Joëlle NOAILLY
Université Lyon 2

Mémoire de Maîtrise

L'ESPIONNAGE INDUSTRIEL AU CŒUR DE LA GUERRE MONDIALE DU RENSEIGNEMENT ECONOMIQUE

Sous la Direction de :

René Sandretto

Année Universitaire 1996-1997

INTRODUCTION

Durant quatre décennies, la confrontation géostratégique entre les deux blocs hégémoniques américain et soviétique a déterminé l'organisation bipolaire du monde. La période des 30 Glorieuses et l'affrontement idéologique Est-Ouest ont longtemps masqué les conflits économiques entre les Etats-nations. Puis, l'effondrement du bloc communiste a brutalement bouleversé l'ordre établi des relations internationales. La problématique militaire Est-Ouest est devenue soudain obsolète, et a laissé la place à une logique économique.

La guerre économique[1] a succédé à la guerre froide. L'objectif, aujourd'hui, n'est plus la conquête territoriale ou coloniale. Sous l'impulsion d'une économie globalisée, il s'agit désormais de conquérir des marchés et des technologies. Chaque nation doit encourager ses entreprises à porter haut ses couleurs, en les mettant en état d'innover, d'exporter sans cesse davantage, de s'implanter à l'étranger… Cependant, alors qu'historiquement les Nations mettent un terme à leurs différents par un Traité, ce n'est pas le cas des entreprises qui sont condamnées, selon les lois de l'économie de marché, à une situation de perpétuelle concurrence.

Dans ce nouvel ordre mondial, à la concurrence acharnée, les vraies richesses ne sont plus les matières premières. La créativité et l'innovation sont des atouts fondamentaux des entreprises jetées dans le conflit mondial. Ces dernières doivent, pour assurer leur survie, se tenir constamment à l'affût de la nouveauté. Dans ce contexte, les systèmes d'informations apparaissent comme un facteur décisif de la guerre technologique et industrielle.

Cependant, l'analyse de la menace économique et de ses pratiques révèle le risque de généralisation d'un nouveau cancer : l'espionnage industriel. Ce phénomène connaît une ampleur sans précédent depuis quelques années et la négation de cette activité, souterraine mais extrêmement bien organisée, peut coûter cher aux entreprises et aux nations industrialisées.

1 L'expression de « guerre économique » a été utilisée dès 1935 par Franklin D. Roosevelt. Elle apparaît en France au début des années 1970 à travers un slogan publicitaire pour une société européenne engagée dans l'électronique : « La Troisième Guerre Mondiale sera une guerre économique : choisissez dès à présent vos armes ». B. Essambert. *La guerre économique mondiale*. Paris : Olivier Orban, 1991. p 15.

Notre étude vise, ici, à établir le constat de l'étendue de ces pratiques qui vont à l'encontre de la loi et de tout code moral. Il ne s'agit donc pas d'y apporter une justification, ni pour autant de les dénoncer ouvertement.

A cette fin, notre analyse suivra le cheminement suivant :

- dans une première partie, nous tenterons d'expliquer le recours massif à l'espionnage industriel. Cette première phase sera l'occasion de souligner le rôle majeur de l'information dans le nouveau contexte mondial ;
- dans une seconde partie, nous mettrons en évidence l'organisation de l'espionnage industriel à l'échelle mondiale. Nous décrirons la structure, les procédés et les règles en vigueur sur le marché des informations volées ;
- enfin, dans une troisième partie, nous nous attacherons à proposer les solutions dont disposent les entreprises pour contrer l'espionnage industriel. Ce sont les instruments de prévention qui restent les plus efficaces dans ce domaine.

CHAPITRE 1

L'INFORMATION, ENJEU DE LA GUERRE ÉCONOMIQUE

Selon Juno Nakagawa, fondateur de la Society of Competitors Intelligence Professionals, système japonais de gestion de la connaissance, l'économie mondiale est entrée dans l'ère de la « révolution de l'information »[1].

Le terme *information* peut prêter à confusion, tant son champ d'application est large. Avant de poursuivre notre analyse, il convient donc de préciser, dès à présent, la définition que nous retiendrons par la suite.

Notre société est submergée d'informations : journaux, radios, télévision… mais toutes ces natures et toutes ces formes d'informations ne visent pas les mêmes objectifs. Il est possible de distinguer trois familles[2] :

- les informations dites générales : elles sont destinées au grand public par l'intermédiaire des quotidiens et autres « bulletins d'informations »,
- celles à finalité pédagogique : elles sont intégrées dans les formations humaines,
- celles qui servent à travailler : l'information juridique, médicale, financière ; l'information sur les marchés, les innovations ; l'information scientifique et technique, industrielle, commerciale, sociale.

C'est cette dernière catégorie que nous retiendrons dans notre étude, c'est-à-dire les informations destinées à l'homme au travail. Nous pouvons les regrouper sous le terme d'« informations professionnelles[3] ». Nous utiliserons indifféremment les dénominations de renseignement, connaissance et information économique.

[1] Christian HARBULOT. *La machine de guerre économique*. Paris : Economica, 1992. p 89.
[2] selon la classification établie par René Mayer. COMMISSARIAT GENERAL AU PLAN. *Information et compétitivité*. Rapport du groupe présidé par R.Mayer. Paris : La Documentation Française, 1990. p 14.
[3] cette terminologie est préférée à celle d'information scientifique et technique qui présente le défaut de ne considérer qu'une logique d'offre – on s'intéresse à la manière dont celle-ci est produite et diffusée dans les laboratoires et entreprises. Au contraire, l'information professionnelle englobe les deux logiques : l'offre et la demande. COMMISSARIAT GENERAL AU PLAN *Information et compétitivité*. op. cit. p16.

L'information apparaît tantôt comme le produit d'un même secteur et tantôt comme un facteur de production qui circule et irrigue tous les secteurs, oriente le choix des entreprises, leur désigne les marchés porteurs, réduit leurs risques d'erreurs et détermine pour une large part leur niveau de productivité et de compétitivité.

Il existe donc un marché de l'information avec une offre – la production d'information par les laboratoires et entreprises – et une demande – la recherche d'informations à l'extérieur de l'entreprise. C'est sur ce marché que va se fixer le prix de l'information.

Après ces quelques précisions, on comprend désormais le sens de l'expression utilisée par Nagakawa. L' ère de la « révolution de l'information » constitue l'avènement d'un nouveau système économique au centre duquel l'information professionnelle est devenue un enjeu de survie, mais aussi de domination. En résumé, le fondateur du système d'intelligence japonais l'a bien compris : tous les acteurs économiques doivent désormais déployer de véritables dispositifs offensifs pour capter l'information et donc s'armer dans la guerre économique.

SECTION 1 – LA NOUVELLE DONNE ECONOMIQUE MONDIALE

Depuis la fin de la seconde guerre mondiale, le paysage économique s'est transformé en un système de plus en plus contradictoire et complexe. La globalisation des échanges s'est faite en parallèle avec la polarisation des rapports de force. Firmes et nations s'affrontent dans une course acharnée pour la compétitivité. L'internationalisation des échanges impose désormais aux agents économiques une démarche anticipative et non plus seulement réactive face aux changements de leur environnement. C'est pourquoi dans cette nouvelle donne économique, l'information et la culture du renseignement acquièrent une importance stratégique incontournable.

1. Un monde complexe et conflictuel

L'analyse du monde économique a atteint en moins d'un quart de siècle un haut niveau de complexité. Les conflits économiques ont remplacé les affrontements militaires. La structure de l'économie mondiale a subit une double mutation : la

mondialisation des échanges et dans le même temps la construction d'un nouvel échiquier mondial autour des pôles économiques émergents.

A – La mondialisation des échanges

La mondialisation des rapports de forces économiques est un phénomène relativement récent. Après la seconde guerre mondiale, la multiplication des liens économiques entre les pays occidentaux a contraint les nations à restreindre l'éventail de leurs mesures protectionnistes. L'ouverture des frontières a bouleversé les règles de fonctionnement de la compétition commerciale. Ainsi, la mondialisation des échanges a contribué à créer un espace-temps particulier, dans lequel la concurrence est intense et surtout perpétuelle. L'essor des systèmes informatisés et la multiplication des moyens de communication ont accéléré ce phénomène.

Nous pouvons citer quelques-uns des éléments qui caractérisent la nouvelle économie mondiale globalisée :

- Les marchés subissent un découpage géographique en marché local, national, régional, et mondial. Chacune de ces strates concurrentielles doit être étudiée de façon spécifique. Les erreurs stratégiques peuvent porter des coups mortels. Avec l'internationalisation des échanges, laissant apparaître la multiplication des OPA et OPE, la notion de secteur protégé n'existe plus.

- La déréglementation et libéralisation des pratiques financières ont créé de nouveaux circuits financiers. L'interconnexion des marchés et l'« électronisation » des valeurs boursières ont accéléré la circulation des informations.

- Le développement technologique se diffuse, à présent, de façon transversale, et non plus horizontale ou verticale, c'est-à-dire cloisonné par secteur d'activité.

- Les marchés se sont atomisés en micro-cibles fugaces, augmentant les risques en matière de lancement de produit. On voit ainsi naître de nombreuses versions de gammes. Les cibles sont définies avec plus de rigueur et de précision, afin de proposer des produits parfaitement adaptés.

- La durée de vie des produits étant de plus en plus courte, le poids de l'innovation dans la bataille pour la compétitivité des entreprises devient primordial. L'entreprise s'est transformée en centre de créativité. Les innovations et inventions techniques sont devenues les aliments essentiels de la guerre économique. Le changement technologique connaît une accélération sans précédent.

- Tous les acteurs se trouvent confrontés à l'ère de l'intelligence de masse. Les vraies richesses sont le nombre d'étudiants et de chercheurs. Or le coût de la recherche est tel qu'une entreprise, quelle qu'elle soit, a intérêt à « profiter » ou exploiter les innovations technologiques des autres entreprises.

- Toute activité économique, même de nature industrielle, connaît une forte tendance à la tertiairisation : les technologies utilisées reposent sur des savoirs-faire ; la production met en œuvre des méthodologies et moyens informatiques sophistiqués ; la prospection commerciale et la vente dépendent largement de l'étendue des données disponibles sur les marchés et la concurrence.

B – Un nouvel échiquier multipôlaire

Les conflits économiques sont nombreux et dispersés autour de différents pôles. Les relations concurrentielles recouvrent désormais quatre champs d'actions :

a) Les rapports de force s'expriment d'abord à l'échelle de la planète entre les 500 premiers groupes mondiaux dans le cadre d'une compétition commerciale et technologique caractérisée par une course effrénée à la taille critique. Le poids de ces multinationales dans les économies nationales et le commerce international acquiert une dimension considérable. La maîtrise de technologies-clés permet de bénéficier d'un avantage compétitif de premier entrant sur les marchés ou d'une position forte dans les négociations[1].

b) L'émergence des zones économiques régionales et l'institution de la Triade fragilisent l'équilibre des relations internationales, d'autant plus qu'il existe des conflits internes à l'intérieur de chaque entité. Chaque pôle développe des stratégies d'expansion en direction des deux autres.

[1] Ces affrontements se développent selon une logique de « coopération-concurrence ».
Les relations de « coopération-concurrence » entre les grandes firmes de deux pays leur confèrent une position dominante et créent un risque de dépendance technologique accrue des entreprises des autres Etats.
COMMISSARIAT GENERAL DU PLAN. *Intelligence économique et stratégie des entreprises*. Rapport du Groupe dirigé par H. Martre. Paris : La Documentation Française, 1994. p14.

c) La montée en puissance de l'économie japonaise et allemande aux dépens des États-Unis caractérise la relance des dynamiques nationales dans la mondialisation des échanges. Les stratégies d'intérêt national se développent de plus en plus dans les relations économiques internationales. Les affrontements se concentrent désormais sur les domaines stratégiques que les États contrôlent (les technologies critiques dans l'industrie de l'armement) ou tentent de préserver (l'électronique ou l'automobile).

d) Instituées comme nouveaux pôles de décision économique, les régions se situent au cœur des nouvelles logiques de la compétition mondiale et développent, notamment en Europe, des relations contradictoires de concurrence et de délocalisation. Les rivalités interrégionales s'accroissent alors que se développent parallèlement de multiples initiatives de coopération et d'alliances entre régions. Ces dernières agissent avec plus d'autonomie, au risque de frictions avec l'État, voire de contradictions avec les politiques économiques nationales.

La matérialisation de l'ensemble de ces conflits économiques dans le temps et dans l'espace nécessite une complémentarité des différents types de savoir. Le savoir de l'entreprise (production, exploitation, management, marketing…) ne résout plus tous les problèmes. Face à la complexité croissante des relations concurrentielles sur les différents échiquiers, l'information est devenue le facteur « discriminant[2] » qui va déterminer en grande partie le niveau de chacun des autres. C'est en ce sens que nous pouvons considérer l'information comme une ressource stratégique.

2. Le rôle stratégique de l'information

Existe-t-il une corrélation entre information et compétition ? Ces deux concepts sont trop larges pour pouvoir répondre précisément à cette question. Cependant, il est établi qu'il existe une corrélation entre, d'une part, la sensibilité à l'investissement immatériel (Recherche & Développement) et, d'autre part, la profitabilité.

---

[2] plus que tout autre facteur qui concourt au développement économique et culturel : l'efficience du capital productif, la productivité des travailleurs, le coût des transports, la disponibilité de l'énergie, le sens de la communication, le dynamisme commercial, etc.
COMMISSARIAT GENERAL AU PLAN. *Information et compétitivité*. op. cit. p14.

Dans l'entreprise, l'information revêt de multiples fonctions : facteur de production, denrée stratégique, ferment d'innovation, atout commercial… Elle s'intègre en deux étapes dans la stratégie de l'entreprise : elle permet, dans un premier temps, de surveiller l'environnement extérieur, puis à partir de ces résultats, d'optimiser les décisions au sein de l'entreprise.

A – Instrument de mesure de l'environnement extérieur

L'information permet de mettre en évidence l'évolution du marché, en révélant les comportements des concurrents, leurs ambitions, les pays où ils commercialisent leurs produits ou services. Il faut également surveiller la vitesse des évolutions de la science, de la technologie, des habitudes, afin de connaître les produits rentables financièrement ou les produits en déclin.

La nécessité absolue d'innover, de ne pas se contenter de produire et de vivre sur ses acquis, a induit une prise de conscience croissante de l'intérêt de maîtriser parfaitement les informations concernant l'industrie et les services pour surveiller, se défendre, attaquer. Être au courant des évolutions dans son secteur d'activité est un impératif vital, les données scientifiques, techniques, technologiques, technico-économiques évoluent sans cesse et il faut surveiller les tendances, déceler les indices de changement, essayer de deviner les synergies possibles, anticiper, être toujours prêt à innover.

En résumé, l'information permet de mesurer le degré de liberté et de menace sur un marché pour une entreprise. La collecte d'informations dans ces domaines est donc au cœur des nouveaux défis de l'entreprise.

B – Optimisation de la prise de décision

Selon H. Martre[3], « pour prendre des décisions économiques optimales, il faut comprendre la réalité dans laquelle elles s'appliquent. Comme dans l'impressionnisme, on se sert des éléments glanés ici et là pour brosser le tableau le plus proche possible de la réalité ». La connaissance de l'environnement est donc un facteur décisif dans la construction d'une prise de décision stratégique.

Une étude menée auprès de chefs d'entreprise a permis d'effectuer un classement entre différents facteurs de compétitivité[4]. Parmi les 6 facteurs arrivés en tête figurent : l'adaptation à la demande, la qualité de service, l'image de marque, le rapport qualité-prix, l'avance technologique et les méthodes de distribution. Or, ces 6 facteurs incorporent tous une proportion d'information considérable.

S'adapter à la demande, améliorer la qualité du service suppose de bien connaître les besoins du client. L'image de marque résulte des efforts de communication intégrés dans la stratégie de l'entreprise. De même, l'avance technologique et la distribution nécessitent une recherche constante d'informations pertinentes.

Ainsi, ce sont ces informations qui vont définir et encadrer le système de production, le système commercial, la recherche et le développement…Le mûrissement rapide des produits amène les entreprises tantôt à se spécialiser et tantôt à se diversifier. L'activité des concurrents oriente les axes de recherche. L'innovation se nourrit des travaux des laboratoires de recherche étrangers. Les stratégies commerciales de partage de marché sont élaborées en fonction de l'évolution du marché.

Dans un contexte économique concurrentiel et conflictuel, les entreprises se doivent d'être toujours en avance sur leurs adversaires. Aujourd'hui, c'est l'information, plus que tout autre facteur de production, qui procure un avantage compétitif. L'information économique permet de prévoir et donc d'anticiper les stratégies : développer de nouveaux produits, devenir plus performants, prendre des décisions, mieux vendre…
Enjeu de survie et de développement des firmes, le renseignement économique stratégiquement utilisé au sein des Etats-nations peut devenir une arme de domination économique sur la scène mondiale.

---

[3] Bertrand Warusfel. « Intelligence économique et sécurité de l'entreprise ». *Problèmes économiques*, n°2.497, décembre 1996. p3.
[4] étude réalisée pour la Direction Générale de l'Industrie et le Commissariat Général du Plan auprès de 845 entreprises , décembre 1989. COMMISSARIAT GENERAL DU PLAN. *Information et compétitivité*. op. cit. p64.

SECTION 2 – L'INFORMATION, ARME DE DOMINATION ECONOMIQUE

Les entreprises ou économies qui maîtrisent l'information sont aujourd'hui celles qui réussissent à s'imposer dans la compétition mondiale. Plus une économie est en mesure de collecter l'information, plus elle accroît sa puissance, et s'arme dans la guerre économique. Les techniques de manipulation de l'information sont devenues des instruments offensifs et destructeurs face aux concurrents. Beaucoup plus qu'un enjeu de survie dans la compétition mondiale, l'information établit les rapports de forces entre nations.

1. Puissance économique et information

Le Japon est le pays qui affiche la plus belle réussite économique et industrielle des 20 dernières années ; grâce à sa « culture de l'information », il a réussi à se hisser dans les plus hautes sphères de l'économie mondiale, dominant ainsi le modèle américain.

En prenant appui sur une industrie lourde de l'information, les Japonais ont redéfini une approche du développement économique très différente de la vision occidentale. Alors que les Japonais sont entrés depuis 15 ans dans la troisième Révolution Industrielle les États-Unis, quant à eux, gèrent encore les séquelles de la seconde. Avant de présenter le modèle japonais, il n'est pas inutile de revenir sur les revers économiques des États-Unis. Cette présentation préliminaire permet de mieux faire apparaître par la suite la spécificité d'une puissance japonaise qui repose entièrement sur l'information.

A – La carence informationnelle des Etats-Unis

Après 70 ans de domination sur l'économie mondiale, la remise en cause de l'hégémonie américaine est dorénavant un fait incontesté. L'aggravation de l'endettement interne et externe des États-Unis a fait passer ce pays du statut de créditeur du monde occidental à celui de débiteur du Japon. Ce renversement de situation a interpellé tous les acteurs mondiaux sur le bien-fondé de leur stratégie économique mais aussi sur l'efficacité de leurs méthodes.

Les entreprises américaines ont pendant longtemps considéré leur marché national comme un sanctuaire économique ; les entreprises étrangères concurrentes ne jouant, elles, qu'un rôle relativement marginal. La situation de leadership dans tous les domaines (militaires, économiques, scientifiques) a incité les managers américains à n'accorder qu'une attention distraite aux tactiques commerciales et stratégies offensives des firmes étrangères. Or, l'influence culturelle américaine était telle que tous ses partenaires ont développé la même perception de l'évolution du marché mondial.

Cependant, depuis quelques années, les États-Unis enregistrent une série de revers technologiques et commerciaux ; dans le même temps, la part de l'Asie dans les exportations mondiales s'est accrue de presque 10 points. Les analystes américains considèrent ce rééquilibrage comme le révélateur des défaillances internes de leur économie. La déficience des entreprises américaines n'est donc pas un phénomène conjoncturel mais structurel.

Le modèle offensif américain souffre d'une carence informationnelle. Or, les nouvelles puissances économiques qui menacent aujourd'hui la suprématie américaine ont une approche stratégique de la gestion de l'information. Le renseignement économique est l'un des leviers fondamentaux de l'essor industriel japonais. Les États-Unis n'ont pas su s'adapter à la nouvelle révolution de l'économie mondiale. Leur position de leadership sur le marché international les a conduits à négliger l'observation de l'environnement mondial, facteur désormais décisif pour participer à la course à la compétitivité.

