Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉCONOMIE
DE L'INDUSTRIE
ET DE L'EMPLOI

MINISTÈRE DU BUDGET
DES COMPTES PUBLICS
ET DE LA FONCTION
PUBLIQUE

Guide des bonnes pratiques en matière d'intelligence économique

Février 2009

PREAMBULE

L'information économique est abondante, voire excessivement abondante. Rechercher des données sur des marchés, suivre ses clients, se faire une idée de la stratégie de ses concurrents, vérifier que l'on est en phase avec ses partenaires, anticiper les évolutions technologiques, suivre l'élaboration d'une norme… autant d'enjeux qui sont au cœur de tout projet d'entreprise, quel que soit le domaine d'activité et indépendamment de la taille. Mais face à cette profusion, facilitée par le développement accéléré d'Internet et ses applications, par où commencer ? Comment trouver, organiser, diffuser l'information utile, celle qui donne un avantage comparatif à l'entreprise ? Comment vérifier sa qualité, valider son contenu, faire en sorte qu'elle arrive au bon destinataire et qu'il en perçoive le sens ? Comment veiller à ce que l'on écrit soi-même dans ses publications, sur son site web, ou ce que l'on explique à un interlocuteur, ne soient pas une source d'informations précieuses dont la communication est préjudiciable à l'avantage que l'on veut acquérir ou du moins préserver ? Comment identifier et protéger ses vulnérabilités ?

L'intelligence économique a pour objet de répondre à ces besoins. Elle est aujourd'hui aussi indispensable aux entreprises que l'a été le marketing il y a 50 ans. Il ne s'agit pas d'une matière obscure, réservée aux initiés, ni d'un prétexte pour des pratiques douteuses, mais bien d'une méthode qui permet d'affronter le jeu de la concurrence. L'objet de ce guide est de présenter cette méthode.

Le Service de Coordination à l'Intelligence Economique (SCIE), rattaché aux ministères de l'Economie et du Budget, a souhaité aider les acteurs économiques, entreprises, associations et syndicats professionnels, chambres consulaires, agences de développement… à appréhender concrètement et simplement cette démarche.

Les turbulences qui bouleversent l'économie internationale vont changer la donne dans de nombreux domaines. S'y préparer, savoir réunir l'information qui transmet les bons signaux sont nécessaires. Le présent référentiel de bonnes pratiques vient apporter sa contribution à cette prise de conscience. Il est libre de droit et destiné à être largement diffusé par voie électronique auprès des entreprises. Fruit d'un travail collectif, il se compose d'une série de fiches brèves assorties de conseils pratiques et d'adresses. De nombreuses références renvoient à des travaux antérieurs menés sur l'intelligence économique, en France et en Suisse francophone.

J'espère que ce guide aidera les responsables d'entreprise, au premier rang desquels ceux des PME, ainsi que les formateurs, dans leur démarche.

Selon le mot, d'Abraham Lincoln, « Les dogmes du passé paisible sont inadaptés au présent tempétueux. Puisque nous sommes confrontés à du neuf, nous devons penser et agir neuf ».

Le Coordonnateur Ministériel
à l'Intelligence Economique

Cyril Bouyeure

SOMMAIRE

Ce guide a été réalisé par Sylvie Domenech, Manuel Marciaux et Dominique Charnassé.

POURQUOI METTRE EN ŒUVRE UNE DEMARCHE D'INTELLIGENCE ECONOMIQUE DANS L'ENTREPRISE ?

Enjeu :

C'est en raison de plusieurs évolutions majeures du contexte économique que le concept d'intelligence économique a émergé au début des années 1990 :

- la première est la mondialisation des échanges qui a placé les entreprises dans une situation de concurrence internationale accrue, contexte souvent qualifié de « guerre économique » ;
- la seconde vient du développement exponentiel des nouvelles technologies de l'information et de la communication et de l'émergence de l'ère numérique. L'information est devenue plus abondante, plus accessible et aussi une matière première stratégique que les entreprises doivent savoir maîtriser pour en tirer un avantage concurrentiel ;
- l'ouverture généralisée des marchés, le rattrapage engagé par les pays émergents a fait apparaître de nouveaux concurrents y compris au stade de la recherche et de l'innovation technologique.

Face aux nouveaux défis, les entreprises, y compris les PME, doivent s'adapter et intégrer l'intelligence économique à leur stratégie, pour accroitre leur compétitivité tout en protégeant leur savoir faire.

Comment ?

1. L'information constitue un élément de compétitivité de l'entreprise

Le chef d'entreprise a besoin d'information concernant ses activités pour :

- **Connaître son positionnement sur le marché**

Exemple : une entreprise de production de protections électriques.

Les enjeux stratégiques : surveiller l'apparition d'une technologie de substitution, rester technologiquement leader et suivre les marchés à venir.

Actions : veille sur les brevets, publications scientifiques, colloques et salons.

Résultats : identification des solutions concurrentes et applications nouvelles, opportunités de nouveaux produits. A terme, développement de nouveaux produits pour préserver sa position de leader.

- **Identifier ses forces et ses faiblesses** (importance quantitative et quantitative de la concurrence)
- **Détecter les opportunités**
- **Gérer la stratégie de développement de l'entreprise**

Exemple : une entreprise de mécanique

Enjeux stratégiques : défendre la performance commerciale de l'entreprise sur des marchés très concurrentiels, assurer la croissance de l'entreprise et le déploiement sur de nouveaux marchés.

Actions : construction d'une méthode de veille commerciale et de valorisation de l'information disponible au sein de l'entreprise, formation d'un pilote au sein de l'entreprise. Sécurisation du système d'information.

Résultats : meilleure connaissance de la concurrence et des marchés, identification et aide à la hiérarchisation d'opportunités commerciales (prospection, applications nouvelles), amélioration de la remontée d'information sur la concurrence et les attentes des clients.

- **Lancement de nouveaux produits et services**

Exemple : une société innovante dans le domaine des lasers médicaux a adopté une démarche d'intelligence économique. Ainsi, à partir d'une action de veille, cette société a pu identifier et approcher certains secteurs de la chirurgie esthétique afin d'être en mesure de concevoir une nouvelle offre. La stimulation de l'innovation suppose également l'élaboration d'une stratégie de propriété industrielle. En outre, le degré très sensible de ses technologies l'a conduit à prendre des contacts fréquents avec des services spécialisés de l'Etat.

- **S'implanter sur de nouveaux marchés**

L'entreprise doit s'informer sur le dispositif de soutien aux entreprises pour le commerce extérieur (portail « Bercy au service des entreprises », site Ubifrance, site Cap sur l'export). Ainsi, une nouvelle convention triennale 2009/2011 d'objectifs et de moyens a été signée récemment entre l'Etat (DGTPE) et Ubifrance (Agence française pour le développement international des entreprises).

L'entreprise doit se familiariser avec les formalités réglementaires requises à l'importation ou à l'exportation en provenance ou en direction des pays clients ou fournisseurs.

Exemple : une entreprise met en place une procédure adaptée de dédouanement.

Enjeux stratégiques : bénéficier d'un dédouanement garantissant souplesse, gain de temps et réactivité ; améliorer la stratégie commerciale et tarifaire ; améliorer la trésorerie et renforcer la compétitivité ; optimiser la situation de votre entreprise à l'international.

Actions : mise en place d'une procédure de dédouanement à domicile (PDD) ; signature d'une convention relative à la télé procédure Delt@ ; aide à l'entreprise dans la classification des marchandises au moyen du renseignement tarifaire contraignant (RTC) ; proposition de régimes douaniers économiques.

Résultats : obtention plus rapide du « bon à enlever » (BAE), importation de produits non communautaires en suspension de droits de douane et de TVA, stockage, utilisation ou transformation de ces marchandises hors taxes.

- **S'adapter aux évolutions de l'environnement de l'entreprise** (concurrence, législation, normes, modes de consommation …)
- **Nouer des coopérations et partenariats**

Exemples : l'adhésion et la participation à la mise en œuvre de projets labellisés au sein des pôles de compétitivité ; développement d'une coopération scientifique, technologique ou commerciale avec des entreprises ou des pôles de compétitivité français ou des « clusters » étrangers.

- **Accroître son influence**

L'information peut aussi être utilisée comme levier d'action permettant de promouvoir les intérêts de l'entreprise dans un cadre légal (lobbying, communication d'influence, utilisation d'internet …). Inversement, celle-ci doit demeurer vigilante face à l'emploi à son détriment de ces méthodes, rumeurs, voire même le recours à des procédés illégaux comme la désinformation.

2. L'information est également un élément de sécurité de l'entreprise

La sécurité de l'information est capitale pour le développement et la pérennité de l'entreprise. L'amélioration de la protection physique et logique de leur environnement nécessite la mise en œuvre de méthodes éprouvées et l'affectation de moyens humains, financiers et techniques. Si la situation au sein des entreprises françaises s'est nettement améliorée au cours de la dernière décennie, des marges importantes de progrès restent encore à réaliser : dans son édition 2008 des « menaces informatiques et pratiques de la sécurité en France », le Club de la sécurité de l'information (CLUSIF) révèle que 73% des entreprises de moins de 200 salariés consultées estiment lourde de conséquence une impossibilité de moins de 24 heures de leurs outils informatiques (voir également l'étude du CREDOC, « La diffusion des technologies de l'information et de la communication dans la société française », 2008). L'entreprise doit savoir communiquer tout en sécurisant son patrimoine informationnel pour :

- **Travailler en toute confiance avec ses collaborateurs dans l'entreprise, et à l'extérieur avec ses partenaires**

Cet objectif suppose de mettre en place un ensemble de dispositifs et procédures techniques, administratives, juridiques qui forment la politique de sécurité de l'entreprise :

- inventorier les risques et les menaces potentielles ;

- protéger le système informatique et les données sensibles (nomination d'un responsable « système d'information », charte informatique, contrôle d'accès, actualisation des logiciels, sensibilisation du personnel …)**.** Le système d'information de l'entreprise est vital, car il structure l'ensemble des aspects de son activité (comptabilité, paye, achats, fichiers clients et fournisseurs, factures, prospects, nouveaux produits, contacts avec les partenaires …) ;
- mettre en place des moyen matériels de protection adéquats ;
- introduire des clauses de confidentialité dans les contrats de travail : « grâce à ses anciens droits d'accès, il était chez nous comme chez lui, alors même qu'il était passé à la concurrence depuis six mois … » ;
- établir un plan de continuité d'activité (en cas de dysfonctionnement grave ou de situation de crise) ;
- évaluer régulièrement le dispositif mis en place.

