GDF-SUEZ, précise comme **Dominique Lamoureux** que l'éthique des affaires se distingue de la morale, qui n'intègre pas les contraintes de la situation, ignore la nuance et est binaire. L'éthique accepte au contraire la discussion et les paradoxes. *« L'éthique des affaires a pour but l'application concrète de ce qui est moralement acceptable, ce qui est conforme aux valeurs de la société et de l'entreprise dans une situation donnée »*. Ce dilemme éthique se pose par exemple avec la question des «cadeaux ». En Allemagne, un simple calendrier peut ouvrir une enquête pour corruption, alors qu'en Chine, le fait de ne pas offrir un cadeau exclut de facto l'entreprise d'un marché. De même, **Gérard Kuster** pose le dilemme des paiements de facilitation que l'OCDE demande de supprimer, et qui s'avèrent indispensable dans certains pays. Dès lors, comme le Directeur de sécurité, le Directeur d'éthique se doit de tenir compte de certaines évolutions du monde :

- Il constate un développement du corps législatif, dont l'extra territorialité donnera à voir des conflits de règles. En témoigne l'usage que le Departement of Justice fait du *FCPA (Foreign Corrupt Practices Act)* pour engager civilement et pénalement la responsabilité de dirigeants, et les amener à avoir des dispositifs de prévention, ou bien du *Bribery Act*

britannique qui permettra dès 2011 de trainer devant un Cour britannique une entreprise ayant des activités même partielles sur le territoire du Royaume-Uni pour un cas de corruption partout dans le monde. Les Directeurs de sûreté jouent un rôle essentiel dans ce domaine, pour discuter, pour assurer une sûreté de transaction, de nos partenariats, par des méthodologies de choix et de certification, nous permettant d'optimiser notre politique de prévention, seul moyen d'éviter les condamnations. **Dominique Lamoureux** estime pour sa part que ce corpus législatif doit permettre à l'entreprise d'élaborer ses propres normes.

- L'approche « Risque » est prégnante dans l'éthique. **Gérard Kuster** a distingué sept risques éthiques pour GDF-Suez, risques composites qui sont l'agrégation de risques traditionnels. Tout d'abord, les risques liés à la présence dans un pays de faible gouvernance et notamment celui de non respect des droits humains. La question du travail forcé ou de travail des enfants se pose, mais également celle de savoir quelle entreprise employer pour protéger ses avoirs (infrastructures, personnels). Le risque existe de recourir à une entreprise qui se comportera en « cowboy » et qui ira jusqu'à filtrer les passages des employés de l'entreprise. Il peut également y avoir un risque financier, a fortiori dans un pays qui s'apparente à un paradis fiscal et dans lequel il faut travailler avec les banques : faut-il optimiser les avoirs dans ces banques ou ne servent-elles qu'à faire la gestion quotidienne des activités dans le pays ? Il y a aussi un risque de réputation : une ONG locale présente dans la zone peut s'attaquer à votre image. Le risque de réputation généré par un manque d'éthique est *« le seul qu'on ne parvient pas à maîtriser »,* avance **Gérard Kuster.**
- Le monde évolue en termes de technologie et le mésusage des systèmes d'information (usage imprudent de l'ordinateur, téléphone portable oublié dans le train…) est source d'enjeux éthiques. Le développement des réseaux sociaux pose de nouvelles problématiques, au regard notamment d'un jugement récent. On est là dans la recommandation visant à faire comprendre aux salariés qu'ils doivent prendre des décisions éthiques consistant à ne pas mettre un certain nombre d'informations en ligne. **Gérard Kuster** cite à titre d'exemple la formation délivrée par Mr **Péchenard** auprès des policiers, à qui il fut demandé la plus grande vigilance dans la publication d'informations pouvant les exposer à des risques, y compris en termes personnels (repérage…).