B- La culture de l'information au centre du modèle offensif japonais

Le retard économique du Japon au début du XX^{ème} siècle ne l'a pas empêché d'employer des méthodes d'approches du marché très novatrices. Le modèle japonais gère l'information de manière stratégique en appliquant trois principes-clés : recueil, centralisation et diffusion, c'est-à-dire capitalisation de l'information.

Le Japon est, incontestablement, la nation qui a su tirer le plus grand profit de l'information. A l'évidence, les Japonais l'utilisent comme une arme nécessaire parmi d'autres pour gagner la guerre économique. Ainsi les auteurs du rapport « Japan 2000[1] », paru en 1991 aux États-Unis, décrivent le modèle japonais en ces termes : « La stratégie du Japon est axée sur la conquête, le contrôle et l'utilisation de la puissance. Toutefois, la puissance du Japon n'est pas construite sur une supériorité militaire mais essentiellement

[1] Christian HARBULOT. *La machine de guerre économique*. op. cit. p 27.

sur la connaissance et sur la technologie de l'information. L'acquisition de la connaissance a été et demeure toujours un fantastique atout de supériorité en faveur du Japon. »

La recherche d'information fait partie intégrante de la tradition japonaise. Le peuple japonais est l'un des plus avides d'informations. Chaque Japonais se sent investi d'une mission au profit de son entreprise. Faisant corps avec son entreprise, il a des réflexes, à l'étranger, de recueil d'informations. En 1986, plus de 5 millions de Japonais sillonnent le monde et 500 000 résident à l'étranger. Cette spécificité culturelle se révèle depuis 40 ans un atout majeur dans la performance économique japonaise.

Les Japonais s'exercent à tirer profit de tout ce qui est étranger. Dès l'époque Meiji, la doctrine japonaise devient : « Nous irons chercher la connaissance dans le monde entier afin de renforcer les fondements du pouvoir impérial ». Ainsi, la méthode japonaise définit un système d'ouverture vers « l'extérieur » dans le but d'enrichir « l'intérieur ».

Au départ, c'est en pratiquant une politique systématique d'achat de technologies et de savoir-faire que le Japon a pu rattraper son retard. A titre d'exemple, entre le 1er janvier 1978 et le 15 juin 1980, on dénombre 102 licences de fabrication acquises par le Japon dans le domaine aéronautique et militaire[2]. Lorsque le savoir-faire et la technologie ne peut être acheté, les entreprises japonaises procèdent à une recherche d'information très active : suivi des brevets, des expositions et salons, participation à de nombreux colloques et séminaires, visites d'entreprises à l'étranger, examen des produits concurrents, utilisation de stagiaires…

Par conséquent, si le Japon a su devenir depuis en quelques années, le leader mondial dans de nombreux domaines, c'est parce que, très tôt, il a su aller chercher l'information chez ses concurrents. C'est en s'inspirant fortement de la technologie de l'optique photographique mise au point avant la seconde guerre mondiale par les Allemands, que le Japon a pu se dresser au premier rang mondial dans ce secteur. Aujourd'hui, à l'heure où les Japonais conçoivent une navette spatiale qui devrait être mise en service avant l'an 2000, leur intérêt se porte vers les matériaux composites capables de résister aux fortes températures et donc vers la France qui possède encore une certaine avance dans ce domaine.

En consacrant 1,5% de son chiffre d'affaires à la collecte d'informations, soit plus du double que les États-Unis, le Japon est devenu un pôle économique offensif. La puissance

[2] Jacques VILLAIN. *L'entreprise aux aguets*. Paris : Masson, 1990. p 64.

du modèle japonais démontre que la réussite économique passe aujourd'hui par la gestion stratégique de l'information.

2. Pouvoir et manipulation de l'information

A l'origine, les techniques de manipulation de l'information, telles que la sous-information, sur-information, les effets de caisse de résonance ou encore la désinformation, ont été mises en pratique par les services secrets soviétiques. Aujourd'hui, les grandes entreprises, quelle que soit leur nationalité, les utilisent volontiers à des fins stratégiques. En avance d'une révolution, c'est, une fois de plus, le Japon qui a le mieux assimilé ces pratiques.

A – Sous-information et sur-information

a) La *sous-information* consiste à filtrer et doser les informations qui sortent de l'entreprise ou du pays. Les renseignements alors disponibles sur le marché sont uniquement ceux que l'entreprise a bien voulu laisser s'échapper.

Depuis toujours, les Japonais ont utilisé cette tactique pour masquer leurs lacunes. Ils ont pratiqué la sous-information en jouant sur la difficile assimilation de leur langue par des étrangers. A titre d'exemple, parmi les 40000 périodiques japonais, tous domaines confondus, recensés par l'Union List of Periodicals, 30% au maximum de ces publications sont en langue anglaise ou possèdent un résumé en anglais[3].

Selon le professeur Umezao, conseiller du gouvernement japonais, « si le Japon est aujourd'hui le deuxième producteur au monde en matière d'information, 2% seulement de ces informations sont accessibles hors du Japon ». Si le Japon est un grand importateur d'information, il sait maîtriser celle qu'il produit à l'extérieur. En contrôlant la diffusion de l'information, le Japon dissimule souvent ses stratégies commerciales pour ne pas alerter la concurrence. Il reste ainsi en position de force.

[3] J. VILLAIN. *L'entreprise aux aguets*. op. cit. p.75.

b) La *surinformation* est, elle aussi, une tactique très efficace. Elle consiste à noyer ses concurrents sous la masse d'informations complexes, rendant leur traitement impossible. Ce danger menace aujourd'hui un grand nombre de pays, quand on sait que la quantité d'informations déversée sur le marché croît de 30% par an.

Le Japon a pratiqué la surinformation sous une forme beaucoup plus subtile. Fort de son système unique au monde de gestion de l'information, le Japon s'est désigné comme un modèle à imiter et a entraîné tous ses concurrents dans la course au renseignement économique. Les Japonais sont les initiateurs du développement du technoglobalisme, défi introduisant la compétitivité dans le monde immatériel de la connaissance. Dans ce climat de « surinformation », le Japon a réussi à vendre comme des données objectives les produits finis de son industrie de l'information. En diffusant ses propres conseils et technologies en matière de recherche d'information, le Japon entend contrôler toutes les sources principales de la connaissance et prendre ainsi une option sérieuse sur le contrôle du nerf de la guerre économique de demain.

B – La désinformation et les caisses de résonance

a) La *désinformation* consiste à communiquer de fausses informations pour masquer les vraies et égarer ainsi l'adversaire vers une connaissance erronée de l'environnement. Cette tactique entraîne les concurrents à négliger des secteurs entiers pendant que l'entreprise responsable de la désinformation développe une stratégie agressive. Elle peut conduire ainsi à une élimination destructrice des adversaires.

La désinformation est une pratique de plus en plus répandue et les exemples sont nombreux. Une société aéronautique américaine avait fait réaliser, il y a quelques années, une fausse étude de marché concernant le renouvellement des flottes aériennes. Elle s'est ensuite arrangée pour que cette étude soit acquise par des concurrents et les a donc lancés sur de fausses pistes.

b) Sans être véritablement faussée, l'information peut également être influencée volontairement. C'est le cas de la technique dite des « *caisses de résonance* ». Une entreprise peut utiliser toutes sortes de moyens pour faire dériver l'information, qui circule sur son compte, de son objectivité. L'information « sous influence » est obtenue par des pratiques allant jusqu'à l'achat des faveurs de politiciens et autres membres administratifs.

Une image de marque trop agressive peut ainsi être considérablement adoucie ; la méfiance des concurrents en sera d'autant plus affaiblie.

C'est par l'utilisation de ces « caisses de résonance » que les Japonais tentent de canaliser les effets de leur expansionnisme commercial, dénoncé comme une nouvelle forme d'impérialisme. Le gouvernement japonais dépense ainsi des millions pour donner une image valorisante à l'action des entreprises nippones sur le territoire américain.

Bien maîtrisée et bien utilisée, l'information est une arme puissante au sein de la guerre économique. Elle permet de construire des stratégies offensives à condition d'être maîtrisée et efficacement gérée. Après l'effondrement du bloc communiste, la plupart des économies occidentales ont brutalement pris conscience de la nouvelle nature des conflits qui se jouaient sur la scène mondiale. Les économies qui avaient placé la chasse à l'information comme objectif majeur se sont imposées en tant que puissance économique. La guérilla de l'information dans laquelle se sont depuis peu lancés tous les pays industrialisés s'organise selon des méthodes où les barrières de la déontologie sont parfois transgressées.

Section 3 – Capter l'information :

de l'intelligence économique à l'espionnage industriel

Nerf de la guerre économique, l'information est devenue un enjeu à la fois de survie et de pouvoir. De nombreux débats nationaux ont été lancés, quant à savoir comment récupérer partout dans le monde cette information devenue stratégique.

La plupart des gouvernements tentent aujourd'hui de mettre en place, au sein de leurs entreprises, des systèmes complets organisant à la fois la collecte, le traitement et la circulation de l'information. De nouveaux concepts, comme ceux d'intelligence économique[1] et de veille technologique, voient le jour pour répondre à cette course à l'information. En France, Henri Martre, ancien PDG de l'Aérospatiale, a été chargé en 1992 d'un rapport pour le Commissariat au Plan sur « l'intelligence économique et les stratégies industrielles ».

Souvent confondu avec la veille technologique, l'espionnage industriel est une toute autre alternative pour le recueil d'informations. Certaines entreprises, dépourvues de déontologie, n'hésitent cependant pas à tomber dans cette forme d'«'illégalité économique[2] ».

1. L'intelligence économique et les différents types de veille

L'intelligence économique et la veille technologique sont des systèmes de gestion stratégique de l'information. Ce sont des méthodes légales, même si nous verrons par la suite que les frontières sont assez floues. Ces pratiques peuvent parfois déboucher sur l'espionnage industriel.

Après avoir défini les champs d'application de chaque concept, nous ferons une rapide description des systèmes en place dans les principaux pays industrialisés. L'organisation de l'intelligence économique dans les économies nationales varie selon les spécificités culturelles du pays.

---

[1] *business intelligence*

[2] le terme illégalité économique regroupe l'ensemble des pratiques d'espionnage industriel, de contrefaçon, de corruption ; le marché de la drogue ; les économies mafieuses... Christian HARBULOT. « La concurrence par l'illégalité économique ». *La machine de guerre économique.* p135.

A – Définitions

L'intelligence économique peut être définie « comme l'ensemble des actions de recherche, de traitement et de diffusion, en vue de son exploitation, de l'information utile aux acteurs économiques[3] ».

L'intelligence économique met en œuvre une intention stratégique et tactique ainsi qu'une interaction entre tous les niveaux de l'activité : depuis la base (internes à l'entreprise) en passant par les niveaux intermédiaires (interprofessionnels locaux) jusqu'aux niveaux nationaux (stratégies concertées entre les différents centres de décision), transnationaux (groupes multinationaux) ou internationaux (stratégie d'influence des Etats-nations).

Englobant toutes les opérations de surveillance de l'environnement concurrentiel, ce système vise à instituer une gestion stratégique de l'information. C'est une véritable culture, un mode d'action.

Le concept d'intelligence économique intègre trois particularités :

- un champ d'application limité aux informations « ouvertes » acquises dans le respect d'une déontologie
- des acteurs représentés par l'ensemble du personnel alors impliqué dans un processus de culture collective de l'information
- une spécificité culturelle dans la mesure où chaque économie nationale génère un modèle d'intelligence économique qui lui est propre.

L'intelligence économique regroupe toutes les activités de renseignement et de veille au sein d'une nation et les organise pour en assurer la diffusion et l'exploitation. Elle rassemble sous sa dénomination les deux types de recherche d'informations : passif (veille), et actif (renseignement, reconnaissance…) dans toutes les activités de l'entreprise, comme le montre le schéma ci-après.

Figure 1: L'intelligence économique

ACTIF	Renseignement Technologique	Renseignement Marketing	Renseignement Financier	Renseignement Production	Renseignement Ventes
PASSIF	Veille Technologique	Veille Marketing	Veille Financier	Veille Production	Veille Ventes
	Recherche et Développement	Marketing	Financier	Production	Ventes

La veille stratégique d'une entreprise correspond à l'effort que celle-ci accomplit pour être à l'écoute de son environnement industriel. En réalité, la veille se contente de gérer et de diffuser des « signaux » d'une situation donnée, représentant les menaces ou opportunités pour l'entreprise. La veille stratégique regroupe l'ensemble des différents types de veille : technologique, marketing, financière, production, commerciale[4].

Chronologiquement, la première est la veille technologique, souvent confondue avec l'espionnage industriel. Sa mission est d'alerter les responsables de l'entreprise, suffisamment tôt, sur toute innovation scientifique ou technique susceptible de modifier le paysage économique.

La pratique de la veille technologique dans les entreprises représente un des sous-systèmes les plus connus de l'intelligence économique. L'intelligence économique vise à la coordination et au déploiement concerté de tous les sous-systèmes nationaux. La coopération de tous ces sous-systèmes permettra une amélioration des performances nationales.

B – Les différents systèmes d'intelligence économique

La protection ou le maintien de la compétitivité économique constitue de plus en plus une ardente préoccupation pour de nombreux gouvernants. Chaque État s'efforce

---

[3] selon la définition donnée par Henri Martre. COMMISSARIAT GENERAL AU PLAN. *Intelligence économique et stratégie des entreprises*. op. cit. p 16.

[4] Ce découpage correspond à l'école prospective française. L'approche américaine développée par Michael Porter distingue 4 types de veille : concurrentielle, commerciale, technologique et environnementale.
P. Antoine – « Un nouveau métier pour les hommes de marketing : la veille prospective et ses applications stratégiques ». *Revue Française du Marketing*, n°139, 1992/4.

donc de jouer un rôle essentiel dans la définition des grandes orientations stratégiques indispensables à ses entreprises. L'analyse comparée de l'intelligence économique dans les économies les plus compétitives fait apparaître que la coopération État/entreprises ou collectivités locales /entreprises est en voie de consolidation dans tous les pays.

Les pratiques d'intelligence économique trouvent leurs racines dans l'histoire et la culture du pays. Aussi la construction d'un tel système se heurte à deux fossés culturels qu'il s'agit de combler : le passage d'une culture fermée à une culture ouverte de l'information et le passage d'une culture individuelle à une culture collective de l'information.

a) Comme nous l'avons vu précédemment, le Japon est le pays de référence en matière de veille technologique. La recherche d'information est fondée sur une dynamique collective. La stratégie japonaise repose sur un trio État, entreprises, citoyens. Il existe ainsi deux formes de « partenariats » de l'information :

- *Partenariat citoyen-entreprise*. Chaque membre du personnel se doit de participer à cette dynamique de l'information dans l'accomplissement de son travail quotidien.

- *Partenariat État-entreprise*. Le traitement de l'information collectée va permettre de construire des stratégies concertées entre administrations et entreprises. Il existe une très forte intégration entre des organismes étatiques comme le MITI ou le JETRO[5] et les entreprises. L'administration japonaise consacre aujourd'hui 10 à 12 milliards de francs par an à la recherche d'informations, qu'elle redistribuera ensuite aux industries.

La circulation de l'information est ainsi facilitée au sein du système japonais ; en Occident, au contraire, l'information est souvent victime d'une rétention au sommet de la hiérarchie.

b) Les États-Unis disposent d'un véritable arsenal dans le domaine de l'intelligence économique ; toutefois, sa caractéristique est d'être dispersé et de ne fonctionner que rarement au niveau national. La logique du système est individuelle et le marché américain

[5] Ministère de l'Industrie et du Commerce International (MITI) – Japan External Trade Organization (JETRO)

de l'information profite plus aux entreprises elles-mêmes qu'à l'économie dans son ensemble.

Cependant, le Président Clinton a créé, en juillet 1995, un Comité national économique pour mobiliser l'ensemble de l'administration, le FBI et la CIA et développer le renseignement économique. Sa mission repose sur la consultation systématique des revues spécialisées étrangères et des banques de données, la veille technologique, la centralisation et la circulation du renseignement.

c) Le modèle allemand est l'un des plus performants au monde. Il s'appuie sur un profond sentiment collectif de « patriotisme économique ». Contrairement au système américain, le mérite du système allemand est d'avoir un centre vers lequel converge l'ensemble des flux d'informations. Il s'est en effet construit autour des principaux centres de décision : banques, entreprises, État…

De plus, les techniciens expatriés se sont révélés d'excellents informateurs pour les sociétés allemandes. L'administration allemande et les entreprises se sont dotées d'un système de collecte des données informatisées très performant. Les 3400 publications professionnelles et les 60 millions d'exemplaires de diffusion constituent dans le domaine de l'ingénierie de l'information un atout majeur.

d) La culture française, quant à elle, reste héritière d'une certaine méfiance vis-à-vis de la veille, qui constitue un frein à la diffusion de l'information. Les entreprises françaises sont en retard et leurs services de veille stratégique sont relativement récents. En 1992, elles ne dépensaient que 0,2% de leur CA à la veille.

La France ne représente à l'échelle mondiale que 4% de la production d'informations tous secteurs confondus. Selon l'expression de Christian Harbulot, il existe dans ce domaine un « no man's land français[6] ». La faiblesse de la France réside dans l'absence de coordination entre les différentes administrations, contrairement au système japonais. De plus, les grandes entreprises françaises qui tentent d'initier leur personnel à une culture collective de l'information sont rares. Quatre-vingts pour cent des structures industrielles ne possèdent même pas de service consacré à l'information.

Tout reste encore à faire en France : l'intelligence économique n'est qu'un chantier en construction. La prise de conscience du problème est apparue récemment parmi les

[6] Christian HARBULOT. *La machine de guerre économique*. op. cit. p.115.

professionnels qui tentent désormais de s'organiser. Le 4 avril 1995, le gouvernement Balladur a créé un Comité National pour la compétitivité et la sécurité économique qui a pour but d'offrir aux entreprises les avantages d'un système centralisé et national de récolte d'informations.

2. L'espionnage industriel

L'espionnage industriel est une pratique qui prête à confusion avec les systèmes de veille et d'intelligence économique. Nous verrons à quel point tenter de délimiter trop strictement ce concept peut s'avérer dangereux ; construire une définition trop stricte reviendrait à nier un grand nombre de réalités de l'espionnage industriel. Espionner ses concurrents représente la démarche aboutie de la recherche d'information. Ces pratiques sont de plus en plus répandues aujourd'hui et sont la source de nombreux préjudices économiques.

Nous pouvons d'ores et déjà faire quelques précisions de vocabulaire. Dans les développements qui vont suivre, nous utiliserons le terme d'espionnage industriel, bien que de nombreux organismes et auteurs lui préfèrent les expressions « espionnage économique », « espionnage d'affaires », ou « violation de secret d'entreprise[7] ». Il est évident que l'intérêt des espions ne se limite pas aux seuls secrets industriels. Toutes les autres activités de l'entreprise sont également des cibles d'espionnage. Nous conserverons, toutefois, l'expression « espionnage industriel » par commodité d'usage, même si celle-ci ne restitue pas le phénomène dans sa globalité.

A – Une définition délicate

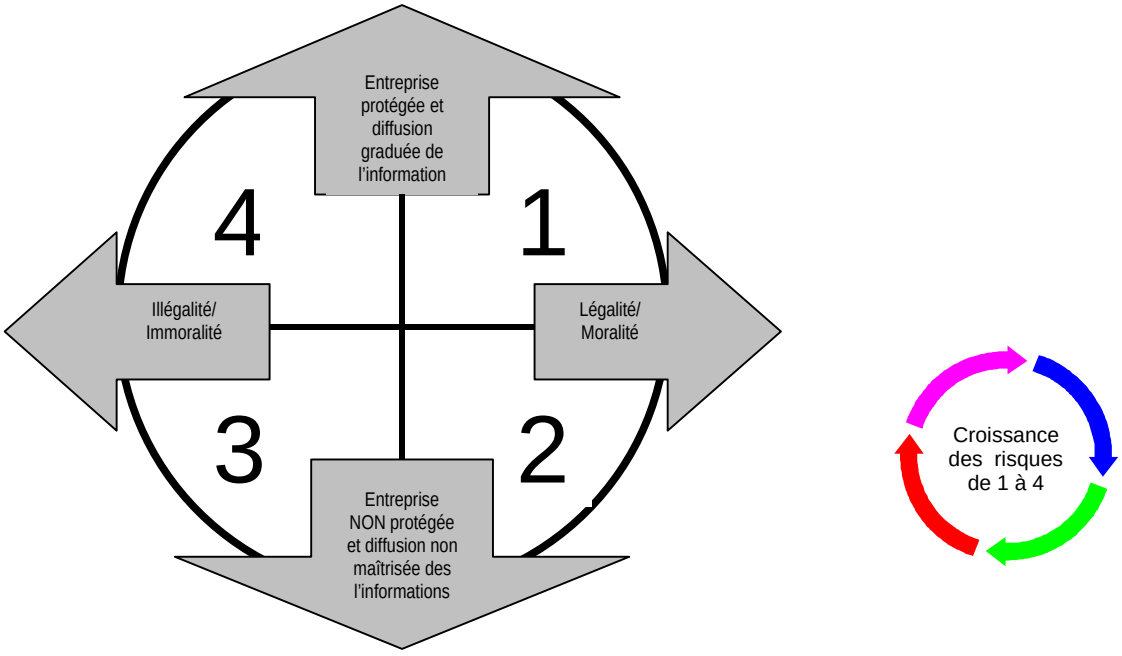
Proposer une définition de l'espionnage industriel nécessite une démarche prudente. Nous pouvons tenter, dans un premier temps, une délimitation stricte qui est souvent celle avancée par les défenseurs de l'intelligence économique. Cependant, cette définition ne permet pas une vision globale du problème. En réalité, les limites entre les concepts de veille technologique, intelligence économique, et espionnage industriel sont souvent floues ; les tentations sont grandes de transgresser les règles d'éthique.