➢ **Communiquer clairement et avec cohérence sur son activité, ses projets, sa stratégie**

➢ **Etre en capacité de se défendre contre des concurrents utilisant des méthodes déloyales** (Piratage d'informations, espionnage économique, contrefaçons …)

Exemple : « … depuis des semaines, un inconnu circulait dans les différents services de l'entreprise sans être inquiété en se faisant passer pour un salarié du laboratoire … » ; « … des attaques modifient la présentation et le contenu du site de l'entreprise ou en bloquent l'accès, celle-ci perdant la confiance de certains clients … ».

En cas d'agression, il faut impérativement porter plainte.

L'entreprise doit définir et mettre en œuvre une politique d'intelligence économique pour maîtriser, protéger ses activités et en assurer la pérennité. L'application d'une telle démarche nécessite d'établir des liens avec les fiches suivantes du guide :

Sites et documents de référence : site du HRIE : www.intelligence-economique.gouv.fr // Site régional Poitou-Charentes : www.ie-poitou-charentes.fr/?tg=oml&file=articles.ovml&ecran=3&article=135 // Guide pratique de mise en place d'une démarche d'intelligence économique pour les PME (www.cher.cci.fr) // ACFCI : www.acfci.cci.fr/innovation/proprieteintellectuelle.htm // Petit manuel d'intelligence économique au quotidien, Pierre Mongin, Franck Tognini, DUNOD, 2006

L'ORGANISATION DE L'INTELLIGENCE ECONOMIQUE DANS L'ENTREPRISE

Enjeu :

L'intelligence économique est une démarche qui concerne toutes les entreprises. En effet, quelle que soit sa taille, une entreprise doit pérenniser son activité en protégeant certaines informations parce qu'elles sont sensibles (savoir-faire, fichiers clients…), être attentive aux initiatives de ses concurrents, aux attentes de ses partenaires et de ses clients, être réactive en veillant à ce que les informations utiles parviennent aux décideurs…

Si le facteur « taille » n'a pas d'influence sur la nécessité de mettre en place une démarche d'intelligence économique dans l'entreprise, il jouera en revanche sur la façon dont va s'organiser l'IE dans l'entreprise et les moyens qui y seront alloués.

Comment ?

On peut distinguer trois modèles d'organisation de l'intelligence économique en entreprise.

1. L'intelligence économique est confiée à un responsable spécialisé au sein de l'entreprise.

L'entreprise s'est dotée d'une équipe spécialisée et dirigée par un responsable à l'intelligence économique, rattaché à la direction générale ou à la direction de la stratégie. L'équipe est composée d'informaticiens, d'analystes des risques, de spécialistes de la veille… Ce schéma correspond aux entreprises disposant de ressources humaines et financières conséquentes.

2. L'intelligence économique est confiée à une personne ayant d'autres responsabilités au sein de l'entreprise.

L'intelligence économique est une activité confiée à l'un des collaborateurs placée à la tête de l'une des unités opérationnelles de l'entreprise (Directeur international, Directeur des Systèmes Informatiques…).

La personne chargée de cette mission occupe des fonctions transversales dans l'entreprise et est rattachée, à ce titre, à la direction générale.

3. Le schéma type dans les PME.

Beaucoup d'entreprises appliquent, sans en avoir nécessairement conscience, des démarches partielles d'intelligence économique. La pratique de l'intelligence économique est alors morcelée, non structurée et partagée par plusieurs collaborateurs sans que la circulation de l'information soit organisée.

La mise en place d'une démarche d'intelligence économique dans les PME, c'est-à-dire la mise en place d'une stratégie organisée et efficace, relève souvent directement des dirigeants. La fonction peut toutefois, selon la taille de l'entreprise, être partagée entre plusieurs responsables ; dans ce dernier cas (fonction d'intelligence économique répartie), l'une des personnes peut être désignée comme étant l'animateur du groupe.

Avec des moyens limités, la PME pourra procéder progressivement à la mise en place de la démarche d'intelligence économique (l'identification et la hiérarchisation initiales des besoins est par conséquent une étape importante) et pourra se faire accompagner par les acteurs publics spécialisés à l'échelon régional en matière d'intelligence économique (notamment les chargés de mission régionaux à l'intelligence économique et les chambres de commerce et d'industrie ; Voir fiche intitulée « Le dispositif public d'intelligence économique »).

Les PME ayant des intérêts communs peuvent également se regrouper pour partager et mutualiser certaines informations, dont elles ne pourraient pas disposer individuellement, ou pour bénéficier de la mise en place d'une démarche globale d'intelligence économique. Cette approche est celle que l'on observe dans beaucoup de pôles de compétitivité.

Sites et documents de référence : Intelligence économique : un guide pour débutants et praticiens, Coordination : IDETRA, 2002 // **«** Petit manuel d'intelligence économique au quotidien, Pierre Mongin, Franck Tognini, DUNOD, 2006.

ENJEUX STRATEGIQUES ET BESOIN EN INFORMATION DE L'ENTREPRISE

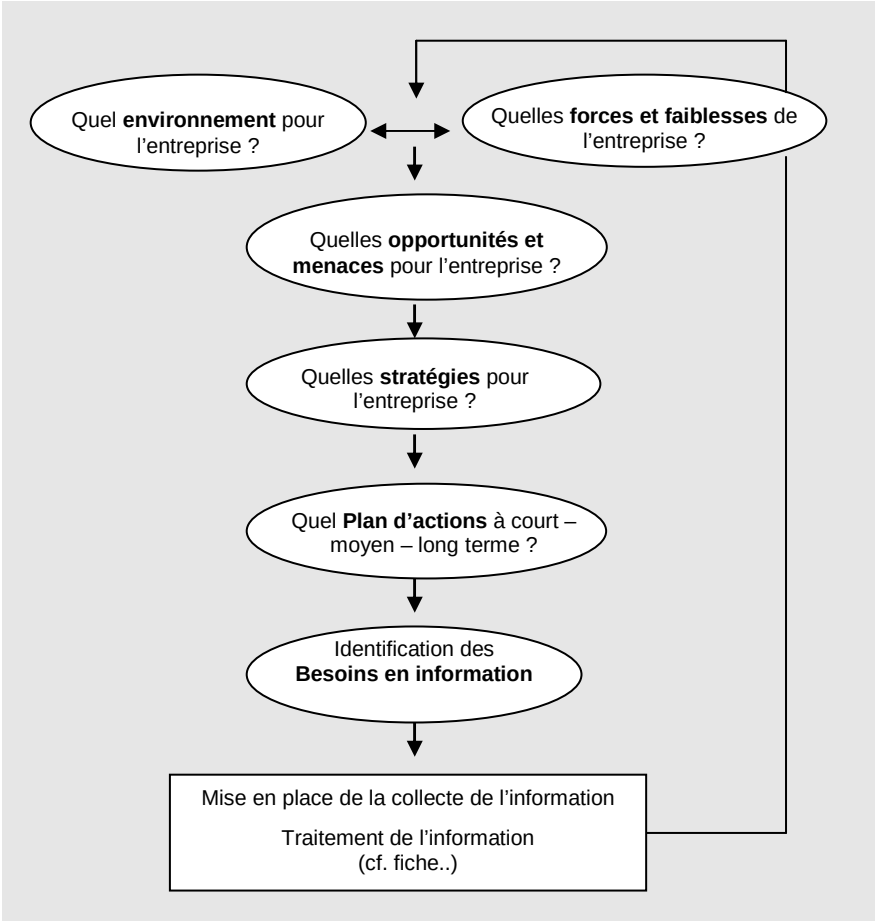
Enjeu :

La pléthore d'informations est un frein plus qu'une contribution réelle à la prise de décision. Afin de pallier ce risque et la perte de temps associée, il est indispensable pour l'entreprise de définir en amont quels sont précisément ses besoins en information.

Cette étape implique que ***l'entreprise mène une véritable réflexion sur les principaux aspects de son activité et les objectifs qu'elle souhaite atteindre.*** Ce n'est pas de la collecte d'informations que doit découler la définition des axes stratégiques mais bien le contraire.

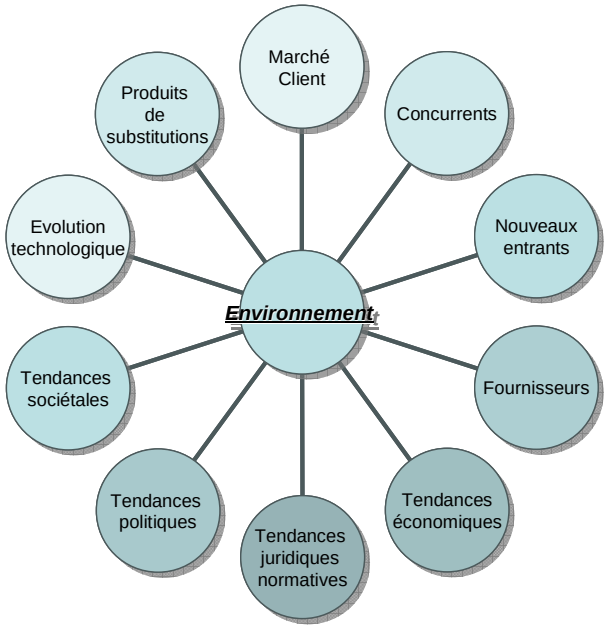
La détermination des besoins en information passe par l'identification des enjeux à long, moyen et court terme.