Bertrand Perrin distingue les contraintes imposées de l'extérieur en termes d'éthique par les différentes parties prenantes de l'entreprise et l'aspect purement éthique, fruit d'une démarche personnelle de l'individu qui se positionne par rapport aux règles morales et légales qui lui sont proposées. Un individu respecte la règle par crainte d'une sanction ou d'être pris et par adhésion personnelle à celle-ci. L'entreprise a pour mission première de créer de la valeur et l'éthique vient autour de cela. Mais il faut être conscient de la finalité qui nous amène à prendre une décision, donc l'entreprise n'est pas elle-même éthique mais s'impose des règles de déontologie soit parce que cet environnement lui impose par concurrence ou par crainte de sanction (vision utilitariste), soit parce que les acteurs de l'entreprise respectent ces enjeux éthiques. La formation est un outil important devant favoriser cette éthique personnelle. **Dominique Lamoureux** poursuit en ce sens et considère que c'est la multiplicité des parties prenantes qui oblige l'entreprise à un arbitrage permanent entre celles-ci : entre celui qui veut gagner plus (l'actionnaire), celui qui veut le produit de meilleure qualité (client), celui qui veut être payé davantage (salarié), celui qui soulève les problèmes sociaux et environnementaux (société civile). Dès lors, il convient selon lui de passer d'une logique rule-based, centrée sur des process en général élaborés par des consultants, vers une démarche value-based, centrée sur l'intelligence des êtres et sur les comportements.

Reste la question de la conciliation entre compétitivité et démarche éthique. Ici, le mot d'ordre semble être le partenariat. **Dominique Lamoureux** évoque ainsi la réunion des industriels européens de l'industrie aéronautique spatiale et de la défense pour élaborer des normes communes en matière éthique. 400 entreprises ont signé les *Common Industry*

Standards. Des négociations ont été ensuite été ouvertes avec leurs homologues américains, ce qui a donné naissance aux *Global Principles*, qui s'inscrivent un processus continu de progrès à travers un Forum annuel. L'aboutissement de le démarche a été l'organisation pour la première fois en 2010 de *l'International Forum on Business Ethics Conduct.* En s'accordant autour de principes communs, les entreprises peuvent faire émerger un front commun de refus, permettant éventuellement de se retirer d'un commun accord d'un appel d'offres comportant des exigences inacceptables sans craindre de se faire doubler par ses concurrents, jusqu'à devenir un avantage compétitif en faisant de cet engagement éthique un label nécessaire à la réponse à certains appels d'offre. L'éthique devient alors un enjeu de compétitivité.

4 - L'entreprise est-elle impuissante face à la cybercriminalité ?

La virtualisation est source de dilution de la sécurité pour l'entreprise, avec comme principal vecteur de fraude la cybercriminalité. Un enjeu si important pour les entreprises que **Régis Poincelet**, vice-président du CDSE, considère que *« le XXIème siècle sera celui du virtuel »*. Il distingue deux types d'attaques, celles que l'on peut qualifier pénalement et d'autres qui relèvent davantage du dénigrement et la diffamation pour lesquelles il n'y a pas de cadre pénal prévu. Face à cela, il estime que les entreprises auront toujours *« une guerre de retard »* par rapport aux criminels : un serveur au Texas où la législation est la plus permissive dans ce domaine, des opérateurs, un propriétaire et une adresse IP dans des pays différents. Face à des dispositifs extrêmement sophistiqués, l'arsenal juridique n'est pas adapté. *« A quoi cela sert de gagner un procès trois ans après l'attaque alors que le mal sera fait ? »* questionne **Régis Poincelet**, avant de rappeler que 110 milliards de spams icruclent chaque jour sur la toile.

Jean-Claude Marin, Procureur de Paris, est intervenu pour répondre à une question aussi simple que complexe dans les solutions à apporter : *« Comment faire face à la cybercriminalité ?»* La fraude a investi le territoire mondial qu'est Internet, ce qui n'est pas sans conséquences dans la vie des Nations. Les Etats ont mis du temps à trouver le bon tempo entre liberté du commerce et encadrement juridique pour lutter contre ces fraudes. *« Tout progrès comporte sa contrepartie en matière de fraude »* précise-t-il. Il n'existe pas de définition globale de ce qu'est la cybercriminalité, et elle n'est d'ailleurs pratiquement pas mentionnée en tant que tel dans le corpus français. La Commission Européenne a regroupé en trois types d'agissements différents ce qu'est la cybercriminalité : les infractions visant les systèmes de traitement informatisés des données, la délinquance traditionnelle utilisant de nouveaux moyens technologiques comme outils de leurs agissements, et les fraudes au contenu (pédophilie, racisme, terrorisme).