L'espionnage industriel est souvent décrit comme un dérivé malsain de la veille technologique, le « cancer » de l'intelligence économique. Il s'agit de l'ensemble des

pratiques à travers lesquelles les informations sont obtenues par des moyens répréhensibles (corruption, piratage, vols de documents…). Cette pratique se trouve très proche des méthodes de renseignement militaire et sort des limites de la morale et de la légalité.

La figure 2, ci-dessous, se propose de bâtir une distinction entre intelligence économique et espionnage industriel autour de deux axes : l'axe légalité-moralité / illégalité-immoralité et l'axe entreprise protégée / entreprise non protégée.

Figure 2 : Veille et espionnage : les limites



Le cadran 1 représente la *veille "classique" active*, c'est-à-dire la veille dans le cadre de la légalité et l'entreprise visée par le veilleur est protégée des attaques extérieures.

Le cadran 2 représente les cas où *le veilleur repère les failles de l'entreprise cible*. La veille est effectuée dans un cadre légal et moral, mais l'entreprise visée par le veilleur n'est pas protégée. Le veilleur risque d'être tenté de passer au cadran 3

Dans le cadran 3, *le veilleur exploite toutes les failles de la cible*. Les moyens employés se dirigent vers des actions illégales et immorales.

[7] expression utilisée par la Ligue Internationale Contre la Concurrence Déloyale (LICCD), considérant l'expression espionnage industriel comme péjorative et limitative.

Enfin, dans le cadran 4, *le veilleur fait de l'espionnage au sens strict*. L'entreprise visée par le veilleur n'est pas protégée et le veilleur est définitivement tombé dans l'illégalité / immoralité.

La veille technologique constitue un terrain juridique accidenté et il est souvent difficile de déterminer où finit la veille et où commence l'espionnage industriel.

La délimitation de l'espionnage industriel aux seuls actes illégaux pose déjà un certain nombre de problèmes. En effet, les procédés utilisés sont très divers et tous ne peuvent pas tomber sous le coup de la loi : écouter une conversation ou engager un ancien employé d'un concurrent n'est pas répréhensible.

La moralité et la déontologie constituent un second point de délimitation entre veille et espionnage industriel. Cependant, il ne faut pas croire que les chefs d'entreprise respectent toujours les principes éthiques fondamentaux. Et cela, pour deux raisons principales :

- c'est parfois une solution de facilité de transgresser la déontologie ; dans tout système, il existe des gens qui en toute bonne foi ne connaissent pas les codes de déontologie,
- d'un pays à l'autre, les lois et la déontologie peuvent varier ; il existe des différences légales mais aussi culturelles d'un pays à l'autre : les pratiques de pots de vin pour acheter des informations sont interdites dans les pays occidentaux, mais tolérées, voire obligatoire dans les pays orientaux

Figure 3 : Les zones grises de la recherche d'informations

Source : B. Martinet, Y-M. Marti. L'intelligence économique. Paris : les Editions d'Organisation, 1995. p137

LA FIN *(INFORMATION RECHERCHEE)*		ouverts	organisés et déontologiques	illégaux
	information noire (fermée, secrète)	interdit	interdit	espionnage (au sens strict)
	information grise (semi-ouverte)	intelligence économique	intelligence économique	bêtise dangereuse
	information blanche (ouverte)	intelligence économique	bêtise dangereuse	bêtise dangereuse

LES MOYENS UTILISES

Plus le veilleur progressera dans son étude de l'entreprise concurrente, plus les informations recherchées se feront fines et stratégiques, et plus il sera tenté d'utiliser des pratiques douteuses, proches de l'espionnage industriel. La figure 3 précédente définit l'existence de « zones grises ».

Il est alors impossible de proposer une approche réaliste des phénomènes d'espionnage sans prendre en compte l'ensemble des « zones grises » qui gravitent autour de l'espionnage industriel au sens strict.

Dans les systèmes d'intelligence économique, même si ceux-ci reposent au départ sur une éthique précise, l'espionnage apparaît comme un moyen de rechercher chez ses concurrents une information déterminante pour l'économie nationale. Souvent, il existe des liens très forts entre les organismes chargés de l'intelligence économique et les services secrets officiels, quand ceux-ci ne sont pas confondus (c'est le cas du JETRO dont la vocation est aussi bien la veille légale que l'espionnage illégal).

L'espionnage industriel s'intègre dans une démarche progressive. La recherche d'informations débute par la mise en place d'un système de veille (zone blanche), puis dérive progressivement vers l'espionnage industriel. Dans la seconde partie de notre étude, nous verrons à quel point il est difficile de délimiter les différents niveaux de gravité des pratiques « douteuses ».

En résumé, il est impossible de fixer strictement une limite juridique ou déontologique à l'espionnage industriel. L'espionnage est un bon complément de la veille, c'est pourquoi les entreprises n'hésitent plus à y avoir recours.

B – Le choix de l'espionnage industriel

Face à la situation de perpétuelle concurrence au niveau mondial, de mondialisation des échanges, c'est-à-dire de guerre économique, l'information a acquis une valeur croissante. L'intérêt est grand et d'une rentabilité certaine d'aller dérober les avantages d'autres entreprises par le biais de l'espionnage. Dans un monde dominé par la technologie, les secrets commerciaux, formule, conception, plan de marketing sont la nouvelle monnaie d'échange sur le marché.

La veille, quant à elle, semble souffrir de certaines insuffisances face aux attentes de plus en plus précises des chefs d'entreprises. Si l'information « ouverte », c'est-à-dire accessible à tous, représente effectivement 90% de l'information disponible sur un sujet donné, et bien que nécessaire, elle conserve un caractère essentiellement descriptif. Ce sont souvent les 10% restants qui seraient vitaux pour aboutir à une bonne compréhension de la stratégie du concurrent. Or, ceux-ci ne peuvent provenir que de sources « grises », comme l'espionnage industriel.

De plus, l'information publiée peut être manipulée, comme nous l'avons étudié précédemment. Les systèmes de veille ne sont pas imperméables à la désinformation. En cas de doute, l'espionnage industriel est une méthode efficace pour obtenir une information de bonne qualité et non détournée, puisqu'elle est récupérée au sein de l'entreprise elle-même.

La motivation première des agents économiques qui s'adonnent à l'espionnage est d'abord le gain de temps et surtout d'argent que cette pratique procure. Dans la nouvelle donne économique mondiale, il faut aller le plus vite possible et ceci aux moindres frais.

Or, la recherche et le développement, de plus en plus sollicités face à la forte demande d'innovations, est un processus très lent, dont les coûts se sont multipliés ces dernières années. Quand on sait qu'il faut, en moyenne, douze ans de travail et 231 millions de dollars aujourd'hui pour mettre un nouveau médicament sur le marché américain, on comprend que les milieux pharmaceutiques soient les proies d'un espionnage intensif. Ainsi, le renseignement, obtenu par des moyens illégaux, peut faire épargner des années et des millions de francs à des firmes, si elles devaient acquérir certains secrets par des voies légales.

Opter pour l'espionnage est, de plus, facilité par l'accessibilité des moyens et techniques. Mettre en place un système de veille nécessite un investissement long et coûteux. L'entreprise doit se créer un fonds documentaire, embaucher du personnel… Faire appel à des cabinets de conseil spécialisés en veille coûte en moyenne entre 20000 et 40000 francs par mois. Nombreuses sont donc les entreprises qui préfèrent utiliser directement des techniques d'espionnage.

Contrairement à la veille, c'est parce qu'il est de plus en plus facile de se doter des techniques, que l'espionnage gagne du terrain dans les entreprises. Avec quelques milliers de dollars et un peu de savoir-faire, il est désormais possible de fabriquer un attirail électronique qui permet d'entendre une conversation, d'intercepter des appels, de savoir ce

qui se passe sur un ordinateur à 30m… Tous ces équipements ne sont plus réservés aux services officiels de renseignement ; les boutiques de gadgets électroniques ne cessent de fleurir sur le marché. Les nouvelles techniques de communication telles que le fax, le courrier électronique ont également facilité le vol de documents secrets.

Ben Venzke, auteur d'un rapport pour le gouvernement américain intitulé «Intelligence Watch Report », s'accorde à dire que la philosophie sous-jacente des Japonais est : « Pourquoi dépenser 10 ans de travail et un milliard de dollars en recherche et développement quand vous pouvez corrompre un ingénieur de l'entreprise concurrente pour un million de dollars et obtenir le même résultat, si ce n'est mieux ? ». Si on y met le prix, il devient très facile de trouver un employé prêt à trahir son entreprise, en jouant le rôle d'espion. Depuis la chute du bloc communiste, les arguments politiques ont cédé la place aux arguments financiers. Seul le Japon, grâce au lien très fort entre l'employé et son entreprise, ne subit que très peu d'attaques de ce genre.

CHAPITRE 2

L'ESPIONNAGE INDUSTRIEL OU L'ORGANISATION DU PILLAGE ÉCONOMIQUE

Si l'espionnage n'est pas une activité récente, il n'en demeure pas moins que l'espionnage industriel tout au moins s'est intensifié depuis la seconde guerre mondiale. Celui-ci fait aujourd'hui l'objet de nombreuses inquiétudes.

Le gouvernement américain présente chaque année au Congrès son rapport annuel sur l'espionnage industriel étranger orienté vers les technologies américaines dont le bilan semble à chaque fois plus accablant[1]. Le dernier en date précisait que, depuis l'initiation du programme économique de contre-espionnage[2], lancé en 1994, le FBI a pu observer une augmentation de 100% du nombre d'entreprises américaines victimes d'espionnage, passant de 400 à 800 cas. Les opérations d'espionnage industriel ne cessent de prendre de l'ampleur dans la mesure où les effectifs des professionnels de l'espionnage ne cessent de croître. Le même rapport recense ainsi 55 500 professionnels sur le sol américain, soit une augmentation de 50% depuis 1980.

En France, le constat est le même. En 1994, la Direction de Surveillance du Territoire (DST) a organisé 700 séances de sensibilisation à l'espionnage industriel auprès des entreprises, contre la moitié dix ans plus tôt. Face à ce nouveau danger, les entreprises se sont transformées en véritables *bunkers* : le secteur de la télésurveillance a progressé de 60% entre 1990 et 1993, et dans le même temps, la demande de vigiles s'est accrue de près de 40%. Cette réponse offensive à l'espionnage industriel ne s'est pas révélée efficace pour autant.

En Allemagne, Klaus Dieter Matschke, PDG de l'entreprise KDM implantée à Francfort et spécialiste du conseil en sécurité, affirme que l' « on assiste à une véritable explosion ». Selon ses dires, le marché de l'espionnage serait extrêmement bien organisé et la menace ne viendrait plus seulement de l'Europe de l'Est, mais de l'ensemble des grandes puissances occidentales.

Dès 1962, Business Week mentionnait « l'existence d'un marché international, dûment organisé, où se négocient les secrets industriels volés ». Actuellement, les deux plaques tournantes du renseignement seraient Genève et Tokyo. Dans ces deux centres, les

[1] CONGRESS OF THE U.S.A.. Foreign Economic Collection and Industrial Espionage. *Annual Report to Congress* 1996 (http://www.infowar.com)
[2] FBI's Economic Counterintelligence Program 1994

secrets industriels se négocient pour les entreprises du monde entier. Dans plusieurs cas, les sociétés victimes de vols y ont racheté, au prix fort, les renseignements qu'on leur avait dérobés.

Dissimulé dans l'ombre mais redoutablement organisé, l'espionnage industriel à l'échelle mondiale repose sur une structure particulière. Les flux d'informations pillées se croisent selon une organisation complexe où il n'est plus possible de distinguer les espions de leurs victimes. Services secrets officiels et multinationales sont les acteurs de cette guerre de l'ombre qui n'épargne plus aucun domaine de l'activité économique. Désormais, les pays industriels, autrefois alliés, s'espionnent mutuellement afin de faire profiter les entreprises nationales des secrets volés à l'étranger.

Pour atteindre l'information-clé, les missions d'espionnage industriel sont de plus en plus organisées. Les procédés utilisés se sont multipliés grâce à l'essor des nouvelles technologies. Des plus bénins aux plus sophistiqués, les délits d'espionnage industriel ont toujours des conséquences graves. Les quelques affaires qui ont fait l'actualité récemment alertent les entreprises sur la réalité de cette menace.

Toutefois, peu d'actes d'espionnage font l'objet de condamnations devant les tribunaux. Les législations nationales, bien que dénonçant ouvertement l'espionnage, présentent des vides juridiques. Malgré l'ampleur des préjudices subis beaucoup d'entreprises préfèrent encore la solution du compromis.

SECTION 1 : LA STRUCTURE DE L'ESPIONNAGE INDUSTRIEL MONDIAL

Lorsque les affrontements idéologiques divisaient encore l'économie mondiale, les espions agissaient entre deux blocs distincts. La menace était identifiée : l'Est s'attaquait à l'Ouest pour lui dérober ses secrets de défense nationale. Dans la guerre économique actuelle, l'organisation bipôlaire de l'espionnage industriel a volé en éclats. Les acteurs se sont multipliés, de nouveaux ennemis ont émergé et les services officiels ont été contraints de se reconvertir. La provenance des menaces ne peut plus être définie. Les secteurs visés ne peuvent plus être aussi clairement identifiés. L'espionnage industriel actuel repose donc sur une structure éclatée où la nature des acteurs et de leurs objectifs s'élargit continuellement.

1. Les acteurs

L'espionnage industriel peut être pratiqué :

- soit par les États et leurs services secrets de renseignement : c'est l'espionnage d'État ;
- soit par les entreprises elles-mêmes contre d'autres entreprises nationales ou étrangères : c'est l'espionnage privé.

A – L'espionnage public

L' espionnage public, également appelé *interne*, est au service des pouvoirs d'une nation ; il est initié par les services secrets nationaux et vise toutes les informations qui peuvent se révéler utiles à l'industrie et à l'économie nationale. C'est l'un des moyens utilisés par de nombreux pays pour améliorer ou conforter leur position politique, militaire, économique, scientifique ou technologique face à leurs adversaires.

Rares sont les gouvernements qui n'ont pas créé des services de renseignements. Les noms de certains de ces services sont particulièrement bien connus : le KGB soviétique, la CIA américaine, le MI 6 britannique, le Mossad israélien ou la DGSE française. Après la fin de la Guerre Froide, la plupart de ces services se sont reconvertis dans l'espionnage industriel ; ces organismes étatiques ont une puissance considérable en la matière. Philip Knightley, spécialiste et observateur du monde du renseignement, estime à 1,5 millions de

personnes les effectifs mondiaux de l'espionnage et du contre-espionnage, tous camps confondus, en 1988. Un budget annuel de l'ordre de 110 à 120 milliards de francs correspondrait à l'ensemble de ces activités.

Cependant, l'avis des différents services de renseignements nationaux diffère, quant à savoir quelle est la position à adopter en matière d'espionnage industriel. A ce sujet, nous pouvons présenter rapidement les différents objectifs des principaux services officiels de renseignement.

a) Pour les Américains, il est hors de question que la CIA ou la NSA[1] redistribuent les informations qu'elles recueillent. A qui faudrait-il remettre de telles informations ? Qui en définirait les axes de recherche ? Le gouvernement ne fausserait-il pas ainsi les lois du marché ? Cette position divise la communauté américaine de l'espionnage et limite les actions de la CIA à des missions politiques et militaires. Cependant, depuis peu, une structure de coordination qui réunit les dirigeants de 19 administrations gouvernementales a été constituée et agit comme « un cabinet de crise ». Ce dernier a pour but de jeter tout son poids dans la bataille dès lors qu'un groupe industriel cherche à enlever un marché[2].

b) Les espions britanniques, quant à eux, évoluent sous la surveillance de la CIA. Le MI 6 ne passe pas pour un champion en matière de renseignement économique.

c) Le JETRO japonais a, lui, fixé sa priorité à la collecte et la compilation d'informations industrielles. Ses 80 bureaux dans le monde sont coordonnés de façon exemplaire. Les renseignements réunis sont directement traités par les 15 000 employés travaillant au MITI, afin d'être redistribués aux entreprises nationales. Le JETRO apparaît, au milieu de tous les services officiels, comme le géant du renseignement industriel et scientifique.

d) La France dispose de deux services : la Direction de Surveillance du Territoire (DST), qui opère à l'intérieur des frontières, et la Direction Générale des Services Extérieurs (DGSE), à l'extérieur. En matière d'espionnage industriel, les renseignements français sont encore handicapés par une culture trop militaire ; de plus, DST et DGSE ont du mal à collaborer. L'absence de coordination des administrations est spécifiquement française. Cependant, les services français sont relativement efficaces en matière de contre-espionnage ; la DST a d'ailleurs multiplié les campagnes de sensibilisation et mis en œuvre

[1] National Security Agency
[2] J. ISNARD. « La France cherche à mieux lutter contre les formes modernes de l'espionnage », *Le Monde* 1er mars 1995 , p8.

d'importants moyens pour lutter contre le vol des technologies françaises. Le gouvernement français considère comme parfaitement normal de jouer le rôle de prestataire de services au profit des firmes, et ne s'embarrasse pas de principes quand il s'agit d'aller espionner chez ses alliés.

e) Le service d'espionnage allemand, le BND[3] est considéré comme l'un des plus efficaces au monde, après le Japon, en matière de renseignement économique. Il aide également les entreprises nationales, et ceci avec le soutien du Chancelier Kohl. Ses résultats sont excellents depuis la chute du Mur de Berlin, car les anciens espions de la Stasi[4] est-allemande ont apporté leurs connaissances en matière de pillage industriel.

f) Malgré l'éclatement du KGB, les services officiels russes, désormais représentés par le SVR[5] semblent bien décidés à reprendre leurs anciennes activités. Le KGB est resté longtemps un leader en matière de renseignement économique. Aujourd'hui, Boris Eltsine lui-même appelle la Russie à rattraper son retard économique en allant puiser les technologies à l'étranger par tous les moyens ; et le directeur du SVR, Evgueri Primakov, a récemment déclaré : « le renseignement de nature scientifico-technique et économique ira en s'élargissant parce qu'il est urgent de relayer, par le biais de l'espionnage industriel, un système de recherche peu performant, faute d'un financement suffisant ». Le SVR s'inscrit donc dans le droit-fil du KGB, mais c'est aujourd'hui l'argent et non plus l'adhésion idéologique au communisme qui est devenu le moteur des agents du SVR à l'étranger.

B – L'espionnage privé

Si le renseignement et l'espionnage étaient autrefois l'apanage exclusif des monarques et gouvernements, ils tiennent désormais une place importante dans le monde des affaires internationales, sous le nom d'espionnage privé ou encore e*xterne*. Selon Robert Redmond, consultant en matière de sécurité, « l'espionnage ou plutôt l'espionnage industriel dans le monde des affaires fait partie de la vie quotidienne des entreprises ».

Si les États-Unis se défendent de pratiquer l'espionnage industriel, ce n'est pas le cas de ses entreprises. Par nécessité et faute d'être aidées par leur gouvernement, les firmes américaines sont leaders du marché de l'espionnage privé.