Comment ?



Le processus d'identification des besoins en information est un ***processus itératif***, c'est-à-dire qu'il est permanent et suppose la possibilité de remise en cause. En effet, il convient de vérifier périodiquement si les hypothèses d'analyse de l'environnement varient et quel est leur impact sur le positionnement de l'entreprise. Parallèlement, le traitement des informations collectées va modifier la perception de l'entreprise et potentiellement amener de nouveaux besoins en information.

Analyse de l'environnement de l'entreprise



- Avez-vous une vision précise de vos concurrents sur votre marché ? (identité – taille et rentabilité - positionnement produits – présence à l'international - axes de développement – partenariats existants – nouveaux acteurs …)

- Avez-vous une connaissance suffisante des évolutions technologiques de votre secteur ? (degré d'importance de la maîtrise technologique - probabilité d'apparition de nouvelles technologies…)

- Avez-vous identifié les principaux facteurs d'influence du comportement de vos clients et du marché dans sa globalité (marché domestique, à l'international)

- Connaissez-vous les grandes tendances économiques, sociétales, législatives, réglementaires… ***susceptibles d'avoir une influence sur la croissance de votre secteur d'activité ?***

……

OBJECTIF ⇨ **Retenir 3 à 4 axes déterminants pour le développement de l'entreprise**

Positionnement de l'entreprise dans son environnement avec ses forces et faiblesses

Quelle est votre vision à long terme (+ de 3 ans) pour l'entreprise ?
Quelles sont les actions à mettre en œuvre à court terme pour atteindre les objectifs ?
Disposez-vous des compétences nécessaires (forces, faiblesses, vulnérabilités) et quelles sont les connaissances à acquérir ou renforcer pour réaliser votre projet ?

⇩

Deux types de besoins d'informations :

- ***Besoins en information permanents*** pour permettre à l'entreprise de surveiller l'environnement du marché (par exemple, *Quelle va être l'évolution technologique de mon marché en France et sur le marché européen ?)* et qui vont contribuer à la réalisation des objectifs de long terme
- ***Besoins en information ponctuels*** pour répondre à une question ponctuelle qui se pose pour mettre en œuvre les axes stratégiques (par exemple, *Quels sont les partenaires qui peuvent m'accompagner dans le développement de ma nouvelle technologie* ?)

  Ce type de besoin peut survenir également pour la résolution de problèmes nouveaux mis en exergue par la veille sur les enjeux stratégiques de l'entreprise ou a contrario suite à une absence d'anticipation du phénomène.

⇩

Hiérarchisation des besoins en fonction de leur importance pour la compétitivité de l'entreprise, de leur caractère d'urgence ou des moyens de l'entreprise

Communiquer en interne sur les besoins en information de l'entreprise afin de favoriser sa collecte et son traitement par les collaborateurs (réseau commercial notamment)

Sites et documents de référence : matrices d'analyse stratégique : swot (forces-faiblesses et opportunités- menaces) – 5 forces de Porter – Pestel (analyse de l'environnement) // Renseignement et Intelligence économique – Franck Bulinge (http://cerad.canalblog.com) // Intelligence économique : un guide pour débutants et praticiens, Coordination : IDETRA, 2002 // Bonnes pratiques en matière d'Intelligence économique, Guide pratique et découverte, CRCI Lorraine, 2002 + autodiagnostic démarche d'intelligence économique (www.lorraine.cci.fr/autodiagnostic)

COLLECTE DE L'INFORMATION

Enjeu :

Etape préliminaire indispensable, la définition des objectifs stratégiques à moyen-long terme permet à l'entreprise de définir précisément ses besoins en information et de s'engager dans le processus de collecte.

De la qualité et de la fiabilité des informations collectées dépendra la valeur ajoutée apportée au processus de décision de l'entreprise en permettant en outre d'éviter les écueils de la surinformation ou de la désinformation. La collecte de l'information doit être appréhendée sur le long terme comme un processus structuré, systématique mais également évolutif capable de prendre en compte l'émergence de nouveaux besoins.

Le recueil d'informations doit impliquer les salariés qui devront être sensibilisés aux enjeux stratégiques de l'entreprise et de ses besoins. L'efficacité de la veille passe par le partage des informations. Néanmoins, en interne comme à l'extérieur, le chef d'entreprise devra veiller à conserver le caractère confidentiel de certaines de ses recherches.

Comment ?

1. Formalisation des axes de recherche de l'information

En fonction de l'identification des besoins (cf. fiche 2 - Enjeux stratégiques et besoin en information de l'entreprise), il est maintenant nécessaire de traduire ces demandes d'information en thèmes et en questions clairs et précis, si possible triés et classés en fonction des différentes sources d'informations sollicitées et de définir les terminologies et mots clés.

2. Identification des sources d'information fiables et pertinentes adaptées aux moyens et problématiques de l'entreprise

- Quelles sont les sources d'information en interne ?

Les sources internes

- **Les documents internes :** tableaux de bord, documents de gestion, guides de procédure interne, compte rendu de réunion, de visites, études marketing, rapports du service après-vente, rapports d'étonnement, les bilans et pièces comptables …
- **Les fichiers :** clients, fournisseurs, prospects …
- **Le traitement des demandes externes :** courriers et courriels reçus, Interrogation du site Web de l'entreprise, CV transmis …
- **Les personnels :** commerciaux, acheteurs, responsable développement, production, responsable SAV, etc.

- Quelles sont les sources d'information externes ?

Les sources externes

- **Les clients** (leurs attentes, leur réclamation…)
- **Internet :** presse généraliste et spécialisée en ligne, sites internet des clients et fournisseurs - forums et blogs (avis d'experts, de consommateurs..), bases de données gratuites ou payantes (technologie, économique et financière…), thèses, réseaux sociaux sur Internet…
- **Les fournisseurs d'information :** presse, centres de documentation, bases de données structurées, courtiers en information…
- **Les partenaires :** fournisseurs, sous-traitants, financiers…
- **Les institutions :** administrations, réseaux consulaires, organisations professionnelles…
- **Les réseaux personnels** : clubs, associations
- **Les manifestations** : colloques, salons (www.salons-online.com / www.expobase.com), voyages…
- **Les experts** : centres techniques, consultants privés…
- **Les documents des concurrents** : plaquettes publicitaires, rapports d'activité, communiqués de presse
- **Les sources fortuites** : lieux publics

! Evaluation et Vérification de la fiabilité des sources d'informations notamment sur le net

Exactitude des informations

L'auteur (Qui est-il ? – Est-il indépendant ? Est-il crédible ?)

Ligne éditoriale du site …

Outils gratuits pour l'identification des sources d'information sur Internet :

- Les Moteurs : Google – Yahoo ! – Exalead – Kartoo …
- Les Méta-moteurs (recherche simultanée sur plusieurs moteurs) : Polymeta – Clusty – Ixquick …
- Les bases de données gratuites ou payantes : Espacenet (brevets),...
- Les annuaires (informations regroupées par thèmes) : Yahoo !, Dmoz…
- Les agrégateurs de sites d'actualité (presse, blogs…) : Google Actualités, Yahoo ! News, Wikio,

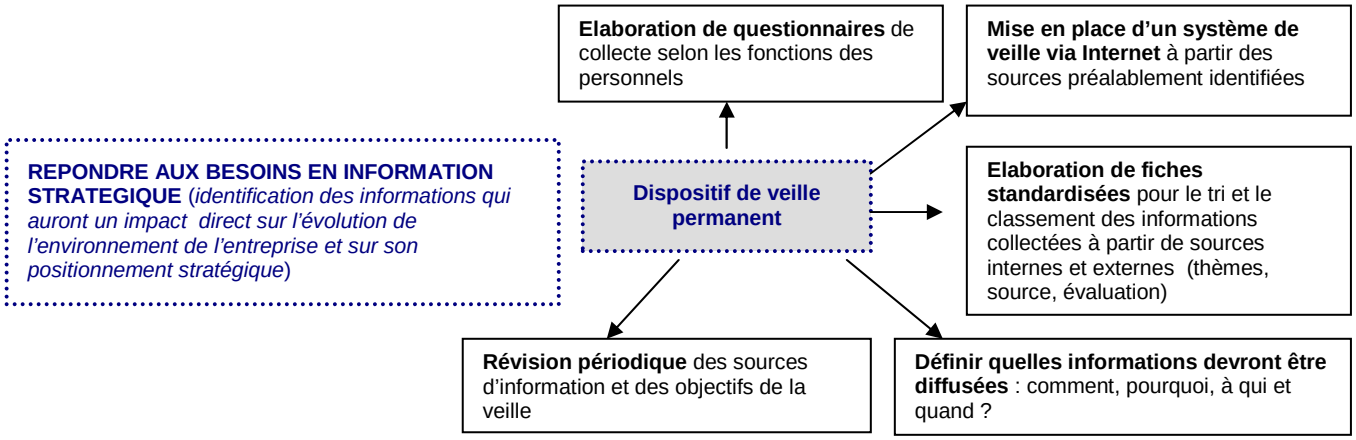
3. Organiser la collecte d'informations

- ***Implication forte du chef d'entreprise*** qui aura la fonction de coordinateur de la collecte
- Désigner une personne responsable de la collecte – lui ***allouer du temps*** pour mener le projet
- ***Evaluer le coût*** de la recherche et l'adapter aux capacités de l'entreprise
- Faire ou Faire faire ? (arbitrage compétences disponibles, coût, confidentialité des informations recherchées)

- Sensibilisation des salariés à la collecte d'information
  - ⇨ Expliciter les enjeux à court moyen et long terme de l'entreprise
  - ⇨ Expliciter les objectifs et les résultats attendus de la collecte
  - ⇨ Fixer des objectifs précis aux salariés impliqués selon leurs compétences et leur fonction dans l'entreprise
  - ⇨ Développer une culture de la collecte d'information (*capacité à s'interroger, valorisation de la participation au recueil et au partage de l'information- favoriser les retours d'expérience*) et expliquer les règles déontologiques (*cf. fiche 13 – cadre juridique de la collecte d'informations*)

- Quel type de dispositif mettre en place ?