Le piratage est sans doute le plus grand risque offert par les nouvelles technologies, dès lors que l'entreprise ou l'Etat détient des informations monnayables. Ces actions sont souvent le fait d'organisations criminelles structurées, peu atteintes par les organes de poursuite, voire de structures dédiées à l'espionnage. Attrayante par *« son rapport bénéfices Vs risques très avantageux »*, cette menace nécessite un investissement très faible, a un effet de dispersion immédiat et offre des capacités de dissimulation considérables pour les fraudeurs. Le Livre Bleu des Assises de la Sécurité et des Systèmes d'Information identifie sept risques : le sabotage par les virus, les bombes logiques ou les dénis de service, le vol d'identités ou de fichiers, l'intrusion dans un système sans le détruire (spaming, fishing), le piratage de contenus numériques, l'atteinte à la vie privée par l'activité d'agents sur des réseaux sociaux,

et les contenus illégaux. Le coût de cette criminalité organisée est peu connu, en raison des coûts indirects et d'un nombre de plaintes inférieur aux crimes commis. La fraude à l'information devient en tout cas une des priorités des entreprises en termes de sécurité. Le risque d'atteinte aux libertés individuelles, via les réseaux sociaux, est important. Le partage des goûts, des centres d'intérêt offrent des éléments de la vie privée à des criminels qui peuvent ensuite les utiliser pour ternir la réputation ou faire chanter l'intéressé sous peine de révéler des informations compromettantes. La sécurité des systèmes d'information n'en demeure pas moins essentielle, à tel point que l'Institut National de la Recherche en Informatique et en Automatique a décidé de lancer un programme de recherche sur ces sujets, en initiant le 1er juillet 2010 un laboratoire de la haute sécurité informatique.

De nombreux cas connus témoignent de l'actualité de la cybercriminalité et de la diversité de ses formes. Tout d'abord la contrefaçon. S'agissant du piratage massif, la DCRI a révélé en mars 2010 qu'un nombre important de sites de collectivités locales et territoriales, ainsi qu'un site du ministère des finances faisaient l'objet d'une attaque massive de la part de deux sphères agissant sous pseudo. La DCRI a pu localiser les sites à partir desquels agissaient les pirates, à savoir la Corse et l'Afrique du nord, a pu identifier les adresses IP qui ont tenté des accès frauduleux et après réquisition auprès de l'opérateur, plusieurs serveurs proxy servant à dissimuler la localisation ont amené de Singapour jusqu'à Boulogne-Billancourt et l'interpellation d'un jeune de vingt ans qui n'avait d'autre but que d'assouvir un plaisir ludique. On voit là la difficulté d'une criminalité où se confond le hacker adolescent et des réseaux structurés qui n'ont pas en tête de visée ludique.

La fausse alerte virale est une autre typologie de fraude. Le site d'un important média s'est vu adresser une alerte émanant d'une structure inconnue, prévenant d'une attaque imminente par des hackers en raison des nombreuses failles du système. Moyennant une importante somme d'argent, cette source inconnue proposait d'identifier les failles et d'apporter les moyens de sécurité adéquats. Un échange a lieu, ce qui permet à une enquête de se mettre en place jusqu'à ce qu'une personne soit interpellée à tort, parce que les hackers avaient usurpé son adresse IP. Actuellement, une commission rogatoire internationale est en cours pour identifier l'auteur de la fraude, qui se situerait aux alentours de Casablanca.