---

[3] Bundesnachrichtendienst
[4] Staatssicherheitsdienst
[5] Smoujba Veriechny Razvietski – Service de renseignements extérieurs

Une entreprise qui désire espionner ses concurrents possède plusieurs solutions : elle peut engager d'anciens cadres de services secrets nationaux, mettre en place sa propre cellule de renseignement ou encore faire appel à des sociétés privées spécialisées.
Ces privés interviennent sur commande à des tarifs motivants.

De grosses sociétés, partout dans le monde, particulièrement en Occident et en Asie engagent désormais des agents expérimentés pour se procurer des renseignements sur leurs concurrents et sur les autres pays. Les multinationales du monde entier s'arrachent désormais d'anciens agents d'Europe de l'Est, réputés comme les meilleurs. Des sociétés comme Eastman Kodak, American Telephone & Telegraph, MCI Communication, Xerox, McDonnel Douglas, Ford…ont toutes engagé d'anciens agents spéciaux au cours des dernières années. De plus, un nombre grandissant de firmes américaines se sont dotées de véritables organes de renseignements. Celui de Motorola ressemble de manière frappante au Conseil National du Renseignement[6], mis en place aux États-Unis par la CIA.

L'essor de l'espionnage, au sein du monde des affaires, se caractérise par l'apparition d'un nombre croissant de sociétés privées qui rivalisent avec les services étatiques. Elles se sont multipliées sous des apparences diverses mais légales : sociétés de consultant, d'audit, cabinets de conseil en « sécurité et gestion de crises », agences de détectives ; cependant, les moyens qu'elles emploient pour se procurer des informations sont loin d'être conformes aux législations en vigueur. Aux États-Unis, nombre d'agents de la CIA ont créé leurs propres sociétés indépendantes telles que Open Source Solution, Strategic Forum, ou Kroll.

Les agents spécialisés dans le pillage du renseignement économique se sont donc considérablement multipliés, qu'ils soient commandités par les services étatiques ou bien par les sociétés privées. Dans le même temps, la nature des informations visées s'est, elle aussi, profondément modifiée. La gamme des secrets volés s'est largement étendue.

2. Les cibles

Il convient à présent de nous intéresser aux objectifs des espions, c'est-à-dire les informations-cibles. Quelles sont les renseignements les plus recherchés ? Quels sont les secteurs sensibles et les entreprises les visées ? Quels sont les pays placés dans la ligne de mire des espions ?

[6] National Intelligence Council

A – Les informations-cibles au sein de l'entreprise

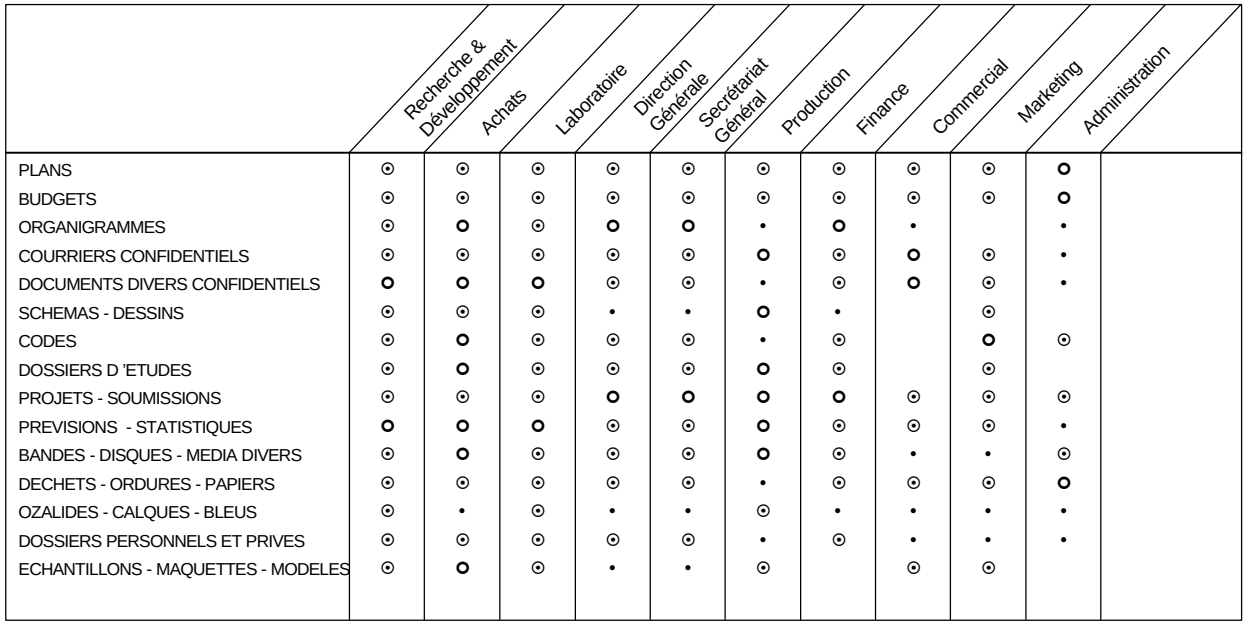
Dans les entreprises, les risques sont partout où il existe un profit. Ce sont, évidemment, les procédés, les techniques et les méthodes de production d'un nouveau produit qui font le plus l'objet de convoitises. Les échantillons sont dérobés afin d'être analysés puis copiés. Cependant, dans le domaine commercial, l'espionnage industriel fait de plus en plus de ravages. Prendre connaissance des stratégies de développement de ses concurrents (participations, fusions, acquisitions, joint-ventures) avant même qu'ils ne les mettent en œuvre permet souvent de gagner d'importants marchés. On ne compte plus chaque année le nombre de vols, de fuites, de détournements de ce qui constitue le cœur de la logistique commerciale de l'entreprise : le fichier.

Selon une étude réalisée en mai 1988 par l'Université de l'Illinois, à Chicago, intitulée « Etude sur le vol de secrets commerciaux dans les industries de haute technologie », les cibles les plus fréquentes des espions, dans les 150 entreprises américaines interrogées, étaient les informations et données concernant la recherche et la technologie (86%), bien plus convoitées que les fichiers de la clientèle (28,8%), les secrets d'ordres financiers (21,2%) et les projets de programmes (24,2%).

Le Cabinet Norbert Chatelet Consultants, spécialisé en conseil en sécurité, a établi la grille ci-dessous à l'intention de ses entreprises clientes. Les cibles de l'espionnage industriel à l'intérieur de l'entreprise sont répertoriées selon leur degré de confidentialité. Dans ce classement, les informations sont plus ou moins sensibles, selon leur nature et le service dont elles proviennent.

Recherche & Développement et Laboratoire sont les secteurs les plus visés, devant la Direction Générale, le Secrétariat Général, le service financier, viennent ensuite les secteurs marketing et commerciaux. Plans et budgets sont également très convoités tout comme les projets, soumissions et dossiers d'études. Cependant, les déchets, ordures et autres papiers ne sont pas non plus à négliger.

Figure 4: Les principales cibles d'espionnage économique dans les entreprises



	Recherche & Développement	Achats	Laboratoire	Direction Générale	Secrétariat Général	Production	Finance	Commercial	Marketing	Administration
PLANS	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	O
BUDGETS	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	⊙	O
ORGANIGRAMMES	⊙	O	⊙	O	O	•	O	•		•
COURRIERS CONFIDENTIELS	⊙	⊙	⊙	⊙	⊙	O	⊙	O	⊙	•
DOCUMENTS DIVERS CONFIDENTIELS	O	O	O	⊙	⊙	•	⊙	O	⊙	•
SCHEMAS - DESSINS	⊙	⊙	⊙	•	•	O	•		⊙	
CODES	⊙	O	⊙	⊙	⊙	•	⊙		O	⊙
DOSSIERS D 'ETUDES	⊙	O	⊙	⊙	⊙	O	⊙		⊙	
PROJETS - SOUMISSIONS	⊙	⊙	⊙	O	O	O	O	⊙	⊙	⊙
PREVISIONS - STATISTIQUES	O	O	O	⊙	⊙	O	⊙	⊙	⊙	•
BANDES - DISQUES - MEDIA DIVERS	⊙	O	⊙	⊙	⊙	O	⊙	•	•	⊙
DECHETS - ORDURES - PAPIERS	⊙	⊙	⊙	⊙	⊙	•	⊙	⊙	⊙	O
OZALIDES - CALQUES - BLEUS	⊙	•	⊙	•	•	⊙	•	•	•	•
DOSSIERS PERSONNELS ET PRIVES	⊙	⊙	⊙	⊙	⊙	•	⊙	•	•	•
ECHANTILLONS - MAQUETTES - MODELES	⊙	O	⊙	•	•	⊙		⊙	⊙	

⊙ Très confidentiel O Assez confidentiel ▪ Confidentiel

Source : Norbert Chatelet Consultants

B – Les entreprises-cibles

La chasse au renseignement se dirige en priorité vers les usines des grands groupes et les centres de recherche scientifique mais aussi vers les administrations. En réalité, aujourd'hui, ce n'est plus seulement l'industrie avec ses secrets de fabrication et son savoir-faire qui est visée, ce sont aussi les banques, les sociétés financières, la bourse, les agents de change…

Les cibles secondaires font l'objet de beaucoup d'inquiétudes : sous-traitants ou prestataires de service constituent des professions particulièrement travaillées par les chasseurs d'informations. Parmi ces nouvelles victimes se trouvent : les agences de publicité – où les campagnes pour les nouveaux produits se concoctent des mois à l'avance, les imprimeries – qui préparent toute la documentation technique et commerciale, les fabricants de moules et modèles, les maquettistes, photographes, consultants…

N'importe quelle entreprise peut être victime de telles exactions. Tous les domaines de l'économie sont désormais touchés. Classiquement, les secteurs les plus visés sont les secteurs de pointe dans lesquels la recherche fondamentale fait l'objet de gros investissements, et les secteurs de forte concurrence commerciale. La liste des secteurs sensibles de l'économie s'est, de plus, considérablement allongée. Il y avait l'armement, le nucléaire, l'espace, l'électronique ; maitenant les opérations d'espionnage industriel se multiplient dans la chimie, l'horlogerie, l'agro-alimentaire, la mécanique, le textile, le design, la mode…

C – Les pays et organisations-cibles

Tous les pays ne sont pas touchés de manière identique par l'espionnage industriel. Il y a dix ans, la DST faisait circuler des chiffres inquiétants : les Soviétiques laisseraient s'échapper à l'étranger 10% de leurs secrets ; les Américains 70%, et les Français 90%. La France est donc l'un des pays les plus pillés ; ses laboratoires et entreprises se vident de leurs secrets industriels ; cependant, de nombreuses brèches ont déjà été rebouchées grâce à une prise de conscience accrue des entreprises.

Les États-Unis par leur puissance technologique et commerciale, sont une cible privilégiée pour tous les services de renseignements de la planète. Peu méfiantes, les entreprises américaines sont plus faciles à pénétrer. Les États-Unis ne croient jamais qu'ils puissent être espionnés par des pays traditionnellement rangés dans le camp occidental

comme le Japon, la France ou Israël. La CIA a établi la « shopping list » des secrets de haute technologie convoités par l'intelligence française. Cette liste mentionne dans leur ordre de priorité pour les espions français : l'informatique, l'électronique, les télécommunications, l'aéronautique et l'armement, le nucléaire, la chimie, l'espace et les biens de consommation. Durant l'année 1996, les États-Unis recensent 12 pays impliqués dans des affaires d'espionnage à l'encontre d'entreprises américaines[7] ; 26 pays supplémentaires sont suspectés et font l'objet d'investigations. Le Canada, l'Australie recensent également chaque année un nombre important d'actes d'espionnage industriel.

Les milieux d'affaires allemands sont, eux aussi, de plus en plus inquiets devant la fuite de leurs secrets. Beaucoup de chefs d'entreprise ont déjà tiré la sonnette d'alarme auprès du gouvernement et sont allés jusqu'à qualifier le marché allemand de « véritable supermarché en libre-service ». En Allemagne, parmi les cibles privilégiées des espions, se trouvent, en premier lieu, l'industrie chimique et pharmaceutique, la branche aéronautique et spatiale, les constructeurs automobiles et l'électronique.

En dehors des entreprises, les administrations et organisations font également partie des priorités des espions. Le FBI, dans son rapport annuel au Congrès sur l'espionnage industriel, détaille les informations provenant de ces organisations qui suscitent le plus d'intérêt chez leurs voisins : les accords économiques, commerciaux et financiers ; les politiques énergétiques ; les plans de marketing ; la politique monétaire et fiscale… Ces renseignements permettent de connaître, à l'avance, les orientations de la politique américaine, des négociations et propositions en vue de donner au pays espion un avantage dans les négociations bilatérales ou internationales.

[7] Contre 10 en 1995 : Annual Report to Congress

Section 2 : Moyens et procédés de l'espionnage industriel

Que ce soit en Asie ou en Occident, les actes délictueux d'espionnage sont en train de devenir un excellent raccourci pour l' emporter sur la concurrence. Les méthodes utilisées pour rassembler les renseignements économiques sont à la fois légales, illégales, traditionnelles et de plus en plus novatrices. Nous n'avons pas l'ambition de faire une liste exhaustive de toutes les méthodes employées ; elles sont trop nombreuses, d'autant plus que le domaine évolue constamment.

1. Les sources de fuite des renseignements

Nous avons déjà vu à quel point il est difficile d'effectuer un classement selon le degré d'illégalité ou d'immoralité des pratiques. Nous ne pourrons donc retenir ces critères pour présenter l'espionnage industriel et les « zones grises » qui l'entourent. Nous préférerons nous en tenir à une classification selon le degré de confidentialité de l'information et donc le niveau d'intrusion au sein de l'entreprise.

La démarche des espions est progressive :

- dans un premier temps, les agents de renseignement s'attaquent aux informations disponibles et ouvertes. Ces méthodes s'apparentent encore à la veille, mais se révèlent parfois offensives ;
- dans un second temps, les espions vont chercher à provoquer la sortie d'information en dehors de l'entreprise. Ces méthodes ne tombent pas toutes sous le coup de la loi mais transgressent la plupart du temps les principes de la déontologie ;
- enfin, pour obtenir une information encore plus précise, il peut s'avérer nécessaire de pénétrer dans plusieurs services fermés de l'entreprise. Pour cela, les espions ont souvent recours à des moyens illégaux comme le piratage informatique, les écoutes téléphoniques, la corruption du personnel interne…Ces intrusions peuvent également se faire ouvertement par l'intermédiaire de collaborateurs de recherche ou autres stagiaires.

A – Collecter l'information depuis l'extérieur de l'entreprise

a) Les bases de données recensant les brevets, les marques, les normes, la presse spécialisée, les rapports d'experts ou les réseaux comme le World Wide Web constituent les sources d'informations les plus évidentes. Consulter ces systèmes d'informations permet d'identifier et de cibler les renseignements. Le suivi des brevets est une activité très

instructive et permet notamment de connaître les domaines de recherches de l'entreprise concurrente et leur progression.

Une seule personne, armée d'un micro-ordinateur, suffit pour trier le contenu des serveurs grand public d'Internet[1] et les forums virtuels où dialoguent les universitaires. Au total, cela représente 400 gigo-octets d'informations gratuites, 5000 bases de données sont accessibles on line, des millions de pages de textes de thèses, de mémoires sur tous les sujets imaginables, de publications scientifiques dans tous les domaines connus et émanant de tous les centres de recherche du monde.

Le moins que l'on puisse dire, c'est qu'Internet a révolutionné les outils de veille technologique et d'espionnage industriel. Les centres de documentation sont accessibles depuis l'ordinateur et parmi les journaux de qualité en Europe et aux États-Unis, très rares sont ceux qui ne diffusent pas leurs articles on line. La CIA a tracé la voie en investissant massivement dans les systèmes de ce type. Son objectif est de traiter en un minimum de temps des quantités phénoménales de données brutes, afin d'en tirer les éléments sensibles. Le CEA (Commissariat à l'Énergie Atomique) a développé pour ses besoins propres le logiciel Spirit, capable de gérer des textes de plusieurs langues après une indexation automatique.

b) Les visites d'entreprise sont une pratique privilégiée par les espions Japonais. Les entreprises se montrent le plus souvent accueillantes envers les visiteurs. Ainsi, même si les Américains reconnaissent que ces intrusions représentent un risque significatif, dans la plupart des cas, ces visiteurs ne peuvent avoir accès à tous les services de l'entreprise.

Cependant, ces visiteurs qui prennent des photos, font des croquis ou ramassent sur le sol des poussières de matériaux composites appartiennent aussi à l'armée des agents du renseignement. Un scientifique très compétent peut se faire une idée précise des axes de recherches et de leur état d'avancement rien qu'en jetant un coup d'œil sur les équipements d'un laboratoire. Ces visites permettent de repérer les systèmes de management, l'aménagement des usines…Le risque est donc bien moins celui d'une expédition nocturne que celui d'une visite courtoise et ouverte.

c) Les salons, expositions, foires sont également un des lieux privilégiés des agents du renseignement. Ils y ramassent l'abondante documentation offerte sur les différents stands, photographient les matériels, produits et réalisations, obtiennent des

[1] J. Guisnel « Internet et l'espionnage économique ». Extraits de *Guerres dans le cyberspace*. Paris : La Découverte, 1995. (http://www.liberation.fr/arc_mult/guisnel/rens.html)

informations de la part du personnel et récupèrent des échantillons. Bien organisé, l'espion peut ainsi récupérer une masse d'informations qui, une fois analysée, pourra être utilisée afin de reproduire un procédé ou un produit. Les Japonais sont très friands de ce genre de manifestations. Si l'entreprise a négligé de déposer un brevet, il y a de fortes chances pour que le modèle soit déposé en premier par une entreprise japonaise. Quand, il y a quelques années, l'attaché commercial de la Corée du Sud est obligé de rendre les photos d'un camion-benne qu'il a prises au Salon du Jouet, quand l'attaché de l'air adjoint soviétique « fait son marché » sur le stand Thomson-CSF au Salon du Bourget et doit rendre à la sortie quatre équipements sensibles, quand une équipe de photographes japonais se voit confisquer des dizaines de rouleaux de pellicules à la sortie d'un salon professionnel de l'électronique, on comprend l'immense intérêt de ce type de manifestations pour le développement du commerce et du renseignement.

C'est l'information ouverte, accessible à tous, qui va orienter les axes d'une recherche plus pointue vers des cibles précises : le service d'un laboratoire ou le département d'une entreprise. Ensuite, il s'agit de faire sortir les informations quand celles-ci ne sont pas accessibles depuis l'extérieur. Ces procédés permettent une approche plus fine de l'entreprise.

B – Provoquer la sortie des informations

L'une des méthodes les plus pratiquées aujourd'hui repose sur l'interrogation plus ou moins ouverte du personnel de l'entreprise. Souvent peu conscients des risques, les employés ont facilement tendance à donner des informations sur leur entreprise.

a) Les Américains se plaignent de l'abondance de ces requêtes non sollicitées. Elles reflètent souvent les intérêts des espions. Un nombre croissant d'incidents implique l'utilisation de fax, e-mail, ou de sondages téléphoniques. Les fausses études marketing provenant de cabinets inexistants sont abondamment utilisées. Ces études peuvent révéler des stratégies de développement et d'affiliation, des politiques de prix, les noms des directeurs techniques… Ces soi-disant cabinets d'études réclament ainsi des documentations techniques complètes aux chefs d'entreprise.

Des organismes scientifiques étrangers ont lancé, il y a quelque temps, dans certains laboratoires français une enquête par questionnaire postal sur les chercheurs, leur formation, leurs centres d'intérêts… Les questions d'apparence anodine suscitaient des

réponses forts indiscrètes sur les plans de charge et permettaient la constitution de fichiers personnalisés très précieux.

b) Certains n'hésitent pas à faire procéder à de faux entretiens de recrutement. En faisant miroiter des opportunités d'emplois alléchantes, le recruteur interroge allègrement le candidat non content de détailler ses actions dans l'entreprise. Sans embaucher personne, le recruteur connaît tout de la stratégie et des axes de recherche de ses concurrents .

c) En matière de renseignement, les oreilles sont partout. Les concurrents n'hésitent pas à placer des agents dans des lieux fréquentés par les employés de l'entreprise. Écouter une conversation entre deux chercheurs peut se révéler très instructif. De nombreux contrats ont été perdus par des bavardages dans le TGV, l'Airbus d'Air Inter ou le restaurant d'affaires.

d) L'embauche de salariés licenciés de l'entreprise concurrente est également pratiquée. L'employé apporte tout son savoir-faire, ses techniques acquises chez son ancien employeur mais également ses connaissances des dossiers en cours. Certains partent même en emportant avec eux des documents confidentiels. Cette pratique n'est pas illégale et fera grandement profiter l'entreprise d'embauche.