Chaque entreprise doit mettre en place son propre dispositif adapté à sa taille, à sa structure, au nombre de ses salariés impliqués dans la démarche, ses circuits d'information, sa culture. Il n'y a pas d'organisation type mais un minimum d'organisation s'impose.



- Quels outils pour la mise en place d'une surveillance permanente ?
  - Les flux Rss : S'informer de l'actualité sur les sites sélectionnés sans avoir à se connecter en utilisant des lecteurs de flux Rss (Netvibes, iGoogle, AlertInfo…)
  - Les agents d'alerte : Détection de changements sur une page web ordinaire (outils gratuits : Newzie, extensions de Mozilla Firefox ; outils payants pour des budgets de quelques dizaines à quelques milliers d'euros : Copernic Tracker, Website Watcher, KB Crawl, QWAM,… et bien d'autres)
  - Les alertes : Recherche à partir de mots clés (Google Alertes)
  - Les newsletters

4. Collecte d'informations et confidentialité

- Pour les sujets particulièrement sensibles à diffusion restreinte, limiter le nombre de collaborateurs impliqués dans la collecte.

- Etre particulièrement vigilant dans la collecte d'information auprès de sources humaines externes (Sensibilisation permanente des salariés sur les informations qui ne doivent en aucun cas être divulguées même pour obtenir une information en retour – scinder la recherche d'informations en plusieurs sujets et diversifiés les contacts – préparer son entretien en ayant bien pesé à l'avance les questions à poser …)

- Concernant la recherche d'informations sur Internet : utiliser une connexion banalisée (abonnement à un fournisseur d'accès internet grand public) – supprimer régulièrement les cookies de votre ordinateur – déconnecter la messagerie…

➢ **Sites et documents de référence :**

Pour plus d'informations sur les outils de recherche :
http://www.adbs.fr // http://c.asselin.free.fr // http://www.crvs.fr/tikiwiki/tiki-index.php?page=Veille - sur les outils payants : http://guideie.gfii.asso.fr/guide_ie.php / http://outils.veille.inist.fr/

Pour plus d'informations sur la collecte d'information : http://www.arist.ccip.fr // Guide pratique de mise en place d'une démarche d'intelligence économique pour les PME, CCI du Cher, 2008 (www.cher.cci.fr) // www.benchmarkie.com Intelligence économique : guide pratique pour les PME Suisse Normande, HEG Genève, 2008

EXPLOITATION ET CAPITALISATION DE L'INFORMATION

Enjeu :

Les informations brutes qui sont collectées (internet, presse, contact direct, téléphone…) ne pourront être exploitées comme instrument d'aide à la décision que si elles ont fait l'objet d'un traitement préalable (validées / organisées, structurées, hiérarchisées…) pour obtenir un produit fini et fiable. C'est cette phase d'exploitation qui donne à l'information et plus généralement à la collecte toute sa valeur ajoutée.

Sans cette étape essentielle, les prises de décision et orientations stratégiques du chef d'entreprise peuvent vite s'avérer difficiles à réaliser (surabondance d'informations brutes non analysées « partant dans tous les sens » parfois incohérentes ou non pertinentes) voire constituer une menace pour les activités et le développement de l'entreprise (mauvaise décision fondée sur des informations incomplètes, erronées, non fiables).

Une fois que l'information brute aura été valorisée, elle devra être capitalisée tout en demeurant accessible et facilement exploitable.

Comment ?

1. Traitement et analyse de l'information collectée

On distingue généralement deux étapes : le traitement puis l'analyse de l'information.

1/ Traitement de l'information	2/ Analyse de l'information
Trier les informations et ne retenir que celles qui sont pertinentes, c'est-à-dire qui correspondent aux besoins d'informations stratégiques qui ont été identifiés en amont de la phase de collecte (éliminer celles qui ne sont pas pertinentes) ; **Valider les informations retenues : évaluer leur exactitude et leur fiabilité** : quelle est la source de l'information ? est-elle crédible ? cette information peut-elle être recoupée ?... Dans la pratique, on peut qualifier les informations en s'aidant d'une échelle d'évaluation (information fiable, peu fiable, non fiable). On peut aussi s'appuyer sur une compétence externe (par exemple, l'appui d'un expert pour des informations très techniques peut se révéler utile voire indispensable).	Il s'agit de **donner du sens** à l'information : - Ne **pas avoir de préjugés** pour ne pas orienter l'analyse sur une mauvaise piste - **Organiser, structurer, hiérarchiser et rapprocher** les informations : toutes ces informations sont elles toutes aussi importantes ? lesquelles sont structurelles ? vont-elles toutes dans le même sens ?… - **Utiliser des outils d'analyse** : analyse SWOT (forces, faiblesses, opportunités, menaces), modèle des cinq forces de Porter… - **Repérer les éventuels signaux faibles** et leur donner une signification - **Interpréter et synthétiser** les principaux résultats de l'analyse : quelle est la tendance ? quels sont les risques ? quels sont les signaux d'évolution de l'environnement... - **Tester** les principaux résultats (auprès d'autres sources, experts…) - **S'interroger** : ai-je en ma possession aujourd'hui de tous les éléments pour prendre une décision ?

Au terme de l'analyse, une nouvelle collecte d'informations peut se révéler nécessaire si les résultats de l'analyse effectuée ne permettent pas de répondre pas aux besoins d'informations stratégiques qui ont été identifiées :

- Les informations sont partielles, mal ciblées, pas actuelles… Les sources de collecte, les outils de collecte des informations… doivent être ajustés ;
- L'analyse a permis d'identifier des besoins d'informations complémentaires qui n'avaient pas été pris en compte initialement.

2. L'information doit être formatée pour qu'elle soit assimilable par la personne à qui elle est destinée et doit être accessible

Les résultats issus de l'analyse sont des outils servant à des prises de décisions stratégiques. Pour cela :

- Il est indispensable que les résultats de l'analyse soient bien compris et assimilés par la personne à qui elle est destinée. A cette fin, il est souhaitable que les résultats de l'analyse s'accompagnent de recommandations simples et claires, d'arguments construits…
- Les décisionnaires doivent pouvoir accéder aux informations issues de l'analyse : la phase de collecte puis d'analyse est un investissement (en temps notamment) et elle doit pouvoir être valorisées par les décisionnaires concernés (pour éviter par exemple qu'un collaborateur ne recherche une information déjà disponible dans l'entreprise) ;
- La conservation des informations dans l'entreprise est indispensable : elles enrichissent le patrimoine informationnel, la connaissance et la mémoire de l'entreprise (au même titre que les comptes rendus de réunions, fichiers clients…). Cette étape est importante car elle permettra de retrouver à tout moment une information pertinente, valorisée et déjà validée ;
- La capitalisation des connaissances sera organisée au sein de l'entreprise par un classement des documents sur des supports papiers ou numériques (classeurs, intranet, base de données, CD-Rom, disque dur…) selon un dispositif d'archivage et stockage efficace c'est-à-dire offrant des avantages sur les plans organisationnel et économique (temps d'accès minimal, coût réduit…) ;
- La classification des documents et leur disponibilité dans l'entreprise prendra en compte le degré de sensibilité des informations qui y sont contenues : par exemple un document d'analyse qui concernent des éléments relatifs à la stratégie de l'entreprise (nouvelles activités, engagement à l'export sur tel ou tel pays…) ne devra être accessible que par le (s) collaborateur (s) proche (s) directement impliqué (s).

Sites et documents de référence : L'intelligence économique, Christian Marcon et Nicolas Moinet, DUNOD, 2006 // L'intelligence économique, François Jakobiak, Editions d'Organisation, 2006 // Intelligence Economique. Un guide pour débutants et praticiens, Coordination : IDETRA, 2002 // Bonnes pratiques en matière d'Intelligence économique, CRCI Lorraine, 2002

VALORISATION DE L'INFORMATION DANS L'ENTREPRISE

Enjeu :

Une fois que l'information a été validée, elle doit être mise à la disposition de ceux qui en ont besoin dans l'entreprise avec un souci de sécurisation.

Dans la mesure où l'acquisition d'informations a un coût (temps passé pour la collecter notamment), que ces informations ont une valeur (maintien d'un avantage concurrentiel, possibilité de gains de parts de marché…), la diffusion au sein de l'entreprise ne doit pas être toujours réservée à quelques « heureux élus», mais elle ne doit pas non plus être réalisée « tous azimuts ».

Pour que chacun puisse toujours avoir accès aux informations nécessaires et utiles pour ses activités, l'information doit être partagée, comprise et facilement accessible.

Comment ?

1. Classification de l'information en fonction de son degré de sensibilité

La **classification** des informations (documents, application métier, messagerie, information non formalisée…) qui seront diffusées dans l'entreprise est nécessaire :

- Elle permet d'éviter que des informations sensibles, confidentielles soient diffusées volontairement ou non à l'extérieur de l'entreprise ce qui pourrait porter préjudice à son activité ;
- Elle permet à l'inverse de ne pas restreindre inutilement l'accès à des informations qui sont ou pourraient être utiles aux collaborateurs dans le cadre de leur travail. La sécurité de l'information est nécessaire, mais il ne faut pas non plus la surprotéger au risque de nuire à l'efficacité de l'activité de l'entreprise.

Classifier les informations revient à affecter un **degré de sensibilité aux informations**. On peut s'appuyer sur des questions simples pour mesurer la sensibilité de telle ou telle information : « cette information, sur mon activité, sur mes projets ou sur mon environnement concurrentiel, est-elle déjà connue de manière générale ou doit-elle rester exclusive » ? « Si mon concurrent prend connaissance aujourd'hui ou demain de telle information, cela me sera-t-il préjudiciable (perte de part de marché par exemple) » ?