L'exemple de la contrefaçon est également intéressant. L'atteinte à la propriété intellectuelle a permis à la fraude d'exploser, notamment par le biais de la vente aux enchères virtuelles. Kroll a évalué cette fraude à 440 milliards d'E. Le terrain de fraude est multiplié par dix chaque année, et les consommateurs sont autant inquiétés que les entreprises, puisque 10 % des médicaments vendus dans le monde seraient contrefaits. La protection de la liberté d'information et de la sphère privée, la garantie de la liberté du commerce électronique sont des obligations qui complexifient la lutte contre l'atteinte à la propriété intellectuelle. Un équilibre légal a pu être trouvé. La loi du 6 aout 2004 a transposé une directive communautaire du 22 mai 2001 autorisant certaines entreprises privées à mettre en place des systèmes permettant d'identifier, notamment par des adresses IP, les personnes mettant en ligne des fichiers contenant des œuvres protégées. Ce contrôle est soumis à l'approbation de la CNIL, laquelle a refusé à nombre d'entreprises la mise en œuvre des dispositifs au motif que les traitements prévus étaient disproportionnés au regard de la finalité poursuivie dans la mesure où ils n'avaient pas pour objet de déployer des moyens ponctuels et limités, mais plutôt une collecte massive de données personnelles et une surveillance exhaustive et continue des réseaux *peer to peer*. Par un arrêt du 23 mai 2007, le Conseil d'Etat a censuré cette décision de la CNIL au motif que la surveillance de quelques milliers de fichiers est minime par rapport à la charge par ces sociétés des droits de plusieurs millions de titres.
Certaines décisions rendues par le Tribunal de Commerce de Paris concernant les ventes aux enchères sur Internet sont intéressantes. Les fraudeurs ont choisi la toile pour évacuer nombre

de produits de contrefaçon sous la forme de ventes entre particuliers. Kenzo, Christian Dior, Guerlain, Louis Vitton ont intenté une action en justice contre Ebay pour violation de réseaux de distribution sélectif et diffusion de produits contrefaits. Ebay a nié toute responsabilité en sa qualité de simple prestataire technique, a contesté l'argument de réseaux de distribution sélectifs et a indiqué ne pas avoir les moyens de contrôler les annonces qui n'ont pas manifestement et intrinsèquement un caractère illicite. Par trois décisions du 30 juin 2008, validées par la Cour d'Appel de Paris, le Tribunal de Commerce a rejeté l'argumentaire d'Ebay. Concernant le contrat de distribution sélectif, Ebay n'est pas qualifié de simple hébergeur mais se livre à une activité de courtage et est donc considéré comme un acteur du commerce qui n'est plus simplement virtuel. Dès lors que le site a amplifié la vente de produits de contrefaçon en tant que courtier, l'entreprise a manqué à son obligation de vérifier que son activité ne générait pas d'actes illicites. Cet exemple démontre que la voie civile peut être parfois tout aussi essentielle que la voie pénale.

Si le corpus pénal s'est accru, la loi pénale est de souveraineté et ne s'applique donc qu'au territoire national. Un certain nombre d'extensions permet d'étendre des investigations mais rend la mise en œuvre longue et non adaptée aux besoins de réaction rapide des entreprises. Au nombre des outils dont ont besoin les entreprises et la justice, il faut des outils d'investigation qui soient à la mesure des nécessités des entreprises. Le temps de réaction et d'adaptation de la justice fut conséquent, mais encore faut-il que celle-ci dispose des spécialistes pour être plus efficace. Si la police a su avancer en la matière (CLTIC, DCRI et la BEFTI), **Jean-Claude Marin** précise que *« le Parquet de Paris est le seul à disposer d'une section dédiée aux fraudes en matière de cybercriminalité »*. Parmi les moyens existant, le Procureur évoque les perquisitions informatiques, le décryptage, le rallongement de la durée de conservation des données personnelles, l'infiltration numérique ou certaines innovations introduites prochainement par la LOPPSI 2 : captation des données à distance à des fins judiciaires, pénalisation du vol d'identité numérique, régime plus sévère en matière de contrefaçon par l'introduction de la « circonstance aggravante ». La Justice doit en permanence lutter contre l'anachronisme en veillant à adapter ses moyens à la réalité de faits criminels à haute technicité.

Précédemment dans la journée, **Olivier Buquen**, Délégué Interministériel à l'Intelligence Economique, avait rappelé que la protection des informations stratégiques des entreprises et des secrets d'affaires fait partie des missions de l'Intelligence Economique. Alain Juillet et Bernard Carayon s'étaient déjà penché sur la question, et un groupe de travail début 2010 fut créé, comprenant des représentants de l'administration, des entreprises, et notamment le CDSE. Ce projet, qui doit être soumis au Parlement prochainement, a trois objectifs : aider les chefs d'entreprise à définir le périmètre de leurs informations stratégiques, les aider à protéger leurs secrets d'affaires pour dissuader les personnes malveillantes de passer à l'acte, et offrir la possibilité aux entreprises de poursuivre civilement et pénalement celles-ci en cas de malveillance.