C – Pénétrer dans l'entreprise

Si ces moyens ne s'avèrent pas suffisants pour obtenir l'information, les espions n'hésitent pas alors à chercher à s'introduire dans l'entreprise.

a) Le risque d'une intrusion du système informatique de l'entreprise est devenu l'un des plus redoutables. Avec la multiplication des réseaux, souvent de simples lignes téléphoniques permettent des branchements enfantins. Internet, une fois de plus, est utilisé pour pénétrer dans les systèmes informatiques. Les services secrets officiels utilisent les talents de pirates capables de franchir les barrières protégeant des serveurs d'informations sensibles. Selon le FBI, 80% des connexions pirates sont faites par le biais d'Internet. Les « hackers », selon le terme anglais désigné pour pirate informatique, pénètre dans les ordinateurs pour y cacher des serveurs secrets dans lesquels ils placeront des logiciels spécialisés pour casser les protections.

Le piratage informatique est une forme très répandue d'espionnage industriel. La fraude informatique n'intéresse pas seulement les banques de données ou les fichiers industriels. Elle s'est progressivement étendue, depuis quelques années, à tous les domaines utilisant l'informatique. Les pertes auxquelles doivent aujourd'hui faire face les

banques pour des contrefaçons de cartes de crédit sont considérables. Les délits informatiques sont de nature diverses : piratage des logiciels, pénétration de réseaux protégés, sabotage de systèmes…Selon le FBI, seulement 1% des délits de ce type sont détectés.

Les dernières attaques d'envergure contre les ordinateurs français remontent à mars 95. Elles ont visé plusieurs centres serveurs comme ceux du Cnam, de l'ENST (Ecole Nationale Supérieure des Telecoms), de l'Institut Blaise Pascal, du laboratoire de l'Institut National de Physique Nucléaire… Cependant, la plus grande affaire mondiale en la matière touche aujourd'hui aux copies de logiciels. Les reproductions pirates de programmes sont légions sur le Web.

Les nouvelles technologies permettent sans cesse d'ouvrir des possibilités. Les interceptions de fax, messages électroniques sont devenues chose courante. Enfin, même s'ils reconnaissent que la menace n'est pas pour demain, certains industriels commencent à s'inquiéter sérieusement des satellites d'observation. Ceux-ci sont en mesure de fournir des photos précises du plan de construction d'une usine ou de prévoir, très à l'avance, la récolte de blé russe ou de café brésilien, permettant pour les concurrents de prendre des positions sur le marché à terme qui permettent de gagner à tous les coups.

b) De tout temps, l'espionnage a mis à profit les plus récents progrès technologiques pour acquérir et transmettre l'information. Depuis 15 à 20 ans, des systèmes électroniques miniaturisés très performants ont largement supplanté les moyens traditionnels, tels que les micro-caméras, micro-appareils photographiques ou encre sympathique. Désormais, les microphones peuvent être introduits dans une enceinte à l'aide de fusils propulseurs. Il n'est même plus utile de pénétrer dans le bâtiment pour en écouter les conversations internes. Ces outils électroniques sont aujourd'hui disponibles sur le marché. Hongkong, par exemple, est un véritable supermarché en matière de gadgets électroniques ; tous les systèmes d'écoutes à distances, matériels pour sur se brancher sur une ligne téléphonique, micro-caméras y sont en vente libre.

L'écoute est largement utilisée par les entreprises pour espionner leurs concurrents. En France, alors que l'affaire des écoutes administratives est au centre des débats, la commission de contrôle des écoutes, la CNCIS[2] a rendu le 17 avril 1997 son 5ème rapport[3]. La Commission recense 100 000 écoutes sauvages en France par an. La CNCIS s'est fixée pour mission de contrôler le matériel d'écoute, mais le rapport est sans équivoque : 4141 entreprises françaises (dont 553 pour la seule Provence-Côte d'Azur) ont pour activité

[2] Commission Nationale de Contrôle des Interceptions de Sécurité

principale déclarée « l'enquête et la sécurité » et emploient au minimum 45 000 personnes. Ces entreprises sont fortement soupçonnées de vendre du matériel d'écoute. Pourtant, 40 entreprises seulement ont obtenu l'autorisation de fabriquer ou commercialiser ce matériel d'écoute et deux d'entre elles font officiellement du renseignement et de la sécurité. De même, en 1996, le Premier Ministre n'aurait autorisé que 4600 écoutes dont 263 demandes (soit deux fois plus qu'en 1995) pour des motifs de sauvegarde économique (derrière le terrorisme, la criminalité organisée et la sécurité nationale).

c) Lorsqu'il s'agit d'infiltrer des agents chez l'adversaire, les sociétés de service sont des intermédiaires efficaces. Les employés chargés du gardiennage et nettoyage sont une couverture facile. Ceux-ci, selon les missions, déposent des micros ou caméras, copient des disquettes qui traînent sur des bureaux, ou plus simplement récupèrent les corbeilles à papier.

La corruption de salariés fait également recette. Devant l'attrait de l'argent, peu nombreux sont ceux qui refusent encore de trahir leur entreprise. Selon Michiano Kodama, président de l'Association des détectives japonais, « la corruption, le chantage et la séduction restent les meilleurs moyens d'obtenir des informations ». Ces trois pratiques ont prouvé leur efficacité pour faire parler les employés. Ensuite, la secrétaire est toute disposée à faire quelques photocopies supplémentaires, le responsable informatique à transmettre quelques fichiers et l'ingénieur à faire part des projets de recherche.

Les stagiaires présentent également une menace pour la sécurité de l'entreprise. La France accueille chaque année entre 60 000 et 100 000 stagiaires étrangers dans ses entreprises, ses laboratoires, ses centres de recherche. Certains chefs d'entreprise n'hésitent pas à utiliser l'expression de « péril jeune[4] ». La DST a établi que la majorité des stagiaires, surtout en provenance d'Asie et d'Europe de l'Est ont reçu une mission de renseignement.

d) Autre vulnérabilité nouvelle : le développement des accords de coopération entre firmes. Les entreprises sont amenées à travailler en coopération de plus en plus étroite avec beaucoup de partenaires industriels et à les associer aux phases d'études et de mise au point. Ces politiques d'accords de joint-ventures, recherches groupées, co-production et autres multiplient les risques de fuite. Les personnels des deux entreprises sont amenés à

[3] « Ecoutes sauvages sous surveillance ». F. Johannes, Libération, 18/04/97, p 11.
[4] Germain CHAMBOST. « Après la guerre froide, la guerre économique », *Science et Vie,* n°921, juin 1994. p 105.

travailler ensemble et donc à fournir un accès potentiel aux informations scientifiques et techniques. L'accès peut être intentionnel ou non, légal ou illégal.

Le rachat pur et simple ou la prise de contrôle de la cible pourrait constituer l'arme absolue pour obtenir des informations secrètes détenues par une entreprise ou un laboratoire. La multitude de PME qui font de la sous-traitance dans les secteurs de pointe sont des objectifs très vulnérables. En utilisant toute une série de sociétés-écrans, on peut s'assurer tous les pouvoirs chez les sous-traitants de Matra, de l'Aérospatiale, de Thomson et, sans être inquiétés, récupérer ainsi tous les secrets jusqu'alors les mieux gardés.

Pour obtenir une information vitale, les agents du renseignement ne reculent devant rien. Les dérapages sont plus ou moins graves, mais dans tous les cas l'entreprise victime doit faire face à des pertes toujours importantes.

2. Quelques affaires récentes

Les méthodes décrites précédemment peuvent parfois sembler extrêmes. Cependant, en quelques années, les affaires d'espionnage industriel ont fait de nombreuses fois l'actualité. Les trois exemples ci-après illustrent à quel point l'espionnage industriel peut prendre des formes diverses.

A – GM contre VW : la très bruyante affaire López

L'affaire d'espionnage industriel entre General Motors et Volkswagen aura duré 3 ans et demi ; elle s'est conclue en janvier 1997 par un compromis entre les deux parties.

En mars 1993, José Ignacio López de Arrirtùa quitte General Motors pour rejoindre le poste de directeur des achats et de la production chez Volkswagen. Dès la fin de l'année 1993, General Motors dépose une plainte contre Volkswagen pour « espionnage industriel » : le groupe allemand est accusé d'avoir débauché López et toute son équipe ; celui-ci ne se serait apparemment pas privé d'emporter des listes de prix concernant les pièces détachées et plans d'usine pour une future mini-voiture.

L'affaire fera grand bruit en Allemagne et aux États-Unis, car elle fera l'objet de nombreux rebondissements qui ne manqueront pas d'être repris par la presse et la télévision.

Après les accusations de General Motors allant jusqu'à employer le terme de « conspiration criminelle », Volkswagen dépose en mai 1996 une plainte contre General Motors pour « atteinte à l'image de Volkswagen ». Il faut préciser que suite aux déclarations de General Motors, le titre en bourse de Volkswagen a dû subir une chute de 3,5%.

Pendant ce temps, le Parquet de Darmstadt en Allemagne faisait saisir dans le bureau de López ou chez ses lieutenants des informations qui ressemblent à des documents confidentiels de chez General Motors, comme le projet de construction d'une usine en pays basque espagnol qui concorde avec une étude similaire menée par López chez General Motors depuis 1992. Au domicile d'un membre de l'entourage de López, une disquette avec des chiffres portant sur un programme de coût pour plusieurs modèles de General Motors.

Le scandale éclate quand la télévision publique allemande ARD révèle que des détectives privés engagés par General Motors auraient déposé ces fausses pièces à conviction chez Volkswagen, avant la saisie du Parquet.

En novembre 1996, López doit quitter le groupe allemand ; finalement, le 9 janvier 1997, les deux groupes automobiles arrivent à un compromis à l'amiable. Volkswagen retire les déclarations qui ont laissé croire que General Motors avait fabriqué de fausses preuves et reconnaît pour la première fois que « des activités illégales ont pu avoir lieu ». Volkswagen doit verser 100 millions de dollars à General Motors, s'engager à lui acheter sur 7 ans pour 1 million de dollars de pièces détachées, licencier deux autres collaborateurs de López embauchés avec lui et fournir des excuses publiques.

Si les firmes ont réglé leur différend sans attendre la décision finale de la justice, López, quant à lui, reste mis en examen par le Parquet de Darmstadt pour recel et divulgation de secrets industriels et commerciaux. Devant les tribunaux, les conséquences pour Volkswagen auraient été beaucoup plus graves. La justice américaine réclamait des peines lourdes allant jusqu'à l'emprisonnement de responsables administratifs du groupe allemand. Le procès aurait dans tous les cas coûté à Volkswagen des milliards de dollars en dommages et intérêts et causé un préjudice important pour la réputation et les ventes américaines du constructeur allemand.

B – Les pirates américains du Parlement Européen

Le 4 août 96, le Sunday Times révèle que des agents de la CIA ont piraté les ordinateurs du Parlement Européen et de la Commission Européenne.

Les secrets économiques et politiques dérobés visaient à conforter la position du gouvernement américain lors des négociations du GATT. Des documents confidentiels sur les accords de commerce, tarifs et quotas ont ainsi été visités, de même que des détails médicaux et financiers concernant des politiciens et chercheurs travaillant à Bruxelles. La brèche a été découverte lorsque les négociateurs européens ont réalisé que les Américains connaissaient en avance certaines des positions confidentielles de l'Union Européenne.

Le réseau informatique du Parlement Européen relie plus de 5000 fonctionnaires avec les quartiers généraux de la Commission Européenne à Bruxelles et le Conseil des Ministres. Les espions de la CIA ont exploité le fait qu'une partie du système informatique avait été fabriqué par des firmes américaines. Depuis, la Communauté Européenne a fait appel à des experts britanniques pour renforcer sa sécurité interne. Les investigations sur les espions américains suivent leurs cours.

Section 3 : Des espions non inquiétés

Personne ne peut aujourd'hui ignorer la réalité de l'espionnage industriel. Les conséquences en sont désastreuses pour les entreprises mais aussi pour l'économie du pays tout entier.

En Allemagne, les pertes dues aux opérations d'espionnage industriel sont estimées, selon une étude récente, à 5,31 milliards de dollars pour l'année 1995[1]. En France, la DST les évaluent à 10 milliards de francs par an[2]. D'autres experts quadruplent ce chiffre, car celui-ci ne fait pas état des activités des sociétés privées. Les pertes potentielles pour l'industrie américaine se montent à 63 milliards de dollars[3] pour 1995, tandis que le seul espionnage privé coûterait 18 milliards de dollars[4] par an au gouvernement australien.

Malgré ces chiffres accablants, il semble que l'espionnage reste encore dans l'ombre. Les gouvernements hésitent à dénoncer des actes d'espionnage sur le devant de la scène car ceux-ci touchent trop à la sécurité nationale,. Pour les entreprises, les conséquences, qu'elles soient commerciales ou financières, sont toujours très importantes et peuvent aller jusqu'à nuire à la survie de l'entreprise. Cependant, rares sont les entreprises qui osent aujourd'hui se lancer dans des poursuites judiciaires.

L'espionnage industriel est une arme silencieuse. Personne dans les milieux politiques ou économiques ne semble vraiment disposé à porter les espions en accusation. Entre firmes, les dénonciations existent, certes ; mais, pour une plainte déposée, combien d'entreprises auront préféré jeter l'éponge ? De plus, la plainte aura-t-elle une chance d'atteindre son but ?

1. La loi du silence

Dans la plupart des pays, les pouvoirs politiques ne semblent pas pleinement disposés à sanctionner l'espionnage industriel à hauteur des conséquences qu'il entraîne. Les gouvernements se heurtent en effet à l'obstacle majeur que représente le risque de

---

[1] D.Kennedy. « Top German Prosecutor Warns Firms about Espionage ». (http://www.infowar.com)
[2] J.Isnard. « La France cherche à mieux lutter contre les formes modernes de l'espionnage ». *Le Monde*, 1 mars 1995, p8.
[3] selon une étude réalisée par l'American Society for Industrial Security : Ben N. Venzke. « Economic/Industrial espionage ». (http://www.infowar.com)
[4] selon l'Australian Business Week du 5 août 1995 : « Economic and Industrial espionage : soup to nuts ». (http://www.infowar.com)

tensions diplomatiques. Les milieux d'affaires sont, eux aussi, très réticents. Faire éclater une affaire au grand jour implique d'en accepter les risques.

A – Les risques de tensions diplomatiques

Les milieux politiques hésitent à aborder le sujet car il est source de tensions diplomatiques. L'existence de l'espionnage entre «amis » que se livrent la France, Israël, l'Allemagne, le Japon et les États-Unis est désormais un fait connu de tous. Cependant, les dénonciations grand public de tels actes sont toujours restés des faits rarissimes. La coopération entre les différents pays est aujourd'hui si forte que peu osent prendre le risque d'enclencher des problèmes diplomatiques.

En février 1995, l'affaire de l'espionnage américain en France a fait grand bruit. Le gouvernement français souhaitait le départ du territoire français de 5 ressortissants américains, dont 4 bénéficiaient de l'immunité diplomatique, pour faits d'espionnage économique. Les affrontements diplomatiques furent de taille, d'autant plus que la France avait révélé cette affaire dans un contexte électoral aux États-Unis. Les deux parties tentèrent cependant rapidement d'éviter les surenchères diplomatiques. En fin de compte, le conflit fut traité à l'amiable ; les représentants américains gardèrent leur poste à Paris et ne furent pas inquiétés outre mesure. En effet, le moment d'une crise diplomatique était d'autant plus mal choisi que la coopération entre les deux pays était essentielle pour empêcher une reprise de la guerre en ex-Yougoslavie. D'autre part, Français et Américains étaient en passe de renégocier un pacte de sécurité transatlantique.

B – Les craintes dans le monde des affaires

Les milieux économiques, eux aussi, restent muets devant l'espionnage industriel. Beaucoup préfèrent garder le silence pour ne pas nuire à leur image ou par peur de devoir détailler les preuves. Si des affaires éclatent, la justice n'est utilisée qu'en dernier recours. Les sanctions imposées aux victimes couvrent rarement le préjudice subi par la victime.

Les entreprises sont rares à avouer avoir été victimes d'espionnage industriel. Cela revient, en effet, pour un chef d'entreprise à avouer ses faiblesses et donner ainsi prise aux critiques. Selon M. Matschke, spécialiste en conseil de sécurité en Allemagne, « aucune entreprise n'avouera jamais avoir commis des erreurs de management en matière de sécurité ».

De plus, lors du procès, l'entreprise victime se doit de fournir une preuve du vol et donc de dévoiler la nature des documents dérobés. L'information confidentielle devra donc être médiatisée devant le tribunal. C'est l'une des raisons les plus fréquemment avancée pour résoudre les victimes au silence. Ainsi Thomas Brunner de la Chambre de Commerce américaine affirme « c'est là une conséquence bien ironique de nos lois que dans le but de rendre justice, la victime d'espionnage industriel doive rendre publique l'information dont elle se plaint d'avoir été volé ».

2. Les vides juridiques

Une fois le délit d'espionnage établi, les tribunaux ne proposent pas encore des sanctions dissuasives. La législation dans ce domaine ne couvre pas suffisamment les victimes. Les barrières techniques s'opposent à des réformes juridiques explicites. Lorsque les actions aboutissent finalement devant la justice, la solution de règlement des différents la plus souvent adoptée est le compromis. Les sanctions pénales sont rarement appliquées.

A – Des réformes difficiles

Les pouvoirs politiques, bien qu'ils semblent prendre de plus en plus conscience de la nécessité de sanctionner l'espionnage industriel, ne semblent pas pour autant décidés à agir, d'autant plus qu'il existe de véritables difficultés à mettre en œuvre les lois.

En France, les textes qui encadrent la lutte contre l'espionnage ne sont plus adaptés depuis longtemps à la nouvelle donne de l'environnement international. Pour l'essentiel, ce sont un décret du 12 mai 1981 qui définit le niveau de protection du secret-défense et une série de circulaires qui a trait à la protection du patrimoine qui recouvrent les délits d'espionnage industriel. Cependant, ces textes sont aujourd'hui sans véritable rigueur juridique car ils ne prennent pas en compte les formes modernes de l'espionnage industriel. Le travail de réactualisation entamé par le gouvernement français se heurte à de nombreux problèmes pratiques.

La justice française réfléchit, en effet, à faire une distinction entre espionnage industriel et renseignement économique, et s'interroge notamment sur la possibilité d'encadrer les différentes « zones grises ». Les obstacles sont nombreux : comment contrôler les débauchages illicites sans entraver la liberté de mobilité du personnel dans les entreprises ? Comment dissuader un chercheur de diffuser sa découverte ? Peut-on limiter

les échanges scientifiques naturels d'une communauté nationale à une autre ? Autant de questions qui risquent de bloquer les réformes juridiques pendant un certain temps.

En Allemagne, les espions ne sont pas inquiétés non plus. Dans la législation allemande, l'espionnage industriel n'est encore considéré que comme un délit léger. L'espionnage de la concurrence, par exemple, ne relève pas des articles 93 et suivants du Code Pénal, concernant les délits de haute trahison, atteinte à la sécurité extérieure ainsi que l'espionnage mais de l'article 17 de la loi sanctionnant toute concurrence déloyale. Ainsi, au lieu de sévères peines de prison, les criminels n'encourent en principe qu'une amende.

Aux États-Unis, depuis une loi promulguée le 11 octobre 1996 par Bill Clinton, les dérapages risquent de coûter chers. L'espionnage industriel est devenu un crime fédéral passible d'une peine pouvant aller jusqu'à 15 ans de prison et 10 millions de dollars d'amende. Cependant, l'application d'une telle directive entre rarement en jeu : dans la plupart des cas, les espions trouvent le moyen de contourner la loi.

Les lois s'avèrent très insuffisantes dans le système américain pour couvrir les risques de vols et transferts de propriété illégaux en matière d'informations. Cependant, il faut reconnaître les efforts du gouvernement américain qui a introduit depuis peu l'l*ndustrial Espionage Act of 1996* qui, s'il est voté, constituera un point de départ conséquent dans la lutte pour l'espionnage.

B – Les inconvénients d'un procès

Ainsi, très souvent, les industries victimes d'un acte d'espionnage n'ont pas intérêt à parler et ne portent donc pas plainte. La plupart préfèrent un arrangement discret à l'option judiciaire, même assortie du huit clos.