Généralement, on classifie la sensibilité des informations internes selon trois niveaux :

- L'information est **générale**, ouverte à l'ensemble du personnel, et en cas de divulgation en dehors de l'entreprise les conséquences sont nulles ou minimes : il s'agit de la majorité des informations (décision interne de procéder au recyclage du papier ou de limiter la cylindrée des automobiles de fonction) ;
- L'information est **restreinte** car sa divulgation peut nuire de façon importante à l'entreprise : la divulgation d'informations concernant les clients par exemple peut se traduire par une perte de confiance de ces derniers et ainsi à terme par des pertes de part de marché au profit de concurrents… ;
- L'information est **strictement confidentielle** car sa divulgation porterait lourdement préjudice à l'entreprise (secrets de fabrication, stratégie de l'entreprise…) : pertes financières élevées, graves atteintes à la notoriété / image de marque de l'entreprise …

Une même information peut être requalifiée au cours du temps : ainsi une information strictement confidentielle (mise au point d'un nouveau procédé, d'une nouvelle technologie) pourra quelques mois plus tard devenir ouverte (après la réalisation de toutes les démarches nécessaires à sa protection par un brevet par exemple).

2. Identification des personnes qui doivent avoir accès à l'information

Pour permettre à son entreprise de fonctionner efficacement (pas de divulgations d'informations sensibles, faire

disposer ses collaborateurs des bonnes informations au bon moment), le chef d'entreprise doit identifier les personnes qui doivent avoir accès aux différentes informations afin de les valoriser au mieux.

En effet, l'accès aux différents types d'information doit être défini car elle peut nuire à l'activité de l'entreprise :

- Surprotéger des informations en les sur-qualifiant de sensibles et ne les divulguer qu'à quelques privilégiés risque de créer un climat de méfiance et peut nuire à l'activité de l'entreprise puisque l'information ne sera pas accessible au collaborateur qui en aura besoin et qui saura la valoriser ;
- De même permettre et encourager un accès large à toutes les informations peut également nuire à l'activité de l'entreprise : outre les risques de fuite d'informations sensibles, la mise à disposition à l'ensemble du personnel d'informations trop nombreuses, inutiles pour leur activité, n'est pas un gage d'efficacité.

Les différents canaux de transmission de l'information peuvent permettre au chef d'entreprise de diffuser vers des personnes identifiées : listes de destinataires prédéfinies dans la messagerie, niveau d'accès informatique restrictif ou non donné aux collaborateurs…

2. Définir les supports de diffusion de l'information.

Les supports sont nombreux et offrent un niveau de partage et de circulation de l'information plus ou moins large :

- Les **réunions :** il convient de définir précisément qui peut et doit y participer, préparer les documents qui y seront diffusés et en préciser le statut (par exemple : peuvent ils circuler au-delà des seuls participants ? Si oui à destination de qui ?). Lorsque la taille de l'entreprise le permet, la tenue régulière de réunions d'information internes permet une bonne circulation de l'information et l'échange d'idées de haut en bas, de bas en haut et également entre les différents services.
- Les **comptes-rendus de visites, rapports de mission** : les destinataires, le degré de confidentialité les modalités de stockage (Où les stocker? Comment : formats papier, numérique ?...), les conditions d'accès aux informations (Qui peut y accéder ?) mais également les conditions de leurs exploitations devront être définis.
- Les **lettres d'information** régulières (*newsletter)* et les **journaux internes :** la politique éditoriale doit être définie préalablement et préciser notamment ce que l'on peut écrire (il convient de prendre en compte la facilité de retransmission qui est associée à ce type de support lorsqu'il est réalisé sous format électronique), qui sont les destinataires, quelle périodicité…
- **La messagerie électronique internet** est un support de diffusion de l'information très utilisé qui présente plusieurs avantages : simplicité d'utilisation, ciblage aisé des destinataires… L'utilisation de ce support doit toutefois s'effectuer dans un cadre sécurisé : utilisation des logiciels et matériels de sécurité (antivirus, anti-spyware, pare-feu, anti-spam…) pour les serveurs et postes informatiques (avec une mise à jour automatique et régulière) et sécurisation des échanges par le chiffrement des données les plus sensibles. Des règles d'usage sont également à prévoir : n'envoyer le courrier électronique qu'aux personnes concernées, le titre du message doit être bref et clair…
- **L'intranet** est un outil qui permet de diffuser et de partager de l'information au sein de l'entreprise : mise à disposition du personnel de tout type de documents, accès centralisé d'informations parfois dispersées dans différents services de l'entreprise (capitalisation des connaissances et mémoire de l'entreprise), possibilité de mise en place de forums… Comme pour la messagerie, ce support doit être utilisé dans un cadre sécurisé et l'information mise à disposition doit être encadrée (structuration autour de rubriques et espaces clairement définis, mise à disposition d'informations utiles…).

Si les supports de communication de l'information sont nombreux et souvent simples d'utilisation, la circulation et le partage de l'information ne se feront pas sans une réelle implication de la direction de l'entreprise (développer la culture du « feed back », création d'occasions pour échanger…). Au-delà du contenant, les informations doivent demeurer simples, claires, compréhensibles et facilement comprises par le personnel pour être efficaces.

Sites et documents de référence : Intelligence Economique. Un guide pour débutants et praticiens, Coordination : IDETRA, 2002 // Bonnes pratiques en matière d'Intelligence économique, Guide pratique et découverte, CRCI Lorraine, 2002 // Intelligence économique : guide pratique pour les PME Suisse Normande, HEG Genève, 2008

VALORISATION DE L'INFORMATION A L'EXTERIEUR DE L'ENTREPRISE

Enjeu :

Il s'agit d'identifier les contacts et relais auprès desquels l'entreprise pourra mener une action afin de favoriser son développement.

Disposer d'un réseau est indissociable de toute démarche en matière d'intelligence économique. En effet, un réseau permet d'obtenir des informations, de les valoriser ou d'en diffuser tout ou partie en appui du développement de l'entreprise. On peut également s'appuyer utilement sur son réseau afin de mener des activités d'influence ou de lobbying en vue de faire prévaloir les intérêts de son entreprise.

Comment ?

1. Construire et animer son réseau

On distingue plusieurs étapes dans la construction et la vie d'un réseau :

1/ Identifier les membres du réseau →

Quelles sont les personnes susceptibles d'être contactées facilement pour mobiliser, en dehors de l'entreprise, une compétence qui peut être utile ?
Dresser une liste des contacts à chercher du côté de son cursus scolaire, de la vie professionnelle –collègues, anciens clients, banquiers …- et au travers de ses activités associatives, sportives…

2/ Elargir son réseau →

Mon réseau est il suffisamment solide dans le domaine financier ? juridique ? institutionnel ? de la presse ? ...
Le réseau n'est pas figé et évolue avec l'entreprise : il peut s'élargir avec le développement de nouvelles activités, le recours à de nouveaux fournisseurs, le départ en retraite de certains contacts…

3/ Faire vivre son réseau →

Il faut communiquer, diffuser, informer, s'informer... Les moyens écrits (support papier, carte de vœux…), y compris sur support électronique (lettre d'information, site web avec adresse mail…), sont bien connus.
Les sites sociaux sur internet (outils utilisant le web 2.0 comme les blogs, wikis…) peuvent également être utiles mais il faut savoir faire preuve de prudence en ce qui concerne les informations mises en ligne (accessibles par tous durant de nombreuses années) et demeurer conscient de la nature réelle de ses « amis »

Lorsque l'on sollicite son réseau, il faut :

- **S'interroger au préalable sur l'objectif précis** que l'on souhaite atteindre **et sur la formulation de la demande** que l'on va faire (il faut faciliter la tâche du contact –lequel n'a pas nécessairement beaucoup de temps, ne connaît pas la situation…) en lui formulant précisément les attentes et en lui suggérant la façon dont il peut vous aider (sans être trop volontariste, ce qui pourrait avoir un effet contre productif sur votre interlocuteur) ;

- **Veiller à ne dire que ce qui est nécessaire**, c'est-à-dire avoir préparé préalablement son message ;
- **Assurer le suivi** et ne pas hésiter à « relancer » son contact lequel peut avoir oublié la sollicitation, n'a pas eu le temps de la mettre en œuvre…
- Ne pas hésiter à **activer collectivement le réseau** (ne pas toujours agir en bilatéral, d'individu individu) ;
- **Savoir répondre à une sollicitation :** le réseau n'est pas « à sens unique » et, pour qu'il soit durablement viable, il faut « jouer le jeu » en apportant ses compétences, son expertise... à des sollicitations d'autres membres de son réseau, ce qui facilitera leur disponibilité lorsque vous les solliciterez ensuite.

2. Les actions d'influence ou de lobbying

Il s'agit d'agir en amont d'une décision, d'un acte, d'un texte ou de le susciter pour qu'il soit conforme aux intérêts de l'entreprise. La stratégie d'influence peut être menée vis-à-vis d'acteurs publics ou privés. Les actions de lobbying doivent s'exercer dans le strict cadre du respect des lois et règlements (pas de dessous de table…).

Un lobbying performant suppose :

- Une bonne **anticipation** : il faut devancer l'acte (par exemple : connaître les modifications de réglementations ou de normes à venir qui pourraient affecter l'activité de l'entreprise ; évolution de la stratégie d'un client) et agir le plus en amont pour intervenir le plus efficacement ;
- Une **bonne connaissance de la situation** (positions des uns et des autres, les soutiens dont ils disposent, arguments, délais…), des processus de décision, des personnes influentes ;
- De **forger une stratégie** (quelles étapes pour atteindre l'objectif ? quels moyens mettre en œuvre ? sur qui s'appuyer ? quel expert ou institutionnel solliciter ? Construire des convergences, développer des argumentaires...) et savoir la faire évoluer en fonction de l'évolution de la situation et des informations (changer d'interlocuteur, d'alliés, accepter un compromis…) ;
- De **savoir agir collectivement** quand cela est nécessaire : il ne faut pas vouloir toujours essayer d'agir seul. Se regrouper, nouer des alliances avec des alliés (des clients, des salariés, voire des confrères, par ailleurs concurrents), agir par l'intermédiaire d'un syndicat ou d'une organisation professionnelle… peut se révéler efficace ;
- De **communiquer** : ne pas hésiter à faire entendre sa voix auprès des élus, de la presse, du public en expliquant et justifiant la démarche menée à l'aide d'un message simple, clair et argumenté.