5 - Les risques d'une externalisation incontrôlée, à travers le cas du *cloud computing*

Nous avons vu avec la question des SMP que nombre d'intervenants exprimaient des craintes quant à au manque de contrôle de ces sociétés auprès desquelles on externalisait des fonctions de sécurité. A travers le *cloud computing* (déportation d'applications et de données d'un particulier ou d'une entreprise vers des serveurs à distance), on constate que l'externalisation de services, même lorsqu'elle ne porte pas sur la sécurité, s'avère porteuse d'insécurité et suscite l'inquiétude des entreprises. La définition introductive de la dernière table-ronde proposée par son animateur **Nicolas Arpagian,** coordonnateur d'enseignements à l'INHESJ, permet de prendre la mesure des risques inhérents au *cloud computing*. Selon la Commission générale de terminologie et de néologie, il s'agit d'un *« mode de traitement des données d'un client dont l'exploitation se fait par l'internet sous la forme de services fournis par un prestataire. C'est une forme particulière de gérance de l'informatique dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance du client »*. C'est cette dernière forme de nuage qui s'ouvre qui préoccupe les directeurs de sécurité. Comme le précise **Patrick Pailloux**, Directeur de l'ANSSI, cette « forme extrême » de l'externalisation informatique est économiquement avantageuse (rationalisation et mutualisation des moyens), mais engendre effectivement des failles du point de vue de la sécurité : mutualisation de serveurs avec d'autres moins sécurisés, méconnaissance de l'endroit de contrôle des données indisponibilité des prestataires en cas de crise, absence d'archivage des données, ou sous-traitance cachée à des prestataires inconnus. **Jean-Claude Marin** rappelle que le *cloud computing* conduit à des délocalisations de serveurs dans des Etats ou des systèmes juridiques où les protections sont défaillantes.

Toutefois, **Patrick Pailloux** ajoute que l'externalisation n'est pas toujours en opposition avec la sécurité et bien au contraire, *« elle peut apparaître comme un moyen de gérer sa sécurité en raison du manque de compétences en la matière au sein d'une entreprise »*. D'après lui, le problème est que l'externalisation est mal pratiquée en matière de sécurité parce que les entreprises s'attachent à la performance, aux coûts ou aux délais sans attention particulière accordée aux correctifs de sécurité. L'ANSSI va produire un guide sur l'externalisation destiné à rappeler un certain nombre de bonnes pratiques, fondées sur une analyse de risques (définir si l'entreprise rencontre un problème de confidentialité, de disponibilité…), la fixation des exigences de sécurité avec les prestataires et leur inscription dans un plan d'assurance sécurité. Ce guide comportera une liste de clauses susceptible d'inspirer nombre d'entreprises.

En dépit de ces limites, **Vivek Badrinath**, Directeur exécutif d'Orange Business Services, défend l'idée d'une croissance naturelle de l'externalisation, de l'ordre de 40 % par an, à mesure qu'augmente la demande de mobilité des particuliers comme des entreprises. Cette demande de mobilité s'exprime notamment via les *smartphones* qui correspondent à 50 % des ventes de terminaux aux entreprises et sur lesquels nombre d'applications nécessitent un traitement à distance. Cette croissance naturelle est en outre accréditée par **Nicolas Arpagian** qui rappelle que 700 millions du Grand Emprunt seront consacrés au *cloud computing* afin de faire émerger des acteurs français d'importances européennes voire mondiales. D'autre part, selon **Vivek Badrinath,** le logiciel qui permet d'affecter les ressources de calcul sur des serveurs virtuels murit, devient plus utilisable et intelligent, ce qui fiabilise son recours. Reste qu'il est nécessaire de prendre un maximum de précautions avant d'utiliser cette technologie. Parmi les méthodes de *cloud computing* envisageables, il évoque l'externalisation destinée à la réutilisation de centres de calculs ou de mutualisation de compétences en matière de sécurité informatique, avant de préciser qu'Orange offre une disponibilité 7j/7j, une