Nombre des rares procédures engagées ne parviennent pas en audience publique et quand elles débouchent, elles finissent par un non-lieu, les preuves faisant défaut. Pour beaucoup d'autres affaires, les enquêteurs doivent se satisfaire de signaler dans leurs

procès verbaux l'existence de documents dits « sensibles » dont on leur a refusé la lecture et les procureurs ne sont pas habilités à connaître le secret-défense qui leur est généralement opposé.

En 1991, la Society for Industrial Security a effectué un sondage auprès de 170 de ses membres pour connaître parmi eux la proportion de victimes d'espionnage industriel. 165 entreprises seulement ont répondu à l'enquête et, parmi elles, 61 ont fait état d'incidents. Les sociétés américaines continuent souvent leur coopération avec des firmes étrangères qui ont commis des délits contre elles. Entamer un procès serait risquer de mettre fin à des accords souvent profitables aux deux firmes.

La justice ne peut contrecarrer un adage fort en vogue chez les « hommes de l'ombre », à savoir que « plus le temps passe, plus une affaire d'espionnage se dégonfle, plus on est d'accord pour la minimiser de part et d'autre et puis ça s'arrange ».

CHAPITRE 3

LA PROTECTION DU PATRIMOINE DE L'ENTREPRISE

Les entreprises se trouvent de plus en plus impliquées dans des problématiques de sécurité. Durant la précédente décennie, ce sont les aspects techniques et physiques de la sécurité d'entreprise qui se sont développés, avec comme corollaire la multiplication des sociétés privées (gardiennage, télésurveillance). Mais, aujourd'hui la place prise par l'information professionnelle dans l'économie mondiale montre que c'est la « sécurité informationnelle » de l'entreprise qui est en plein essor. L'entreprise se retrouve face à de nouvelles fonctions en matière de sécurité, d'autant plus qu'elle peut être directement source d'insécurité pour la collectivité toute entière.

Comme nous l'avons étudié dans le premier chapitre, la logique libérale et le processus d'intégration internationale ont développé une hyper-agressivité concurrentielle entre les entreprises. La fragilisation des situations relatives de chaque entreprise sur son marché et vis-à-vis de ses concurrents, jointe à l'accélération des processus économiques et des retournements de conjoncture, engendre une véritable insécurité dont les effets peuvent dépasser les seules limites du domaine économique. Lorsqu'une entreprise connaît un affaiblissement soudain de sa position de marché, cela peut affecter gravement le niveau d'emploi, la cohésion du tissu économique et social d'une région ou encore le maintien d'une filière économique importante au niveau national.

Le secteur privé se voit investi, chaque jour un peu plus, de nouvelles responsabilités ayant un impact sur la sécurité collective. La puissance publique est, en effet, incitée à se désaisir progressivement, au profit du privé, de certaines fonctions ayant un lien avec la sécurité du patrimoine. Cette tendance est particulièrement nette en ce qui concerne les grands services publics de réseaux, tels que les télécommunications, les transports ou l'énergie. Les impératifs de concurrence et de transparence des marchés nationaux amènent les États à réduire leurs activités sous monopole.

Cette mutation conduit à une société de privatisation des problèmes de sécurité : ces derniers deviennent pour toutes les entreprises « une obligation de service public ». L'entreprise devient acteur de la sécurité économique de l'entité nationale. L'État n'est plus seul en charge des missions de sécurité collective.

L’entreprise doit donc être consciente qu’elle a le devoir de protéger sa technologie, son savoir-faire, ses innovations, ses écrits, ses hommes, c'est-à-dire tout ce qui constitue sa richesse, son patrimoine intellectuel et industriel. Toute fuite d’informations relative à ce patrimoine peut être utilisée par la concurrence et se traduit par une perte d’activité ou de profit pour l’entreprise et par conséquent pour la nation.

Les difficultés en matière de sécurité sont nombreuses. L’entreprise doit savoir protéger l’ensemble des informations ; celles émises par l’entreprise elle-même et qui concernent les études, la mise au point de ce produit, de savoir-faire, les gammes de fabrication, de montage, de contrôle, l’élaboration des stratégies commerciales, financières, mais aussi celles acquises à l’extérieur et qui font également partie de sa richesse. Le problème est donc bien de maîtriser le flux d’informations sortant de l’entreprise et faire en sorte que seules les informations strictement indispensables aux relations avec l’extérieur sortent effectivement de l’entreprise, c'est-à-dire celles qui permettront aux agents commerciaux de vanter les qualités des produits, ou celles nécessaires lors des réunions avec les clients, fournisseurs ou sous-traitants.

Les chefs d’entreprises n’ont pas de difficulté à admettre que la protection du patrimoine de leur entreprise est à prendre en considération ; cependant, le problème se situe le plus souvent dans la manière de mettre en application les moyens de protection.

Les mesures globales de protection à prendre recouvrent plusieurs disciplines. La propriété intellectuelle met en œuvre des moyens de protection tels que les brevets, les marques. Cependant, ces instruments présentent certains inconvénients, et dans tous les cas ils s’avèrent insuffisants pour répondre à l’ensemble des besoins de sécurité de l’entreprise .

La protection industrielle concerne particulièrement la protection contre l’espionnage, qu’il soit privé ou d’État ; elle prend parfois le nom de contre-intelligence ou contre-espionnage privé. Dans ce domaine, vu le peu de recours juridiques, il s’agit davantage de changer les états d’esprit et les comportements de tout le personnel de l’entreprise que de vouloir faire de celle-ci un camp retranché. Un nombre minimal d’actions pensées avec logique peuvent s’avérer beaucoup plus efficaces.

Enfin, quand les mesures précédentes ont été épuisées, les professionnels de la sécurité recommandent des parades plus offensives : la dissimulation et l’intoxication. Ces alternatives sont aujourd'hui largement répandues mais ne sont pas toujours sans risques.

Section 1 : La propriété industrielle

L'appellation propriété industrielle est un sous-ensemble de la propriété intellectuelle qui comprend en plus la propriété littéraire et artistique avec les droits d'auteurs. C'est le Code de la Propriété Intellectuelle (CPI) qui fournit aux entreprises les principaux moyens juridiques de protection de leur patrimoine.

Les produits, le savoir-faire, les écrits, les logiciels créés par l'entreprise forment l'essentiel de sa richesse et constituent son patrimoine. C'est le rôle de la propriété industrielle de protéger ce patrimoine résultant des efforts d'étude et de recherche et de l'expérience de l'entreprise. La propriété industrielle regroupe les brevets d'invention, les marques de fabrique, de commerce ou de service, et les dessins et modèles. Il s'agit de véritables titres de propriétés reconnus et protégés à l'échelle internationale qui fournissent à son détenteur un monopole d'exploitation.

C'est un moyen efficace pour lutter contre l'une des fins de l'espionnage : la contrefaçon. Les espions ne seront pas habilités à utiliser l'information volée. Déposer un brevet ou une marque dissuade les espions de pénétrer dans l'entreprise puisque l'information est rendue publique, mais verrouillée.

1. Les armes de la propriété industrielle

Des actions d'information, de sensibilisation et de formation sont régulièrement engagées par l'Institut National de la Propriété Industrielle (INPI) auprès des entreprises. Ces actions sont d'autant plus nécessaires que le réflexe de la protection existe peu dans les entreprises françaises. En France, il arrive souvent que l'inventeur n'ait pas conscience de la valeur inventive de sa découverte ; on pense en général que seule l'invention géniale est protégeable. Or, la majorité des brevets déposés, surtout au Japon, ne concernent que des améliorations de produits ou procédés existants.

Le choix du titre de protection dépend de la nature de la création. Un procédé de fabrication novateur relève d'une protection par brevet. Le nom du produit ainsi que ses signes distinctifs (logo, emballage, étiquette) seront protégés par une marque. L'esthétique du nouveau produit relève, elle, d'une protection par dessins et modèles.

A – Le brevet

Le brevet est le titre de propriété industrielle qui confère à son titulaire, inventeur ou entreprise, un droit exclusif sur une invention pour une période de vingt ans. En cas de contrefaçon prouvée, le détenteur du brevet peut justifier de sa propriété de l'invention et obtenir la cessation de la contrefaçon et des dommages et intérêts.

Les critères de brevetabilité sont au nombre de trois : la nouveauté – toute invention doit être nouvelle, sinon elle ne justifierait pas son nom, l'activité inventive[1], et l'application industrielle – l'invention doit pouvoir être réalisée de façon industrielle.

Le brevet a des rôles multiples. Il sert tout d 'abord à se protéger. C'est son rôle défensif. Il sert à la conquête des marchés ou à consolider une position de leader ; il est utilisé pour réaliser une stratégie. C'est son rôle offensif. Enfin, il peut être utilisé pour empêcher des concurrents de prendre une part de marché dans un segment donné et sert à intimider d'éventuels copieurs. C'est son rôle dissuasif. Ces trois fonctions se révèlent efficaces pour faire barrage aux tentatives d'espionnage que des concurrents peuvent mettre en place. Le brevet peut être une protection internationale, à condition d'effectuer les démarches supplémentaires nécessaires.

Le brevet français ne donne des droits que sur le territoire français. Pour se protéger à l'étranger, l'entreprise dispose depuis 1978 du brevet européen ou du Patent Cooperation Treaty qui permet de déposer une demande internationale dans les pays ayant signé ce traité.

Fin 1994, on estime à 4 millions le nombre de brevets en vigueur dans le monde. 670 000 dépôts de brevets ont été recensés en 1994 par l'Organisation Mondiale de la Propriété Intellectuelle. Les demandes de brevets européens auraient progressé de 6% entre 1994 et 1995, ce qui représente 78 300 nouvelles demandes enregistrées par l'Office Européen des Brevets[2] (OBE).

Par rapport aux autres nations industrielles (Japon, États-Unis, Allemagne et Royaume-Uni), la France occupe la dernière place en ce qui concerne le dépôt de brevets. La faible position de la France s'explique dans le fait que les entreprises françaises et leurs dirigeants ont été peu sensibilisés au rôle de la propriété industrielle. L'industrie japonaise,

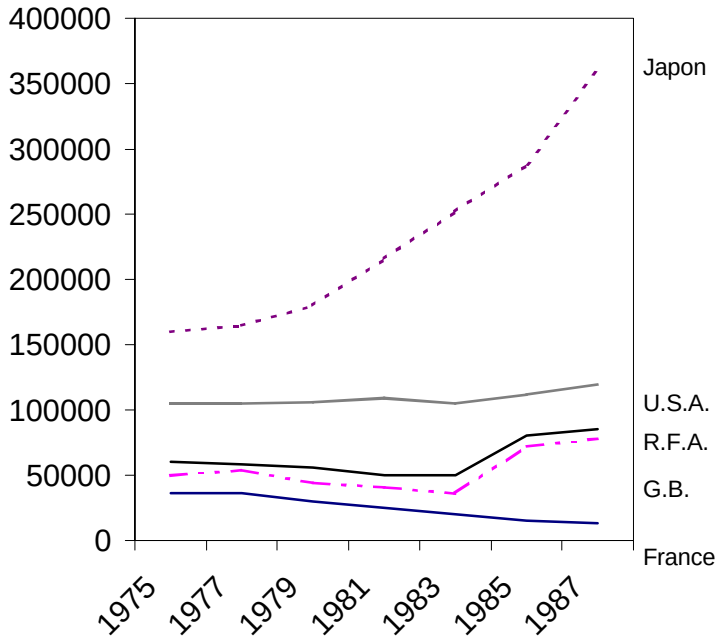
---

[1] selon le droit européen : une invention est considérée comme impliquant une activité inventive « si, pour un homme de métier, elle ne découle pas de manière évidente de l'état de la technique. »
J. Villain « Principaux décrets, lois, instructions et accords européens relatifs à la propriété intellectuelle » *L'entreprise aux aguets* . op. cit. p 167.

[2] OBE. *Rapport Annuel* 1995. (http://www.epo.co.at/epo)

quant à elle, a véritablement le souci de protéger sa technologie comme l'indique le nombre annuel de brevets déposés, qui dépasse de très loin celui des autres pays. En 1987, les demandes de brevets japonais représentaient 40% du total des demandes mondiales et quatre fois plus que le nombre de dépôts japonais de 1965. Aujourd'hui, la seule société Hitachi dépose autant de demandes de brevets que l'ensemble des entreprises françaises.

Figure 5 : Evolution du nombre de dépôts de brevets nationaux et étrangers dans les principaux pays industrialisés



En 1987, les Japonais ont, en outre, procédé à l'achat de brevets étrangers pour un montant de 260 milliards de yen, dont 174 milliards pour les seuls brevets américains. Cette situation fait d'ailleurs l'objet d'un sérieux mécontentement des industriels américains et de l'administration américaine qui reprochent au Japon de tirer trop facilement profit de la technologie américaine en limitant ses efforts de recherche et développement. Les Américains reprochent, de plus, aux Japonais leur lenteur dans la délivrance des brevets étrangers au Japon.

B – Les marques, dessins, modèles

Un produit, un objet ou un service peuvent être protégés par une marque qui les caractérisera sur le marché et qui les associera directement à l'image de l'entreprise. En France, le droit à la marque s'acquiert par le dépôt. La protection conférée par la marque est valable pour une période de 10 ans renouvelable.

De même, un dessin nouveau, une forme plastique nouvelle, un objet possédant une esthétique originale peuvent être l'objet de dépôt de dessins ou de modèles. La durée de protection est de 25 ans, renouvelable une fois. Si l'auteur ne l'exploite pas lui même, il peut le vendre ou en concéder l'exploitation en exclusivité.

Si les industriels français sont en retard en matière de brevets, ils sont en revanche plus portés à utiliser les marques. Une progression de l'ordre de 23% a été observée entre 1987 et 1988.

C – Les enveloppes Soleau, cahiers de laboratoires, et dépôts chez le notaire

Il est parfois utile, en vue d'une négociation ou plus simplement pour avoir des arguments incontestables en cas de litige, de faire reconnaître que l'entreprise est propriétaire de certaines informations ou résultats d'études. Trois moyens peuvent être utilisés pour faire reconnaître cette propriété.

Tout d'abord, l'enveloppe Soleau. Valable uniquement en France, elle attribue à son détenteur un droit de possession antérieure lui permettant d'exploiter ce qui a été consigné dans cette enveloppe et qui a été maintenu secret. L'enveloppe Soleau est donc un moyen rapide et gratuit de faire reconnaître son invention et de l'exploiter. Mais, contrairement au brevet qui donne son monopole d'exploitation en échange de la publication de l'invention, l'enveloppe Soleau ne met pas l'inventeur à l'abri d'un dépôt de brevet ultérieur d'un tiers sur le même sujet

Les cahiers de laboratoire consignant périodiquement l'état d'avancement des recherches constituent aussi un moyen de notifier les documents. Ces deux moyens, pour être valables, doivent être visés par un officier public. L'enveloppe Soleau peut être déposée à l'INPI.

Enfin, on peut aussi procéder au dépôt de « plis cachetés » auprès d'un notaire ou de certaines associations accréditées, toujours dans le but d'attester que ce que contiennent ces plis était bien, à date dite, en possession du déposant.

D – La protection des logiciels

Les logiciels doivent être protégés au même titre que les inventions relatives à des procédés ou à des produits. Cependant, dans ce cas précis, le brevet ne peut s'appliquer. En effet, la loi du 3 juillet 1985 assimile la protection des logiciels au droit d'auteurs. Néanmoins, lorsqu'on connaît l'ampleur actuelle de la contrefaçon de logiciels, l'entreprise aura tout intérêt à prendre des mesures destinées, en cas de litige, à prouver sa propriété du logiciel et à apporter la preuve de sa création en son sein.

Ces mesures peuvent être de plusieurs natures : établissement de la liste chronologique des logiciels créés ; dépôt éventuel chez notaire du nom du logiciel et de tout ou partie des pièces utiles à l'établissement de la preuve de la création du logiciel sur lequel le droit d'auteur est revendiqué (listings, cassettes, disques, documentation…) ; dépôt éventuel de la marque ; insertion dans le logiciel d'un signe ou d'une instruction particulière identifiable par le créateur ; etc.

2. Limites de la propriété industrielle

Tous les éléments du patrimoine informationnel de l'entreprise ne relèvent pas de la protection par la propriété industrielle, soit qu'ils y échappent par nature, soit que l'entreprise ne veuille pas se soumettre aux contraintes qui s'attachent à l'obtention de droits de propriété industrielle.

A – Les informations qui échappent à la propriété industrielle par nature

Échappent ainsi par nature à la protection par le brevet les simples idées n'étant pas susceptibles de donner lieu à un résultat industriel ou ne présentant pas une nouveauté ou une activité inventive suffisante[3]. Le même article du Code exclut également du champ de la brevetabilité les simples présentations d'information, les méthodes intellectuelles ou encore, comme nous l'avons vu précédemment et bien que cela soit très contesté, les programmes d'ordinateurs.

[3] Article L. 611-10 CPI : « 1. Sont brevetables les inventions nouvelles impliquant une activité inventive et susceptibles d'application industrielle. 2. Ne sont pas considérées comme des inventions au sens du premier alinéa du présent article notamment : a) Les découvertes ainsi que les théories scientifiques et les méthodes mathématiques ; b) Les créations esthétiques ; c) Les plans, principes et méthodes dans l'exercice d'activité intellectuelles, en matière de jeu ou dans le domaine des activités économiques, ainsi que les programmes d'ordinateurs ; d) Les présentations d'informations.»

D'autres restrictions s'appliquent aux marques (exclusion des signes descriptifs) ou aux dessins et modèles (exclusion des dessins ou formes insuffisamment distinctifs ou présentant une physionomie purement fonctionnelle).

B – Les contraintes qui pèsent sur les entreprises

A part ces cas où la propriété industrielle n'est pas susceptible de couvrir certains éléments du patrimoine de l'entreprise, il arrive également que l'entreprise souhaite échapper aux contraintes liées à ce mode de protection.

La principale de ces contraintes, outre celle d'effectuer les démarches auprès de l'INPI ou des autres offices étrangers ou internationaux, est la publicité qu'impose la constitution de ce type de droits[4]. Passés certains délais d'examen (pour les brevets) et de publication, la demande de titre de propriété industrielle est, en effet, rendue publique et accessible à tous, notamment via le relais des bases de données électroniques, fournissant d'ailleurs ainsi aux entreprises un excellent outil de surveillance de leur environnement concurrentiel au niveau national et international. En effet, les brevets renferment 80% de la technologie de l'invention, la rendre publique c'est donc informer et orienter directement les concurrents sur ses axes de recherches.

La propriété industrielle est une protection juridique mais, pour être efficace, encore faut-il que ce droit soit reconnu partout et surtout que les dommages et intérêts soient mieux estimés. Le tribunal donne raison aux plaignants dans 93% des cas, mais ne leur accorde que 31% des dommages et intérêts qu'ils demandent. Il est souvent difficile d'établir une évaluation justifiée des dommages. La couverture du préjudice subi est donc souvent très faible ; c'est pourquoi, les détenteurs de brevets renoncent souvent à faire respecter leurs droits. Une enquête réalisée par l'Union des fabricants[5] montre ainsi que 64% des petites et moyennes entreprises déclarent avoir été victimes de la contrefaçon, mais que 25% d'entre elles n'ont rien fait pour se défendre, que 34% ont négocié un accord et que seulement 41% ont intenté un procès. Ces résultats provoquent chez les chefs d'entreprises de nombreuses hésitations, quant à l'efficacité de la protection et donc l'utilité des droits de propriété industrielle.

Autre inconvénient : un brevet, c'est cher. Il faut bien être conscient de la dimension financière du problème. Les services d'un ingénieur-conseil sont souvent indispensables pour estimer s'il y a matière à dépôt. Le coût du dépôt lui-même est modéré si on se limite à

[4] La seule exception à l'obligation de publicité concerne les dessins et modèles où il existe une possibilité d'effectuer des dépôts non rendus publics durant une période maximale de trois ans (art. R. 512-10 CPI)
[5] P. Poncelet. *L'Entreprise* « Brevet ou Secret » n°128, mai 1996, p45.

une protection pour la France. Mais l'addition monte vite dès lors qu'il faut l'étendre à l'étranger. Déposer dans quinze pays coûte autour de 500 000 francs. Les vingt annuités à payer pour conserver le droit de propriété d'un brevet sur vingt-cinq pays sont de l'ordre de 900 000 francs. Le coût annuel est de 200 000 francs au Japon contre 30 000 francs en France.

Ainsi, les armes de la protection industrielle imposent beaucoup de contraintes aux entreprises. Nombreuses sont alors les entreprises qui renoncent à la protection industrielle et préfèrent utiliser le secret, par exemple. Cependant, cela suppose que l'entreprise puisse protéger efficacement ses informations au sein de l'entreprise. Pour cela, l'ensemble du personnel doit être sensibilisé à lutter contre le vol d'informations. Quelques règles simples peuvent se révéler très efficaces.