Disposer d'un réseau se révèle très souvent utile lors des différentes étapes de lobbying : il peut permettre de s'informer très en amont d'un événement ou d'une décision à venir, il peut également offrir des appuis importants permettant d'influencer les prises de décision à venir.

Les activités des entreprises sont de plus en plus influencées par des décisions arrêtées dans les **enceintes européennes** (nouvelles normes, nouvelles obligations ou recommandations inscrites dans les directives, règlements…). C'est pourquoi il est important pour une entreprise d'essayer d'être à l'écoute des textes qui sont discutés, préparés au niveau communautaire ; en effet, ainsi informée, elle pourra essayer de faire relayer ses attentes, ses aspirations sur l'évolution des textes à venir.

Si la disposition d'un bureau à Bruxelles peut se révéler coûteux, une entreprise pourra s'appuyer sur d'autres structures connaissant les « rouages » des décisions communautaires (organisation des groupes d'experts, liste des participants…) : par exemple le syndicat professionnel auquel elle est affiliée, la représentation de la France à Bruxelles (le point d'entrée pouvant être la « Cellule entreprises »), le bureau de représentation de son Conseil régional (de nombreuses Régions disposent aujourd'hui d'une représentation à Bruxelles)…

Sites et documents de référence : Suivi de l'actualité communautaire : http://europa.eu/press_room/index_fr.htm // Accès à la législation en vigueur et en préparation : http://eur-lex.europa.eu/fr/legis/20090101/index.htm ; http://eur-lex.europa.eu/fr/prep/latest/index.htm // Organigramme de la représentation permanente de la France à Bruxelles (cellule entreprises) : www.rpfrance.eu/spip.php?rubrique42 // // Intelligence Economique. Guide pratique pour les PME de Suisse Romande, HEG Genève, 2008 // Site régional Poitou-Charentes consacré à l'intelligence économique : fiches pratiques (www.ie-poitou-charentes.fr/?tg=oml&file=articles.ovml&ecran=3&article=135) // AFNOR (nouvelles normes) : www.afnor.org/portail.asp?colfond=Bleu&ref=ESP%5FNormalisation&lang=French

SENSIBILISATION DU PERSONNEL A LA PROTECTION DES INFORMATIONS SENSIBLES

Enjeu : Toute entreprise est exposée au risque de perte ou de détournement d'informations : vols de supports informatiques, interception de communications, manipulation de salariés… La protection des informations sensibles doit être une préoccupation de l'ensemble des acteurs impliqués dans l'entreprise (collaborateurs, cadres dirigeants, membres des organes sociaux…). Il est essentiel que chacun ait conscience de la sensibilité et de la vulnérabilité des informations qu'il détient, des pratiques frauduleuses existantes et de la nécessité d'une diffusion maîtrisée de cette information en interne comme en externe. C'est véritablement une prise de conscience qu'il convient de développer au sein de l'organisation et dans ses relations avec l'extérieur.

Comment ?

- Définir une politique de protection de l'information adaptée aux besoins de l'entreprise

Les informations sensibles

⇨ ***Quelles sont les informations sensibles de l'entreprise*** ?

- Les informations dont la divulgation procurerait un avantage à la concurrence ou aux partenaires ou réduirait l'avantage dont dispose l'entreprise (*R&D, travaux d'innovation, savoir-faire technologique, contenu d'offres commerciales, structure des comptes, fichiers clients projets de développement, fonctionnement de l'entreprise…)*
- Les informations encadrées par des exigences légales et/ou contractuelles (secret des affaires, engagement de confidentialité…)

! *Veiller à bien identifier les informations qui prises individuellement sont peu sensibles mais constituent ensemble une information confidentielle*

Les situations à risques

⇨ ***Quelles sont les situations à risques ?*** réponse à des appels d'offres, enquêtes, sondages, interviews, colloques, salons, déplacements, diffusion d'informations à des actionnaires, négociations commerciales, échanges d'informations avec les partenaires de l'entreprise, utilisation d'Internet…

Formaliser un référentiel de bonnes pratiques pour encadrer le comportement des salariés de l'entreprise dans ces situations

2. Sensibiliser et former les salariés à la protection des informations sensibles de l'entreprise

Sensibilisation du personnel

⇨ ***Quelle sensibilisation du personnel ?***

- ***Expliquer aux salariés*** la notion d'information sensible, les enjeux de la sécurité et les objectifs des mesures prises pour protéger l'information (différenciées en fonction des personnels et de leurs responsabilités), afin de faciliter l'acceptation et l'application de règles qui peuvent être parfois contraignantes
- Organiser une ***sensibilisation permanente*** via des **formations** (différenciées en fonction des personnels et de leurs responsabilités), des notes régulières, des réunions internes, la diffusion des bonnes pratiques, l'affichage des précautions à prendre dans les zones sensibles (photocopieurs…), écrans de veille rappelant le respect des règles de sécurité sur les postes de travail…

Sensibilisation du personnel

- ***Responsabiliser les salariés***
  - Inclure des clauses spécifiques dans les contrats de travail,
  - Prévoir des clauses de confidentialité dans les relations avec les contacts externes,
  - Recueillir l'engagement des salariés à respecter les règles de sécurité du système d'information
- ***Contrôler régulièrement le respect des règles*** de protection des informations et la connaissance des dispositions pratiques inscrites dans le **règlement intérieur** (conditions de circulation sur le site, l'utilisation des moyens de communications et des systèmes d'information, les sanctions éventuelles…)

3. Utilisation des outils « juridiques »

- ***Le contrat de travail des salariés*** (clauses de confidentialités qui restent valables après la rupture du contrat, clauses de restitution des données confidentielles, clauses de non-concurrence…)
- ***L'engagement de confidentialité*** à faire signer le plus largement possible, par exemple aux fournisseurs, aux clients, aux sous-traitants, aux prestataires extérieurs (maintenance, nettoyage, restauration, etc.), aux sociétés d'assurance, aux fournisseurs d'accès et hébergeurs pour l'informatique, aux stagiaires, aux intervenants occasionnels…
- ***Le contrat de confidentialité*** lors de la mise en place d'un partenariat (collaboration, sous-traitance, prestation de services….).

  Ce contrat constituera un engagement réciproque sur la sécurité que chacun apportera aux informations confiées par son ou ses partenaires

Principaux points à retenir pour la rédaction d'un contrat de confidentialité dans le cas d'un partenariat

- Indiquer les informations sensibles qui seront échangées ou partagées,

- S'accorder sur les niveaux de classification des informations et s'assurer que chacun donne la même signification aux dénominations retenues,

- Convenir des mesures de protection à mettre en place, en relation avec le niveau des informations à protéger,

- Contrôler la mise en place des mesures de sécurité et leur efficacité ou s'engager sur la validité d'une grille d'auto-évaluation de la sécurité annexée au contrat,

- Déterminer les responsabilités relatives à la protection des informations communiquées (qui est en charge de quoi ? obligation de résultat ou obligation de moyens en matière de protection de l'information),

- Contrôler la diffusion des informations sensibles en interdisant les sous-contractants ou en prévoyant de leur imposer des règles de confidentialité,

- Définir des procédures d'habilitation des personnes qui auront « besoin d'en connaître » dans le cadre du contrat (directement ou en sous-traitance),

- Préciser, pour le personnel du partenaire accueilli sur site, les autorisations d'accès accordées, les moyens de communication mis à disposition et leurs conditions d'utilisation (par exemple création d'une adresse électronique sur le serveur de messagerie de l'entreprise ou possibilité d'utilisation dans des tranches horaires « hors normes » en raison des décalages horaires).

- Pour plus d'informations sur la rédaction d'engagements contractuels de confidentialité dans le cadre des **pôles de compétitivité** :
  http://www.industrie.gouv.fr/guidepropintel/fiches_pratiques/la_confidentialite.htm

A Noter :

La perte ou la destruction d'informations sensibles est le fait dans 80 % des cas de maladresses internes ou de l'absence de process de sauvegarde fiable (cf. fiche sur la Sécurité des Systèmes d'Informations).

Sources : www.clusif.fr // www.ssi.gouv.fr

REFERENTIEL DE BONNES PRATIQUES POUR LA SENSIBILISATION DES SALARIES

Enjeu :

L'élaboration et la diffusion de bonnes pratiques est indispensable pour prévenir le risque humain dans la perte d'informations sensibles. Cela permet d'identifier clairement les situations dans lesquelles, les salariés, en dépit de relations de convivialité, doivent rester attentifs aux respects des règles de protection des informations sensibles de leur entreprise. Ces règles pourront faire l'objet de formations et devront être rappelées périodiquement.

Comment ?