supervision depuis le territoire national pour les clients qui le souhaitent, une sécurisation des données au repos et dans le transfert, l'authentification des utilisateurs (notamment ceux en mobilité), l'isolation des ressources (serveurs sécurisés), et la conformité aux lois et règlementations en vigueur. Concernant la gestion des données médicales, Orange a obtenu la conformité pour cette solution intelligente : pour les entreprises qui n'ont ni les ressources, ni la taille pour mettre en place tout le dispositif de sécurisation données médicales, il devient intéressant de recourir à l'externalisation.

Alain Bensoussan, en tant que spécialiste de droit des contrats, considère *« totalement incongru de ne pas lancer dans cette nouvelle informatique »* qu'il traduit par *« informatique dans le brouillard »*. Le *cloud computing* apporte trois gains technologiques qu'il faut inscrire dans les contrats et organiser juridiquement. Le *cloud computing* offre une « informatique de flux » et un gain pour l'informatique industrielle où à la différence des systèmes de type ERP, tous les logiciels sont identiques et le programme source est vérifiable car rendu public. Le niveau de sécurité est donc beaucoup plus élevé que dans une sécurité dite fermée. Enfin, le *cloud computing* offre une « informatique synchrone » à travers la conjugaison irréversible entre le besoin et l'informatique.
Selon **Alain Bensoussan**, il est impératif de veiller à sécuriser les contrats à travers le respect de quatre droits : le « droit à la transparence » (savoir à tout moment où est et ce que fait la machine virtuelle) qui est totalement garantissable via des outils de supervision, le « droit à la localisation » (accéder aux logs qui donnent l'accès à la machine réelle et la machine virtuelle) en inscrivant dans le contrat l'interdiction d'une localisation dans tel ou tel pays, le « droit au contrôle immédiat » permettant un audit en temps réel de l'ensemble des machines virtuelles, et enfin le « droit à la sûreté », obligeant le fournisseur à démontrer à n'importe quel moment que son système est sûr. La localisation des données est totalement fiable mais la difficulté réside dans le suivi de ces données qu'il faudra inscrire contractuellement à travers notamment la garantie d'un « droit au cryptage » ou d'un « droit à la continuité » qui interdit la sous-traitance des machines virtuelles ou oblige à une autorisation préalable. Enfin, **Alain Bensoussan** rappelle qu'il faut observer la loi Informatique et Libertés qui prévoit dans ses articles 34 et 35 l'obligation de sécurité pour les responsables de traitement. Or la directive 95-46 a généralisé la protection des données personnelles à l'ensemble des pays européens, et il n'est possible d'exporter des données que vers les pays où le niveau de sécurité est équivalent. Cela a incité le Japon, la Chine, l'Inde et d'autres pays à mettre en place une règlementation adaptée aux normes européennes, laquelle Union Européenne s'est adossée à la position française. L'exigence de sécurité devient donc petit à petit universelle.

Pascal Brier, Directeur général adjoint d'Altran Technologies, précise de son côté que l'externalisation ne se limite pas au *cloud computing*, parce que l'on peut externaliser bien plus qu'un service informatique, à savoir une partie de son ingénierie ou de sa R&D. Trois problèmes se posent plus généralement : assurer la continuité de service, assurer la sécurité des biens et des personnes, et la confidentialité des informations. Finalement pour les deux premières obligations, il n'y a pas grande différence en termes de sécurité entre l'externalisation et la réalisation en interne. Il est par exemple possible d'imposer ses normes de sécurité aux prestataires. Par contre, un enjeu se pose concernant la confidentialité des informations mises à disposition, car « le facteur humain est souvent le maillon faible de la sécurité » selon **Pascal Brier**. De surcroît, dans les entreprises de services, la population relativement jeune n'est ni formée ni sensibilisée à ces problématiques de sécurité. Reste également à définir l'aspect critique d'une mission qui est externalisée. Pour cela, Altran a formalisé un *scoring* de ses missions qui va s'appuyer sur la sensibilité des personnes envoyées puis s'attacher aux accès de ses personnes (laboratoires, prototype, salle particulière, base de connaissances). Cette politique de sécurité doit se traduire par des pratiques simples à mettre en œuvre, à travers la formation, le contrôle des connaissances et le