Section 2 : La protection industrielle

Le brevet, la marque, le modèle, l'ensemble des armes de la protection industrielle sont des moyens juridiques qui permettent à leur détenteur de faire reconnaître ses droits face à un contrefacteur. Si dans les pays industrialisés occidentaux, on peut s'attendre logiquement à une reconnaissance des droits de protection industrielle et donc à une condamnation du contrefacteur, en est-il réellement de même dans les pays de l'Est et dans les pays du Tiers-Monde ? La réponse est sans doute plus nuancée. Serait-il donc raisonnable que l'entreprise ne se réfugie que derrière la protection industrielle ? Peut-on admettre, en outre, que seules les inventions soient protégées ? Un concurrent ou un pays étranger n'est-il pas aussi attiré par d'autres secrets comme les procédés de fabrication, de montage, de contrôle, par la nature des investissements réalisés, par la santé économique de l'entreprise, par la compétence même de ses employés, par son organisation interne ?

Ainsi, tout ne peut être protégé par la protection industrielle qui a sa propre efficacité, certes, mais aussi ses limites. La protection de ce qui ne peut l'être par la protection industrielle incombe alors à la protection industrielle. Le dispositif ne saurait être global sans ces deux fonctions complémentaires.

Inéluctablement, l'espionnage conduit à fragiliser l'entreprise qui en est victime. Il conduit à une perte d'activité plus ou moins grande pouvant déboucher sur le chômage si la compétitivité de l'entreprise est réellement atteinte.

En fait, la protection dépasse la stricte lutte contre l'espionnage industriel. Il convient aussi de discipliner l'entreprise dans la diffusion des informations vers l'extérieur.

Se protéger est une nécessité mais vouloir assurer une protection absolue est illusoire. Il y a donc une juste mesure entre ne rien faire et ériger l'entreprise en bastion ou camp retranché. Il convient alors de prendre en considération les dépenses à consentir aux moyens de protection et les contraintes acceptables par les personnels. Concilier protection et climat social est une nécessité. Par ailleurs, la protection ne doit pas générer des comportements qui iraient à son encontre.

Pour la plupart des entreprises, il s'agit, avant tout, de prendre quelques précautions élémentaires et peu coûteuses pour assurer un minimum de protection.

1. L'organisation du contre-espionnage dans l'entreprise

Face aux menaces et compte tenu de ses propres vulnérabilités, l'entreprise a donc intérêt à se protéger et à construire sa propre sécurité.

Étant donné l'importance de l'enjeu mais aussi la complexité du problème, il est clair que la sécurité ne peut être improvisée. Elle doit résulter d'une réflexion approfondie, au niveau global mais aussi sectoriel de l'entreprise. Les actions entreprises doivent être cohérentes et concerner aussi bien les hommes que les biens.

La sécurité dans l'entreprise est l'affaire de tous ; cependant, il est utile qu'elle soit orchestrée par un responsable sécurité. Après avoir identifié les menaces par leur nature, leur importance, leur probabilité d'occurrence, il doit recenser ce qui doit être protégé : les informations, les produits, les locaux, les hommes. L'élaboration d'un plan de sécurité résulte d'une véritable méthodologie du management des risques.

Dans tous les cas, organiser la sécurité du patrimoine de l'entreprise doit se faire autour de trois axes : la responsabilisation du personnel, la protection des biens, et la surveillance de la communication. Il faut veiller à ce que chacun des ces principes soit effectivement appliqué à l'intérieur et à l'extérieur de l'entreprise.

A – La sensibilisation auprès du personnel

L'effort principal d'amélioration de la sécurité concerne les hommes de l'entreprise. Ceux-ci doivent être sensibilisés aux risques qu'ils encourent et aux comportements qu'ils doivent adopter pour rendre l'entreprise plus sûre. Les actions de sensibilisation doivent s'adresser à l'ensemble du personnel et notamment aux nouveaux embauchés. Chez Thomson, Fernand Colin, directeur de la sécurité du groupe assure que « l'ensemble du personnel intègre la sécurité comme un élément de ses compétences professionnelles et de son cursus de formation ».

La difficulté de ces actions réside dans le fait qu'elles doivent être à la fois crédibles, suffisamment fréquentes pour maintenir une pression nécessaire sans créer pour autant un climat de paranoïa et s'adresser à tous en s'adaptant aux différentes spécificités des personnes dans l'entreprise. Il convient d'utiliser des moyens diversifiés et les plus attractifs possibles : conférences, films, brochures de sécurité…

La DST peut apporter une aide aux entreprises dans ce domaine. Chaque année, elle intervient auprès de plusieurs centaines d'entreprises sensibles (armement, aéronautique, laboratoires) et organise des conférences de sensibilisation pour le personnel et les dirigeants. Plus de 500 conférences de ce type ont été réalisées en 1986.

a) Dans l'entreprise, la sécurité doit se construire par des règles simples vis-à-vis du personnel, des nouveaux embauchés, et des stagiaires. En plus de la sensibilisation et responsabilisation, les experts recommandent aux chefs d'entreprise d'exiger des employés la confidentialité concernant les travaux réalisés dans l'entreprise, d'établir des engagements de non-concurrence avec certains employés[1].

Il faut se montrer attentif également à ne pas divulguer de nouveaux projets dans des annonces publicitaires ou offres d'emplois.

En ce qui concerne les stagiaires, il est préférable d'avoir un entretien avec eux et les employés quand ils quittent l'entreprise, mais il convient également de contrôler attentivement les informations des rapports de fin de stages.

b) A l'extérieur de l'entreprise, les employés doivent se montrer prudents à ne pas évoquer dans des conversations des informations confidentielles relatives à l'entreprise, ou bien s'assurer d'abord qu'elles ne peuvent être écoutées par des oreilles indiscrètes.

Le personnel doit être informé du danger que représente la lecture de documents confidentiels dans des lieus publics (gares, trains, avions). Certaines lignes aériennes comme celles de Paris-Bordeaux et Paris-Toulouse qui voient chaque jour de nombreux ingénieurs du domaine aéronautique et spatial sont régulièrement fréquentées par des

[1] Extraits tirés d'un contrat de travail établi pour l'entreprise X., société de services en informatique :
« Article 3 – Discrétion professionnelle : Vous êtes lié(e) par le secret professionnel le plus absolu en ce qui concerne les affaires de la Société X., pendant l'exécution, mais aussi après la cessation du contrat. Vous êtes soumis(e) à la confidentialité la plus absolue et, en conséquence, vous vous interdisez de diffuser toutes informations dont vous aurez eu connaissance dans le cadre de votre activité. Vous vous engagez à ne divulguer à qui que ce soit, aucun des procédés de fabrication ou des méthodes commerciales de la Société. Vous vous interdisez de faire usage, à titre personnel ou sous quelque forme que ce soit, de toutes informations sur les logiciels, programmes informatiques et études appartenant et ayant été réalisés par notre Société et dont vous aurez pu avoir connaissance. (…) Article 9 – Clause de non-concurrence : En cas de départ, vous vous interdisez de conserver toutes pièces, documents ou correspondances appartenant à la Société ou d'entrer, pour quelque fonction que ce soit, au service d'un client de la Société (...). Ces interdictions sont limitées à 6 mois si votre départ a lieu durant les 6 premiers mois de présence, 12 mois si votre départ à lieu durant la première année de présence, 18 mois si votre départ a lieu après la première année de présence. En cas de violation de cette obligation, l'entreprise sera en droit de réclamer le versement de dommages et intérêts. »

agents de renseignements étrangers. Le Wall Street Journal du 10 novembre 1995 a lancé une rumeur selon laquelle dans certains avions français, les lampes de lecture individuelles auraient été remplacées par des mini-caméras filmant les documents des hommes d'affaires.

Lorsqu'un employé donne sa carte de visite professionnelle, il faut s'attendre à ce qu'on lui téléphone pour lui demander de l'information. De même, chacun doit faire attention à conserver toujours sur soi son cahier de notes personnelles, ne jamais abandonner la garde directe d'informations ou de matériel pendant une visite à l'extérieure (sur le siège arrière d'une voiture par exemple).

B – La protection des biens

Concernant les biens eux-mêmes, c'est-à-dire les documents et les produits, des dispositifs variés peuvent être mis en œuvre : clôtures, organisation des locaux facilitant le contrôle des visiteurs, armoires fortes, système de surveillance, d'alarmes.

a) On ne peut éviter la présence d'étrangers au sein de l'entreprise. Il convient donc d'organiser le contrôle et la circulation des personnes. C'est notamment le cas pour les clients, fournisseurs et visiteurs qui ne doivent pas avoir accès à toutes les zones de l'entreprise. Ces personnes doivent être facilement identifiables afin de mieux contrôler leur cheminement pour éventuellement intervenir au cas où leur présence en des endroits non prévus se manifeste. Le port de badges « société » et « visiteurs » est un moyen de contrôle de ce type d'intrusion ; cependant, il ne suffit pas toujours. Dans la mesure du possible, ces visiteurs doivent être accompagnés dans leurs déplacements internes. Il ne faut montrer de l'entreprise que le strict nécessaire et ne jamais laisser un visiteur seul dans l'entreprise ou dans un bureau.

Le marquage des documents et matériels sensibles est également recommandé. Cette classification des éléments du patrimoine de l'entreprise permet de les protéger selon leur degré de sensibilité. Chaque entreprise se doit d'organiser son propre système de protection en veillant toutefois à ce que les mesures prises ne soient pas contraignantes au point de paralyser la circulation de l'information.

Les documents sensibles ne doivent être diffusés qu'à un nombre restreint d'individus afin de limiter les risques de divulgation des informations. Ils doivent être également être soumis à des règles quant à leur reproduction, leur circulation, leur stockage. Il est fortement recommandé de les ranger dans des coffres.

A titre d'exemple, IBM a instauré quatre niveaux de classification : document à usage interne, niveau « Confidential IBM », niveau « IBM Confidential Restricted », et le niveau « Registered IBM Confidential ». Ainsi les documents avec la mention RIC ne sont diffusés qu'à un nombre très limité de personnes qui ne peuvent les photocopier sans autorisation ni les transmettre par téléphone sans qu'ils aient été préalablement codés.

Dans tous les cas, au sein de l'entreprise, aucun document ne doit être laissé en vue sur un bureau et surtout pas en dehors des heures de travail. Les brouillons doivent eux aussi être classés ou sinon détruits et non pas jetés à la corbeille. Chez Procter & Gamble, on pratique le clean desk policy : aucun papier ne doit traîner, tout document non conservé doit passer au broyeur, y compris les photocopies ratées.

Pour la sécurité interne des biens, les entreprises peuvent également faire appel à des sociétés de service susceptibles de fournir des prestations d'installation de systèmes de surveillance et d'alarme ou de gardiennage si l'entreprise le juge nécessaire. Cependant, le choix de ces sociétés doit être particulièrement bien fait.

b) En dehors du cadre de l'entreprise, la protection des biens se heurte au problème du transport. Chaque étape nécessite de faire preuve de vigilance. Les employés doivent avoir pour recommandation de ne jamais abandonner la garde de leur attaché-case et de ne pas ranger les documents de travail dans les bagages.

De même, beaucoup de grandes entreprises évitent consciencieusement de faire descendre leurs cadres systématiquement dans les mêmes hôtels et refusent que l'interlocuteur étranger les réserve. Dans certains pays, dont la France, les hôtels sont très souvent la cible des services de renseignements nationaux qui peuvent agir aisément et photographier les documents laissés seuls dans la chambre. Il vaut donc mieux également ne pas utiliser les coffres-forts de l'hôtel et éviter de recevoir des appels téléphoniques et fax à l'hôtel.

Chez Thomson, on conseille aux cadres de changer d'hôtel à chaque séjour pour déjouer une éventuelle installation de micros dans les chambres, de ne pas envoyer de fax depuis les hôtels, de se méfier des guides et interprètes locaux.

C – Surveiller la communication

a) A l'intérieur de l'entreprise, les moyens de communication doivent faire l'objet de méfiances. Personne ne doit transmettre d'informations sensibles par des lignes de communication non protégées. Toutes les demandes d'informations transmises via Internet doivent être analysées avec suspicion. Il ne convient de répondre qu'aux personnes connues et uniquement après avoir vérifié leur adresse et identité. Le gouvernement américain a établi une liste des indications qui doivent susciter le méfiance de son destinataire : l'adresse est située dans un pays étranger ; le destinataire ne connaît pas l'expéditeur ; l'expéditeur se présente sous le statut d'étudiant ou de conseiller ; il cherche à s'informer sur une technologie, un projet, ou un contrat sensible.

Pour lutter contre le piratage informatique, nombre d'entreprises ont décidé de ne pas raccorder leurs systèmes les plus sensibles à des serveurs extérieurs. Cela ne suffit pas pour autant à assurer une protection maximale.

b) Il est également préférable de contrôler au préalable les exposés et articles destinés à être communiqués à l'extérieur et maîtriser attentivement les relations avec la presse. Aucun membre du personnel ne doit faire état dans les colloques de résultats d'études confidentielles. Il faut aussi veiller à ne pas donner des informations de façon unilatérale. La démarche commerciale professionnelle impose des actions de promotion ; dans ce cas, il faut veiller à communiquer vers ses clients et non pas vers ses concurrents. La vente directe vers un client identifié est préférable à la publicité dans les journaux et magazines.

La sécurité du patrimoine informationnel est une affaire de comportement des individus plus que de barrières. Il faut, avant tout, sensibiliser et former le personnel à la protection de l'information, et ensuite instaurer des règles simples, basiques. Cependant, le responsable de la sécurité doit rester conscient des dysfonctionnements et des limites que comporte un tel système.

2. Les limites de la protection industrielle

Il existe de nombreuses d'erreurs sécuritaires à ne pas commettre. Porter la protection du patrimoine à son paroxysme peut provoquer des résultats inverses à ceux attendus. Il est impossible de tout protéger ; l'organisation de la sécurité doit faire preuve de réalisme, d'autant plus qu'elle est soumise à des contraintes de prix.

A – Les dangers de l'artillerie sécuritaire

Réputées plutôt laxistes il y a encore 10 ans, les sociétés françaises font à présent preuve d'un zèle sécuritaire qui frise parfois la paranoïa. Les chefs d'entreprise ont de plus en plus tendance à développer des procédures excessives en sécurité ; celles-ci peuvent conduire à des situations complètement absurdes, voire dangereuses et illégales.

La première erreur des chefs d'entreprise consiste à vouloir transformer leur entreprise en véritable forteresse. Or, la multiplication des contrôles d'accès à l'intérieur de l'entreprise finit par nuire à l'efficacité et à la communication entre les services. A la direction générale de France Télécom il faut désormais un badge spécial entre chaque étage. De même, l'imposition d'un véritable arsenal réglementaire au personnel conduit à des situations où les employés ont tendance à s'abriter derrière des procédures de façon formaliste, sans engager leur responsabilité.

Une procédure trop tatillonne peut obliger une secrétaire à passer l'essentiel de son temps à déposer et à retirer ses disquettes d'un coffre-fort ! Une trop grande rigidité ne tarde d'ailleurs pas à provoquer des comportements antisécuritaires qui peuvent très facilement ouvrir des brèches dans les systèmes les plus perfectionnés : le salarié peut trouver plus pratique de bloquer une porte à accès contrôlé ou de communiquer son mot de passe à son collègue.

Une seconde erreur que les chefs d'entreprise peuvent être tentés de faire consiste à espionner leurs salariés. Les employeurs ont peur des bavardages de leurs salariés. Les standards téléphoniques électroniques modernes, très sophistiqués, permettent non seulement de contrôler tous les numéros appelés, mais aussi parfois d'enregistrer les conversations, pratique complètement illégale. L'installation de caméras surveillant les salariés au travail est également sujette à caution. Une entreprise de BTP a été condamnée pour avoir filmé ses ouvriers dans les vestiaires sous prétexte de lutter contre le vol. L'entreprise dérive alors par ces pratiques vers des moyens dangereux et illégaux.

Enfin, certaines entreprises adoptent la stratégie du mutisme général, qui peut, elle aussi s'avérer dangereuse. Lorsqu'on téléphone à une entreprise pour connaître le nom du directeur commercial, certaines croient bon de ne donner aucun nom par téléphone, alors que ce genre de renseignement peut se trouver facilement dans des annuaires spécialisés. Une telle attitude peut se révéler anti-commerciale dans de nombreux cas. On arrive à des situations où un ingénieur commercial refuse d'expliquer les possibilités techniques de ses produits à un de client sous prétexte que l'information est confidentielle.

Ainsi, il faut doser les mesures protectrices, tâche difficile, de façon à ce qu'on n'aboutisse pas à des situations dangereuses.

B – Tout ne peut pas être contrôlé

Il est impossible de retenir certaines informations, soit parce que la loi exige qu'elles soient rendues publiques, soit parce que certains agents sont moins enclins à respecter les consignes de sécurité, ou encore parce que l'employeur n'a pas tous les pouvoirs pour contrôler les informations.

La législation comptable, financière, commerciale contraint les entreprises à diffuser des informations qui peuvent se révéler utiles pour un public avisé : la composition d'une préparation surgelée, la formulation d'un médicament, doivent être mentionnées sur le produit. Et toutes ne peuvent pas, comme les sociétés japonaises, diffuser des bilans tellement consolidés qu'ils en deviennent indéchiffrables, ou, comme certaines sociétés françaises omettre en toute illégalité de publier dans leur rapport annuel leur compte d'exploitation.

Il est également difficile de contenir une pratique, courante chez les chercheurs occidentaux, qui consiste à publier des articles au fur et à mesure de l'avancement de leurs recherches. Pratique indispensable, estiment les intéressés, pour faire progresser leur notoriété dans la communauté scientifique internationale. Les chercheurs mettent en avant l'universalité de la science pour ignorer ostensiblement les conseils de discrétion qu'on leur demande d'observer. Ce sont également les ingénieurs des bureaux d'études, mais aussi les créatifs des services de publicité, qui admettent le plus difficilement, lorsqu'elles existent, les consignes de sécurité industrielle.

Ces publications constituent une brèche considérable dans les dispositifs de protection nationaux. Cependant, l'expérience prouve que ces informations ne sont exploitables que par des entreprises qui ont un niveau proche ou peu de retard par rapport à l'entreprise pillée.

L'employeur français souffre d'un handicap qui l'empêche d'effectuer une recherche sur le passé et la vie d'un salarié dans l'entreprise. C'est une liberté à laquelle il est impossible de porter atteinte. La loi Informatique et Libertés interdit la constitution de fichiers sur les individus à problèmes. L'employeur ne peut que se reposer sur l'entretien de recrutement pour tester la déontologie de son futur employé. Les actions passées du salarié sont des informations que l'employeur ne maîtrise pas et qu'il ne peut donc pas contrôler.

C – Le prix de la protection

La sécurité de l'entreprise coûte cher, en argent et en temps. Peu de chefs d'entreprise sont prêts à alourdir leur budget pour assurer une sécurité toujours fragile.

Un simple coffre-fort servant à consigner des documents sensibles coûte en moyenne 60 000 francs. Le prix d'un système de contrôle d'accès avec badge à mémoire oscille entre 200 et 600 000 francs, celui d'un système de détection périmétrique n'est pas loin des 4,5 millions. L'achat d'une centrale de télésurveillance atteint facilement 8 millions de francs.

Il est très difficile de doser les dépenses consacrées à la sécurité. Il faudrait évaluer l'ampleur des risques encourus. Mais comment déterminer le coût d'un vol de fichier, ou celui de la divulgation prématurée d'une opération marketing ? Comment chiffrer ces pertes qui ne se traduiront que par des manques à gagner en termes de parts de marché ou d'image publicitaire ?

Rares sont les entreprises qui consacrent des sommes importantes à la protection. Bien souvent, ce budget arrive au dernier rang des préoccupations et subit les contrecoups de la situation financière de l'entreprise.

Section 3 : La protection offensive : dissimulation et intoxication

Nous avons pu montrer à quel point les techniques traditionnelles de la propriété intellectuelle et du contre-espionnage industriel peuvent encore s'avérer insuffisantes. Au fur et à mesure de la prise de conscience des pays occidentaux quant à l'ampleur de l'espionnage industriel, de nouvelles formes de protection plus offensives se sont répandues.