⇨ *Les comportements dans l'entreprise*

- Mettre sous clé les documents sensibles, les ordinateurs portables et fermer les bureaux
- Verrouiller les postes de travail à l'aide d'un mot de passe complexe et le changer périodiquement
- Téléphone, fax, mail : utilisation à proscrire pour les informations les plus sensibles – pour les informations moins sensibles, limiter néanmoins les échanges au strict nécessaire – usage de fax sécurisés – usage de moyens de signature et de chiffrement pour la messagerie et internet - sécuriser les PDA.
- Veiller à l'effacement du disque dur des photocopieurs et fax, notamment lors de la maintenance du matériel
- Ne pas jeter les documents comportant des informations sensibles à la poubelle sans les avoir détruits – mise à disposition de déchiqueteuses…

⇨ *L'accueil des visiteurs (clients, fournisseurs, prestataires…)*

Avant la visite

- Se faire communiquer l'identité et la fonction des visiteurs
- Répertorier les informations qui pourront être portées à la connaissance du visiteur et celles qui ne pourront être divulguées
- En cas de visite des locaux, établir un parcours évitant les zones sensibles
- Dans le local où se déroule une réunion, ne pas laisser en évidence des documents sensibles

Pendant la visite

- Remettre un badge identifiable aux visiteurs
- Les accompagner / faire accompagner en permanence
- Ne remettre que des documents indispensables,
- Raccompagner tous les interlocuteurs jusqu'au point d'accueil
- Tenir à jour les badges individuels d'accès et veiller à les récupérer à la fin de la visite

⇨ *L'accueil des stagiaires*

Avant le stage :

- Examen complet du Curriculum Vitae. Accueil de stagiaires encadrés avec enquêtes préalables pour les ressortissants étrangers (contacter la Direction Régionale du Renseignement Intérieur de votre région)
- Définir le contenu du stage et désigner un tuteur
- Définir éventuellement des lieux non autorisés dans l'entreprise

Pendant le stage :

- Veiller à ne pas octroyer un accès sans contrôle ou sans surveillance à l'intranet ou à certains fichiers et documents
- Veiller aux respects des horaires et des lieux autorisés

Après le stage :

- Examen approfondi des travaux du stagiaire visant à vérifier la non divulgation de donnes jugées stratégiques ou sensibles (communication du rapport de stage)
- Rédaction d'un rapport par le tuteur
- Supprimer les droits et le badge d'accès des partants

⇨ *La communication à l'extérieur de l'entreprise : le cas des salons*

Avant le salon :

- Définir les informations qui pourront ou non être diffusées sur le salon
- Identifier les besoins d'informations et définir la façon de les obtenir (rencontre sur le stand avec le partenaire / concurrent, acquisition de plaquettes de communication, participation à une présentation organisée sur le salon …)
- Etudier la disposition du salon, la place des exposants (concurrents, prestataires…), les opérateurs présents et ceux qui ne le sont pas (pourquoi ?)
- Limiter au strict minimum le nombre de documents ou matériels sensibles
- Préparer les axes de réponses sur les sujets délicats (savoir-faire, innovations…)

Pendant le salon :

- Ne pas laisser sans surveillance les matériels à risque (prototypes, maquettes…) et conserver les informations sensibles avec soi
- Profiter du salon pour collecter des informations stratégiques (prises de notes, plaquettes, rencontres …)
- Eviter les entretiens sensibles dans les lieux trop publics
- Faire preuve de discrétion au restaurant et à l'hôtel où séjournent peut-être d'autres exposants
- Face aux visiteurs, s'assurer au mieux de son identité (carte de visite) ; faire attention aux concurrents anonymes ou aux faux journalistes
- Lors de la clôture, faire place nette sur le stand et vérifier l'ensemble des matériels et documents

Après le salon :

- Suivre les réactions d'après salon dans la presse ou sur internet
- Etablir un rapport de visite qui répertorie les informations stratégiques collectées (nouveaux contacts, informations techniques sur des produits, nouveaux matériaux…) et le diffuser aux collaborateurs concernés

⇨ *Les relations avec les fournisseurs et les clients*

- Sensibilisation renforcée pour les acheteurs et commerciaux qui ont une relation ancienne avec leurs interlocuteurs
- Limiter au strict minimum les informations diffusées - attention aux appels d'offre détournés…

⇨ *L'utilisation des ordinateurs portables*

Prévenir les risques de vol ou de copie	Réduire les conséquences d'un vol	Précautions d'utilisation
- Garder toujours votre ordinateur près de vous - Equiper le d'un cadenas et/ou d'une alarme - Utiliser un mot de passe complexe (mêlant caractères numériques et alphabétiques) et le changer régulièrement - Ne pas le mettre à disposition pour une présentation (risque de copie via une clé USB en quelques secondes)…	- Transport des données via des supports amovibles (CD rom, clé USB…), à séparer de l'ordinateur portable - Chiffrer le disque dur…	- Dans un espace public, travailler uniquement sur des documents non confidentiels et utiliser des filtres rendant l'écran opaque - Désactiver tous les moyens de communication offerts par votre portable (ports infrarouges, Wifi, Bluetooth… - Mettre à jour des correctifs de sécurité avant de le reconnecter sur le réseau de l'entreprise…

⇨ *Les déplacements*

Principales règles de sécurité :

- Emporter uniquement les pièces d'identité et documents administratifs nécessaires, tout document (carnet d'adresses, agenda, notes, badge, papier à en-tête de la société, etc.) peut être volé ou dupliqué
- N'aborder jamais de sujets confidentiels en dehors de l'entreprise (transports, clubs…)
- Ne jamais laisser de documents confidentiels sans surveillance même quelques minutes

A l'hôtel

- Ne jamais laisser de documents sensibles dans sa chambre sans surveillance
- Ne pas mettre de documents ultraconfidentiels dans le coffre de la chambre ou de l'hôtel ; les conserver avec soi
- Ne pas aborder de sujets confidentiels au téléphone

Sources : www.clusif.fr // www.ssi.gouv.fr

SECURITE DU SYSTEME D'INFORMATION

Enjeu :

Dans 80 % des cas, ce sont les maladresses internes, (volontaires ou non) ou l'absence de sauvegardes fiables qui sont à l'origine de la perte ou de la destruction d'informations sensibles. Les 20 % restants sont imputables à des actes externes mal intentionnés. Au cours de ces dernières années, le risque sur le système d'information s'est accru avec le développement du travail à distance et des nouvelles technologies.

L'entreprise doit concilier la nécessité de communiquer des informations et de préserver certaines d'entre elles en mettant en place une politique de sécurité de son système d'information (SSI).

Pour être efficace, la politique de sécurisation du système d'information doit s'appuyer sur la mise en place de moyens techniques mais son efficacité reposera également fortement sur l'organisation du processus dans l'entreprise et sur les comportements individuels.

Comment ?

Que protéger ?

- Le système d'information comprend :
  - le ou les serveurs réseau et des postes de travail informatique (fixes et nomades) ;
  - les applications (systèmes d'exploitation, suites bureautiques, logiciels métiers …) ;
  - les infrastructures de communication et de télécommunication (réseaux locaux, liaisons inter-sites, réseau téléphonique, accès Internet, liaison radio …).
- Les informations sensibles détenues par l'entreprise (Les informations dont la divulgation procurerait un avantage à la concurrence ou aux partenaires ou réduirait l'avantage dont dispose l'entreprise telles que la *R&D, les travaux d'innovation,* le *savoir-faire technologique, le contenu d'offres commerciales, la structure des comptes financiers, les fichiers clients, les projets de développement, le fonctionnement de l'entreprise…)*. Les informations les plus sensibles devront faire l'objet de procédures renforcées.

Quels sont les risques pesant sur le système d'information ? vols, destruction de données ou de matériel, captations d'information, indisponibilité du système, etc. avec une origine qui peut être externe mais souvent interne (malveillance ou négligence).

Quelles sont les vulnérabilités du système d'information ? (modes d'accès au réseau de l'entreprise – protection insuffisante des serveurs et postes de travail, équipements nomades, messagerie non protégée…)

Formalisation d'une politique de protection du Système d'Information

Désignation et formation d'un **responsable de la sécurité du Système d'Information**

Formation et sensibilisation permanentes de l'ensemble des salariés à la protection des informations sensibles

(Voir fiche sur la sensibilisation du personnel à la protection des informations sensibles)

Etablir une charte avec les **règles de bonnes pratiques quant à l'utilisation du Système Informatique**

- Confidentialité et renouvellement des mots de passe
- Verrouillage de l'ordinateur
- Gestion des courriers électroniques
- Déclaration de tout incident
- Sauvegarde et suppression des données les plus anciennes
- Installation de tout nouveau logiciel interdite sans autorisation
- règles d'utilisation d'internet (téléchargement – participation à des forums…)
- etc.

Engagement de la responsabilité des utilisateurs (charte d'utilisation annexée au règlement intérieur ou document qui renvoie au règlement intérieur pour les sanctions – attention aux conditions de mise en place).

Implication forte de la direction

Quelles procédures de sécurisation du système d'information ?

Authentification :

➢ Déterminer des droits d'accès au système d'information différenciés selon les responsabilités des salariés et les statuts des autres personnes pouvant avoir accès au système d'information (stagiaires, personnels temporaires, prestataires extérieurs) : qui a le droit de faire quoi ? de savoir quoi ?

➢ Gestion des codes d'accès et des mots de passe (attribuer des mots de passe suffisamment sécurisés (agrégat de caractères alphabétiques et numériques), les renouveler régulièrement (tous les 3 mois par exemple), les supprimer lors du départ des individus) ;

➢ Configuration des postes par le responsable de la sécurité du système d'information …

Sécuriser les informations et le système :

➢ Utilisation des logiciels et matériels de sécurité (antivirus, anti-spyware, pare-feu, anti-spam, etc.) pour les serveurs et postes informatiques (fixes et nomades) ;

➢ Sécurisation des échanges (Internet - extranet – Wifi ...) par le chiffrement des données les plus sensibles ;

➢ Pour les données très sensibles, utilisation de matériel non connecté au réseau ;

➢ Application des mises à jour et correctifs des logiciels ;

➢ Contrôler régulièrement la configuration des pare-feu ;

➢Veille sur les nouveaux virus, logiciels espions (www.certa.ssi.gouv.fr - www.cert-ist.com).