maintien en condition : rappel des règles élémentaires de sécurité, rappel du cadre légal et des attentes spécifiques des clients en matière de sécurité. En dernier lieu, Altran fait signer un engagement de confidentialité aux intervenants lorsque la mission le requiert. Si **Pascal Brier** ne considère pas que cet engagement puisse avoir de légalité juridique, il estime toutefois que c'est un signe de responsabilisation pour l'entreprise, qui peut se couvrir.

Gwendal Le Grand, chef du Service de l'Expertise Informatique à la CNIL, précise que la CNIL est compétente en matière de *cloud computing* dès lors qu'il s'agit d'externaliser des données à caractère personnel, à travers un encadrement juridique et des garanties techniques.
Le problème de confidentialité des données se pose, que ce soit vis-à-vis du prestataire qui stocke les données ou bien des autorités d'un Etat étranger où opère le prestataire. Il existe également des enjeux de disponibilité du service, notamment pour ce qui est des données médicales qui peuvent permettre de sauver la vie d'une personne lorsqu'elles sont disponibles.
La loi de protection des données personnelles veut que les mesures de sécurité soient proportionnées aux risques présentés par le traitement. Juridiquement, la CNIL cherche à savoir qui est le responsable de traitement, c'est-à-dire la personne qui définit les finalités et les moyens. En tant que sous-traitant présumé, le prestataire aura des obligations particulières vis-à-vis de la loi, mais dans certains cas le manque de transparence du prestataire empêche un contrôle précis des conditions de stockage. Cela dépend également du type de *cloud computing* auquel une entreprise fait appel. Dans les solutions SAS, il y a plus de chances que le prestataire soit responsable de traitement.
La CNIL communique sur son site sur les bonnes pratiques en matière de sécurité, notamment via la publication récente d'un guide sécurité. La Commission Européenne envisage mi 2011 une évolution de la directive sur la protection des données et il y a des chances que la loi Information et Libertés inspire l'évolution de la directive. La CNIL aide également les entreprises et les Etats à se doter du cadre juridique adéquat. **Gwendal Le Grand** raconte ainsi que lors de la Conférence internationale des Commissaires à la protection des données l'an dernier, ceux-ci ont adopté les standards de Madrid. Une nouvelle résolution adoptée en 2010 pousse les Etats à adopter une Convention internationale en matière de protection des données. Le Président de la CNIL s'est rapproché du parlement et du gouvernement, afin d'obtenir leur soutien pour l'adoption d'une Convention Universelle sur la protection des personnes, qui s'avère être indispensable à l'ère de l'économie numérique.

Les entreprises de service s'accordent pour reconnaître à leurs clients une prise de conscience des exigences en matière de sécurité. Il y a un socle de certification requis (ISO 27000), ou un nombre considérable d'audits annuels. La CNIL envisage en 2011 de lancer une labellisation de procédure d'audits des systèmes d'informations et une labellisation de formations.

Un représentant du groupe La Poste note que l'un des soucis pour les entreprises est que les individus qui signent les contrats avec les prestataires de service ne relèvent pas de la DSI (Direction de la Sécurité de l'Information) mais la MOA (maitrise d'ouvrage), laquelle ne connait pas l'étendue de l'engagement qu'elle prend avec le prestataire. En ce sens, il existerait donc une rupture en termes de responsabilité entre le *cloud computing* et l'externalisation. Tout dépend, selon un autre intervenant, du type de *cloud computing*. *« Il y en a pour tous les deux finalement. Si une entreprise est en IAS* (*Infrastructure-As-Service) ou en PAS (Platform-As-Service), la DSI jouera un rôle de premier plan. De l'autre côté la responsabilité reviendra à la MOA si le cloud est en SAS (Software-As-Service) »*.

Synthèse du colloque annuel du CDSE du 25 novembre 2010, à l'OCDE, 2 rue André Pascal, 75016 Paris réalisée le 18 janvier 2011.