La dissimulation, plus communément appelée préservation du secret, n'est pas un phénomène très nouveau. Cependant, c'est une tactique très largement adoptée aujourd'hui. Les entreprises japonaises sont devenues des adeptes de la dissimulation ; lors du développement de nouvelles technologies, elles préfèrent désormais conserver le secret le plus longtemps possible : déposer des brevets reviendrait à alerter les concurrents.

L'intoxication est un instrument particulièrement offensif. Il s'agit de répondre à l'espionnage industriel en diffusant de fausses informations. C'est ce que nous avions appelé, dans le premier chapitre, la désinformation. Associée à tous les précédents moyens de protection, elle assure une protection optimale. Les nouveaux réseaux de communication facilitent d'autant plus l'usage de cette méthode

1. La dissimulation : conserver le secret

Le premier des réflexes lorsque l'on veut protéger ses documents et notamment une invention consiste à maintenir le secret. Toutes les entreprises sont confrontées au dilemme : brevet ou secret ?

Bien que le secret soit reconnu par la loi, c'est un choix qui reste très risqué. En réalité, il peut s'avérer justifié pour une courte période ; à long terme, c'est une solution plutôt dangereuse.

A – Le choix du secret

Comme nous l'avons vu précédemment l'intérêt du dépôt de brevet est sujet à discussion. Déposer un brevet, c'est toujours s'exposer à ce qu'un concurrent utilise

l'invention décrite dans le texte. Les coûts de la protection juridique et les incertitudes qui entourent le brevet expliquent que nombre d'entreprises préfèrent la stratégie du secret.

Les notions de secret de fabrique et de secret des affaires sont définies juridiquement. La loi punit la révélation par tout directeur ou salarié des secrets de fabrique de leur entreprise, secrets que la jurisprudence définit comme « tout moyen de fabrication qui offre un intérêt pratique ou commercial et qui, mis en usage dans une industrie, est tenu caché à ses concurrents ». On considère que la protection des « secrets d'affaires » est assurée en France par la conjonction du secret de fabrique avec d'autres dispositifs juridiques spécifiques, tels que le secret des correspondances et des télécommunications, le secret professionnel, la répression des fraudes informatiques ou encore le secret bancaire, le secret statistique…

Depuis de nombreuses années, la parfumerie et les industries alimentaires pratiquent largement le secret. C'est aussi le cas d'industries plus récentes comme l'électronique ou les biotechnologies. Dans la cosmétique, les brevets ne sont pas efficaces puisqu'il suffit au contrefacteur de changer un tant soit peu la composition pour contourner la protection. Il convient également de préciser que le savoir-faire (know how) ne peut être protégé par le brevet. Dans ces industries, où toute la production est basée sur un savoir-faire, le secret reste l'unique solution.

Certaines entreprises ont ainsi organisé le secret industriel. L'accès aux différents laboratoires est contrôlé, les fiches de fabrication détaillant la composition des produits sont codées dans un langage que seuls les plus anciens peuvent déchiffrer. Dans les Cristalleries d'Arques, les machines de production les plus « sensibles », intégrant des procédés de fabrication exclusifs, sont installées à des endroits où clients et fournisseurs n'accèdent pas. Lorsque la venue de réparateurs est indispensable, ces machines sont recouvertes de bâches.

Le secret est souvent utilisé comme une étape préalable au dépôt de brevet. En effet, la publication du brevet offre des pistes gagnantes aux concurrents, alors que le déposant a financé des pistes perdantes pendant ses recherches. Conserver le secret pendant un certain temps permet d'avoir toujours une innovation d'avance en sommeil. Il s'agit de la mettre sur le marché lorsqu'un concurrent nous rattrape, mais pas avant. Patrick Colin, PDG d'Unither, explique ainsi qu' « il faut parfois savoir attendre et retarder la mise en œuvre de son innovation pour rendre le concurrent prisonnier de son nouvel investissement sur une technologie déjà dépassée ». Aujourd'hui, 63% des entreprises développent des innovations sans déposer de brevet.

B – Une efficacité controversée

Cette méthode du secret se heurte à de sérieuses limites, non seulement sur le plan juridique, mais aussi pratique.

Il faut constater que le droit français n'assure qu'une protection juridique très faible et très lacunaire au secret d'entreprise. Le secret de fabrique repose sur une définition qui en limite non seulement la nature (un secret technique uniquement) mais également les personnes qui peuvent être mises en causes juridiquement (salariés ou directeurs). De plus, toutes les autres formes de secret qui définissent le secret d'affaires ne sont que des instruments juridiques partiels qui répondent chacun à des conditions différentes et qui ne peuvent en aucun cas être additionnés pour déboucher sur la protection uniforme des secrets de l'entreprise.

Sur le plan pratique, on peut s'interroger sur la façon d'assurer l'étanchéité d'une information au sein de la collectivité que constitue l'entreprise et dans une société toute entière tournée vers la communication.

Le secret est une pratique d'autant plus risquée que, travaillant sur les mêmes pistes de recherche, un concurrent peut très bien breveter la même innovation et obtenir des droits exclusifs. En optant aussi pour le secret, on court le risque de voir partir un salarié chez le concurrent avec une innovation en poche.

Garder le secret est difficile et, dans la plupart des cas, illusoire. L'expérience montre d'ailleurs que de nombreux secrets finissent par être révélés, même les plus jalousement gardés. Les affaires d'espionnage qui apparaissent régulièrement sont là pour en témoigner. La révélation d'un secret, si elle n'est pas toutefois inéluctable, n'est très souvent qu'une question de temps. Plus le groupe d'hommes chargé de la mise au point d'un savoir-faire ou d'un produit au sein d'une entreprise est grand, plus les risques de fuite d'informations sont élevés.

2. L'intoxication : piéger ses concurrents

Les techniques qui consistent à intoxiquer ses adversaires avec de fausses informations sont de plus en plus répandues. Les professionnels de la sécurité n'hésitent pas à recommander ce type de protection plus offensive : bluff et intoxication font partie du jeu.

La désinformation est couramment utilisée par certains pays pour rendre plus efficaces leur politique et leur diplomatie. En milieu industriel, elle est pratiquée par certaines entreprises situées dans des domaines fortement concurrentiels. A titre d'exemple, elle peut s'exercer :

- au niveau technologique.

La guerre des brevets consiste à faire diversion en déposant plusieurs brevets dont un seul correspond réellement à la protection de l'invention, les autres brevets étant là pour engager les concurrents sur de fausses pistes. On peut également déposer des brevets de barrage qui dissuaderont un adversaire de s'engager dans une voie de recherche donnée. Ces brevets piégés (ou encore brevets « leurres » ou « de papier ») peuvent faire croire que l'entreprise a réussi à résoudre un problème sur lequel beaucoup piétinaient depuis longtemps, ou encore qu'elle a amélioré certains des produits ou procédés concurrents. Au Japon, ce type de brevets représente 40% de l'ensemble des dépôts.

- au niveau commercial.

Les fausses études de marché sont très répandues ; les entreprises n'hésitent pas non plus à lancer des campagnes de publicité fictives pour tromper leurs adversaires. Pour contrer l'espionnage au sein de l'entreprise, les rédacteurs des publications internes ont parfois pour ordre de fausser les résultats des bilans commerciaux.

- au niveau stratégique.

Dans ce cas, il s'agit de faire en sorte que les concurrents soient informés d'une stratégie qui ne sera pas réellement celle de l'entreprise.

Il est clair que la désinformation ne sera efficace que si elle est mûrement pensée et orchestrée. Il est souvent préférable de la faire réaliser par un intermédiaire, afin d'en accentuer la crédibilité auprès des concurrents.

CONCLUSION

L'accroissement et le durcissement de la concurrence internationale soulignent chaque jour davantage les lacunes dans la déontologie des économies de marché. L'ampleur prise aujourd'hui par l'espionnage industriel est là pour le démontrer. A la lecture de ce bilan, il reste difficile de croire que les entreprises pourront lutter seules contre ces pratiques souterraines. Les instruments de protection à leur disposition sont bien maigres face à la détermination des espions.

L'instauration d'un dialogue entre les États apparaît comme une solution pour contenir les dérives à l'échelle mondiale. Dans un contexte économique qui voit resurgir les intérêts nationaux et individuels, une coordination de ce type risque de se heurter à de nombreuses difficultés. Qui pourra prétendre au rôle de médiateur ?

De même, la coopération de firmes de toutes nationalités pourrait aboutir à la mise au point d'un code de déontologie universelle. A l'image d'un traité, les entreprises signataires s'engagent à respecter les règles d'une course à l'information « loyale », où les pratiques illégales et immorales seraient abolies. Le développement d'une ingénierie de l'information, à travers les concepts de veille et d'intelligence économique, va dans cette voie, même si les définitions nécessitent encore d'être harmonisées.

A défaut de l'ouverture de tels dialogues à l'échelle mondiale, la guerre de l'ombre risque de s'amplifier. Les menaces économiques peuvent se répercuter sur la sphère politique. Dans ce cas, les délits d'espionnage industriels peuvent créer des tensions politiques, qui seraient préjudiciables à la paix mondiale.

Ce n'est qu'au prix d'un désarmement multilatéral, c'est-à-dire de l'abolition universelle de ces pratiques souterraines que le monde pourra prétendre au pacifisme économique.

INDICATIONS BIBLIOGRAPHIQUES

REFERENCES SE RAPPORTANT AU CHAPITRE 1

- Ouvrages

DESVALS Hélène., DOU H. *La veille technologique : l'information scientifique, technique et industrielle.* Paris : Dunod, 1992. 434p.

COMMISSARIAT GENERAL DU PLAN. *Intelligence économique et stratégie des entreprises.* Rapport du groupe dirigé par Henri Martre. Paris : La Documentation Française, 1994. 212p.

COMMISSARIAT GENERAL DU PLAN. *Recherche et innovation : le temps des réseaux*. Rapport du groupe « Recherche, technologie et compétitivité » dirigé par Guy Paillotin. Paris : La Documentation Française, 1993. 159p.

COMMISSARIAT GENERAL DU PLAN. *Information et compétitivité.* Rapport du groupe présidé par René Mayer. Paris : La Documentation Française, 1990. 302p.

PORTER Michael E. *L'avantage concurrentiel des nations*. Paris : InterEditions, 1993. 883p.

ROUACH Daniel. *La veille technologique et l'intelligence économique.* Que Sais-je, n° 3086. Paris : Presses Universitaires de France, 1996. 127p.

- Articles

BRIDIER Gilles. «Le renseignement : arme de la guerre économique» *Le Monde* , 6 juillet 1995, p22.

DELBES Roger. « La veille concurrentielle : comment peut-elle être stratégique ? ». Revue Française du Marketing, n°155, mai 1995, pp 69-79.

DOU Henri. « Principes et méthodes de la veille technologique appliqués à l'environnement », *Compte-Rendu du CRRM*, 03/11/94. (http://www.crmm.org)

KAHN Annie. « Le rôle clé du renseignement ». *Le Monde*. 30 mars 1990, p 35.

LECLERE Jean-Philippe. « Veille technologique : un terrain juridique accidenté », *L'Usine Nouvelle*, n°2430, 28 octobre 1993, pp 65.

LEMAITRE Frédéric. « La chasse à l'information est ouverte ». Supplément Initiatives-Emploi*, Le Monde*, 26 septembre 1990, p IX.

LESCA Humbert. « Pour un management stratégique de l'information ». *Revue Française de Gestion.* sept-oct 1992, pp 54-63.

LESCA H., CARON M-L. « Veille stratégique : créer une intelligence collective au sein de l'entreprise ». *Revue Française de Gestion*. sept-oct 1995, pp 58-68.

MILON Alain. « La situation actuelle de la veille stratégique dans les secteurs de pointe ». *Humanisme et Entreprise*, décembre 1992, pp 69-89.

VOISIN Bruno. « L'information et l'entreprise : l'enjeu d'une quête ; entretien avec Hervé Sérieyx ». *Médiaspouvoirs*, n°34, 1994, pp 63-67.

REFERENCES SE RAPPORTANT AU CHAPITRE 2

- Ouvrages

SCHWEIZER Peter. *Les nouveaux espions : le pillage technologique des USA par leurs alliés*. [*Friendly Spies* : *How America's Allies are Using Economic Espionage to Steal our Secrets* – traduit de l'américain par M. Truchan-Saporta] Paris : B.Grasset, 1993. 345p.

WOLTON Thierry. *Le KGB en France*. Grasset : Paris, 1987, 310p.

- Articles

BEAUDEUX Pierre. « Espion, es-tu là ? », *L'Expansion*, n°248, 15 novembre 1984, pp 52-63.

BERNARD Catherine. « Entreprises, gare aux espions », *Science et Vie Economie*. n° 43, octobre 1988, pp 66-73.

CHAMBOST Germain. « Après la guerre froide, la guerre économique ». *Science et Vie Economie*, n°921, juin 1994, pp 104-106.

CHIRAYATH J.B. « Industrial espionage victimizes company of revolutionary internet technology worth $250 Million ». *PR Newswire*, Aug 16, 1996 (http://www.infowar.com)

COUNTERINTELLIGENCE OFFICE OF THE DEFENSE INVESTIGATE SERVICE. « Technology collection trends in the US defense industry », *Working Paper*, 1996. (http://www.infowar.com)

CROCK Stan. « Le renseignement économique gagne les Etats-Unis », *Courrier International*, n°319, 12-18 décembre 1996, p 29.

FEDERAL BUREAU OF INVESTIGATION - NATIONAL COMPUTER CRIME SQUAD (NCCS). *Computer fraud and abuse act*. 1996. (http://fbi.gov/nccs)

Frachon Alain « Paris s'efforce d'éviter une crise diplomatique ». *Le Monde*, 24 février 1995, p3.

FRACHON Alain « Paris dénonce l'espionnage de la CIA en France : les secrets d'une guerre économique entre alliés ». *Le Monde*, 23 février 1995, p9.

GUISNEL Jean. « La guerre mondiale de l'espionnage économique ». *Capital*, février 1995, pp 56-68.

GUISNEL Jean. « Internet et l'espionnage économique ». Extraits de *Guerres dans le cyberspace.* Paris : La Découverte, 1995. (http://www.liberation.fr/arc_mult/guisnel)

INCIYAN Evin. « La CNCIS autorise le gouvernement à multiplier les écoutes administratives ». *Le Monde*, 18 avril 1997, p9.

ISNARD Jacques. « La France cherche à mieux lutter contre les formes modernes de l'espionnage », *Le Monde*, 1 mars 1995, p8.

JOHANNES F. « Ecoutes sauvages sous surveillance ». *Libération*, 17 avril 1997, p11.

KENNEDY David. « Top German prosecutor warns firms about espionage ». November 14, 1996. Article sent to Infowar.com. (http://www.infowar.com)

LETEISSIER Ivan. « Les détectives à l'assaut des entreprises ». *L'Entreprise*, n°131, septembre 1996, pp 80-83.

PLENEL E. « L'ambassade des Etats-Unis a été fermement invitée à rapatrier 5 ressortissants américains ». *Le Monde*, 23 février 1995, p9.

RICARD Philippe. « Un compromis met fin à l'affaire López entre General Motors et Volkswagen ». *Le Monde*, 11 janvier 1997, p21.

RICARD Philippe. « Des pièces à conviction auraient été fabriquées pour nuire à Volkswagen dans l'affaire López ». *Le Monde*, 21 mai 1994, p19.

SAVEROT Denis. « Comment espionner vos concurrents sur Internet ». *Capital*, octobre 1996, p 140.

SCARAMUZZINO B. « Quand l'espionnage ne fait pas rire ». *Carrière Commerciale.* n°8, 17 avril-1er mai 1986, pp 26-27.

SCHWARZ Harold. « Les entreprises allemandes ouvertes aux espions », *Courrier International*, n°319, 12-18 décembre 1996, p 28.

SERVICE CANADIEN DU RENSEIGNEMENT DE SECURITE. *Rapport Public 1993.* (http://www.csis-scrs.gc.ca/fra/public)

TREAN Claire « L'affaire de l'espionnage américain en France : le Quai d'Orsay stigmatise la divulgation de l'affaire à la presse ». *Le Monde*, 25 février 1995, p3.

WOLF Frank. « French intelligence shopping list of American high technology secrets ». *DEST Collection Plan : Memorandum*. Central Intelligence Agency, 1996 (http://www.infowar.com)

ZECCHINI Laurent. « Washington et Paris se refusent à une surenchère à propos de l'espionnage américain en France ». *Le Monde*, 25 février 1995, p3.

ZECCHINI Laurent. « Volkswagen porte plainte contre General Motors dans l'affaire López ». *Le Monde*, 14 mai 1995, p19.

REFERENCES SE RAPPORTANT AU CHAPITRE 3

- Ouvrages

BOUJU André. *Les actions en contrefaçons de brevets dans le monde*. Jupiter Précis. Paris : EJA, 1989. 385p.

CHEVALLIER Robert. *La propriété industrielle : protection des inventions, marques et modèles.* collection Entreprise Moderne d'Edition, Paris : ESF, 1992. 150p.

I.N.P.I. *Le brevet : protéger son invention*. Publication de l'Institut National de la Propriété Intellectuelle, Paris. 1996.

I.N.P.I. *Protéger sa marque*. Publication de l'Institut National de la Propriété Intellectuelle, Paris. 1996.

I.N.P.I. *Protéger ses dessins ou ses modèles.* Publication de l'Institut National de la Propriété Intellectuelle, Paris. 1996.

- Articles

AGEDE Pierre. « Protégez vos marques et vos produits ». *L'Entreprise*, n°128, mai 1996, pp 32-34.

AGEDE Pierre. « La meilleure défense : l'attaque ». *L'Entreprise*, n°128, mai 1996, pp 37-41.

BOUTAULT Jacques. « Des solutions pour éviter le piratage », *L'Exportation*, n°36, juin 1987, pp 36-39.

CALVO J., COURET A. « La protection des savoir-faire de l'entreprise ». *Revue Française de Gestion*. sept-oct 1995, pp 95-107.

COLLOMB Florentin. « Des entreprises entre méfiance et paranoïa ». *L'Expansion*, 23 nov-6 dec 1995, n°513, pp 73-74.

COUNTERINTELLIGENCE OFFICE OF THE DEFENSE INVESTIGATE SERVICE. « Industry CI trends ». Working Paper, December 26, 1996. (http://www.infowar.com)

GUISNEL Jean. « Les entreprises doivent apprendre à se protéger ». Entretien avec Pierre Lacoste. *Capital*, février 1995, p 68.

NATIONAL COUNTERINTELLIGENCE CENTER.
« Counterintelligence News and Developements : news, trends, and analysis on CI and security issues ». Vol 4, November 1996 (http://www.infowar.com)

OFFICE EUROPEEN DES BREVETS.
Rapport annuel 1995. Extraits. (http://www.epo. co.at/epo)

PIOTRAUT J-L. « Vos secrets sont-ils bien gardés ? ». *L'Entreprise*, n°120, octobre 1995, pp 43-45.

PONCELET Pascale. « Brevet ou Secret ». *L'Entreprise*, n°128, mai 1996, pp 42-51.

SOL Selena. « Intellectual Property in the Information Era ». (http://www.infowar.com)

WARUSFEL Bertrand. « Intelligence économique et sécurité de l'entreprise », *Problèmes Economiques*, n°2497, 4 décembre 1996, pp 1-7.

REFERENCES GENERALES SE RAPPORTANT AUX TROIS CHAPITRES

- Ouvrages

ESSAMBERT Bernard. *La guerre économique mondiale*. Paris : Olivier Orban, 1991. 247p.

HARBULOT Christian. *La machine de guerre économique* : Etats-Unis, Japon, Europe. Paris : Economica, 1992. 163p.

MARTINET B. MARTI Y-M. *L'Intelligence économique : les yeux et les oreilles de l'entreprise*. Paris : Les éditions d'organisation, 1995. 244p.

VANDENBUSSCHE Corine. *Secret des affaires et informatique*. Thèse pour le doctorat de droit : Université Paris 1 – Panthéon -Sorbonne, 1990. 282p.

VILLAIN Jacques. *L'entreprise aux aguets : information, surveillance de l'environnement, propriété et protection industrielles, espionnage et contre-espionnage au service de la compétitivité.* Coll : Le nouvel ordre économique. Paris : Masson ;1990. 192p.

- Articles

CONGRESS OF THE U.S.A. *Industrial espionage act of 1996*. 2nde Session, 104th Congress. (http://www.infowar.com)

CONGRESS OF THE U.S.A. *Foreign economic collection and industrial espionage.* Annual report to Congress, May 1996. (http://www.infowar.com)

VENZKE Ben N. « Economic/industrial espionage ». *Intelligence watch report*. 1996. (http://www.infowar.com)

TABLE DES MATIERES