Sauvegarde :

➢ Définir le type de données à sauvegarder, selon quelle périodicité, pour quelle durée (obligations légales pour certaines données) – Revoir périodiquement le périmètre de sauvegarde

➢ Dupliquer les sauvegardes - Répartir les informations confidentielles sur plusieurs supports

➢ Sécurisation des lieux de sauvegardes, conservation des supports mensuels et annuels en dehors de l'entreprise

➢ Contrôle du bon fonctionnement des sauvegardes

➢ Sous-traitance à un prestataire : s'assurer du cryptage des données sauvegardées chez le prestataire …

Contrôle de la bonne utilisation du système d'information par les salariés *(Cf. www.cnil.fr pour les conditions d'application)* – Le contrôle est nécessaire, l'entreprise étant responsable de la protection de son système d'information. – Ces mesures doivent notamment être transparentes, connues de tous, faire l'objet d'une discussion collective, faire preuve de précision et mesure, définir clairement les procédures concernant les messages privés.

Gestion des incidents :

➢ Détection des vulnérabilités et anomalies le plus en amont possible

➢ Les instances à alerter en cas d'attaque informatique :

La Gendarmerie – La DCRI (Direction Centrale du Renseignement Intérieur) – L'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'information et de la Communication) – le BEFTI (Brigades d'Enquêtes sur les Fraudes aux Technologies de l'Information) - Pour plus d'informations : www.clusif.fr (Portail Cybervictime) ;

➢ Prévoir des solutions de secours en cas d'indisponibilité du système informatique (assistance dépannage – mise à disposition de matériel de secours).

Recours à la sous-traitance

Les 10 points clés du contrat de sous-traitance (*source : Guide SSI – Medef 2005*)

➢ S'assurer de la santé financière du prestataire

➢ Veiller au respect de la confidentialité des informations (clauses de confidentialité)

Le contrat de sous-traitance

1. Mention dans le document contractuel de l'ensemble des documents (cahier des charges, propositions du prestataire…) **- 2.** Description précise des prestations **- 3.** Régime de l'obligation du prestataire (moyens ou résultats) **- 4.** Prix des prestations (critères d'évolution des prix) **- 5.** Etablissement du montant des pénalités **- 6.** Définition du statut et la propriété des matériels et logiciels **- 7.** Etendue de la responsabilité **- 8.** Limitation du préjudice réparable **- 9.** Cession de droits (développement de logiciels par le prestataire) **- 10.** Juridiction compétente en cas de litige

Quels enjeux juridiques ?

(les principaux)

Risque de mise en cause civile ou pénale de l'entreprise induite par le comportement de ses salariés :

- L'utilisation malveillante des moyens informatiques et de communications électroniques (messagerie, forums) (contenus diffamatoires à l'égard de tiers par exemple) ;
- Le téléchargement de documents ouvrant droit à des poursuites pénales (pédophiles, incitation à la haine raciale …) ;
- La contrefaçon : utilisation de copies illicites de logiciels ou d'œuvres protégées sans autorisation des ayants droits ;
- Traitement de données nominatives sans autorisation (cf. www.cnil.fr et fiche sur la collecte d'information) ;
- Le non respect du secret des correspondances privées.

En cas de défaut de protection de son système d'information, la responsabilité de l'entreprise peut également être engagée :

- Par ses partenaires extérieurs (atteinte à leur système d'information, non respect des engagements de livraison, de confidentialité …) ;
- Par ses actionnaires et ses salariés (mise en cause du dirigeant pour faute de gestion).

La responsabilité du chef d'entreprise peut être également mise en cause en cas de non respect des procédures dans la mise en place d'un processus de cybersurveillance des salariés (cf. www.cnil.fr)

L'entreprise est soumise à la nécessite de veiller à **l'intégrité,** la **confidentialité,** la **disponibilité,** et la **traçabilité** de ses informations et de mettre en place les moyens adaptés tant d'un point de vue technique qu'organisationnel (procédures – encadrement du comportement humain).

Sites et documents de référence : www.afnor.org (norme ISO 27001 : référentiel pour le management de la certification de la sécurité des systèmes d'information – stratégies – mise en œuvre et bonnes pratiques) // CLUSIF : Menaces Informatiques et Pratiques de Sécurité en France, juin 2008 – Maîtrise et Protection de l'Information, juin 2006 (www.clusif.fr) // Sécurité économique : Les bonnes pratiques pour votre entreprise, Comité Opérationnel Défensif à l'Intelligence Economique de Lorraine // Dispositif de Sécurité Economique, Comité Opérationnel de Sécurité Economique de Basse-Normandie // Guide méthodologique de Sécurité économique dans les pôles de compétitivité, INHES // Guide SSI, Medef, 2005 // www.securite-informatique.gouv.fr // www.ssi.gouv.fr (Méthode de gestion des risques EBIOS – Guide d'élaboration des Politiques de Sécurité des Systèmes d'Information)

PROTECTION
PAR LA PROPRIETE INDUSTRIELLE OU LE SECRET

Enjeu :

L'innovation contribue au succès des entreprises. Celles-ci, détentrices d'un savoir-faire spécifique, s'exposent à un risque de pillage de leurs innovations et/ou de contrefaçon. La contrefaçon représente 10 % du commerce mondial et détruit 30 000 emplois chaque année, en France. Tous les secteurs industriels sont touchés (produits alimentaires et boissons, électroménager, jouets, médicaments, pièces détachées pour l'automobile…).

Afin de protéger son patrimoine immatériel, l'entreprise doit définir ***une véritable stratégie de protection de ses innovations.***

Comment ?

1. DEFINIR LES OBJECTIFS DE LA STRATEGIE DE PROTECTION DE L'INNOVATION

- Quels sont les savoir-faire qui doivent être protégés ? (savoir-faire dont la perte impliquerait une perte de compétitivité de l'entreprise)
- Comment les protéger ? (protection par la *propriété industrielle ou secret*)

⇨ ***La propriété industrielle***

Principaux outils de la propriété industrielle

Brevet	Dessins et modèles	Marques	Enveloppe soleau
Protège les innovations techniques et donne à son titulaire le monopole de son exploitation (durant 20 ans, voire 25 ans dans le cadre de médicaments ou et de produits phytosanitaires)	Protection du design des produits avec un monopole d'exploitation pour une durée minimale de 5 ans qui peut-être prolongée par tranche de 5 ans jusqu'à 25 ans.	Assure le monopole d'exploitation de la marque pour 10 ans et est renouvelable indéfiniment.	Permet de constituer une preuve de la création d'une idée ou d'un projet mais n'offre pas de protection
Pour plus d'informations www.inpi.fr/brevets	Pour plus d'informations www.inpi.fr/dessins et modèles	Pour plus d'informations http://www.inpi.fr/fr/marques.	Pour plus d'informations http://www.inpi.fr/soleau

Outre la protection des innovations, la propriété industrielle contribue également à la valorisation de l'entreprise :

- valorisation financière (concession de licences, cession de titres)
- valorisation de l'image auprès des fournisseurs, clients, financeurs…

➪ ***Le secret industriel ou de fabrication*** : savoir-faire de l'entreprise tenu caché des concurrents. Il est indispensable en cas d'inventions non brevetables

Brevet ou Secret ? Avantages - Inconvénients

	Protection juridique	Coûts	Divulgation des informations
Brevet	• Monopole d'exploitation **OPPOSABLE À TOUS**	• Potentiellement élevés (Frais de dépôts, honoraires, taxes…) mais également **source de revenus** par la concession de licences	• Elevée (condition de validité du brevet) Donne **accès aux CONCURRENTS À L'INFORMATION TECHNOLOGIQUE de l'entreprise** 18 mois après le dépôt du brevet
Secret	• **PROTECTION LÉGALE LIMITÉE** (action en concurrence déloyale ou pour violation du secret professionnel ou du secret de fabrique) **ATTENTION** à mettre en place les mesures de protection (système de sécurité, clauses de confidentialités…) pour prouver le caractère confidentiel du savoir-faire	• Plus faibles mais prévoir des **coûts internes de maintien du secret**	• Exclue afin de conserver le caractère confidentiel

- Sur quelles zones géographiques ?

La protection industrielle à l'étranger

- ***Pour les brevets*** : au niveau européen www.epo.org / par voie PCT (Patent Cooperation Treaty) www.ompi.org / pour l'Afrique francophone subsaharienne www.oapi.wipo.net / dans chaque pays

- ***Pour les dessins et modèles*** : au niveau communautaire oami.europa.eu / au niveau international www.ompi.org / dans chaque pays

- ***Pour les marques*** : dépôt de marque à international / au niveau communautaire oami.europa.eu / pour l'Afrique francophone subsaharienne www.oapi.wipo.net / dépôt dans chaque pays

2. EVITEZ LA CONTREFAÇON

- ***Surveiller ses brevets et ses marques par une veille technologique et concurrentielle*** pour s'assurer que personne n'utilise son invention sans autorisation (publication et presse spécialisée, salons professionnels, sites Internet, bases de données sur les titres de propriété industrielles, etc.)

- Chercher à ***repérer le plus en amont les signaux de la contrefaçon*** (baisse de l'activité par la perte de marchés, dégradation inexpliquée de la notoriété, etc.).

- ***Mettre en place des mesures de protection*** (inclure des clauses particulières dans le contrat de travail des salariés, mise en place d'un système de sécurité, d'une charte de la confidentialité, formation du personnel à la propriété industrielle…)

- Bien ***gérer ses droits de propriété industrielle*** (suivre les délais auxquels les titres sont soumis, renouveler ses marques et noms de domaines)

- ***Surveiller les titulaires de licence*** afin d'éviter tout manquement de leur part

- ***Avoir recours au service des Douanes*** afin d'identifier d'éventuels contrefacteurs

  Les agents des douanes ont le pouvoir de retenir des marchandises afin de permettre à l'entreprise de saisir les autorités judiciaires **à condition** qu'une demande d'intervention ait été préalablement déposée par l'entreprise.

La demande d'intervention

Pourquoi ?

- Attirer l'attention des douanes sur des produits suspects
- Unique procédure pour obtenir une saisie par les Douanes dans les cas notamment de contrefaçon présumée de dessins et modèles, de marques ou atteinte à un brevet…
- Disposer de 10 jours ouvrables pour saisir les autorités juridiques compétentes

Indispensable pour permettre aux Douanes d'agir contre la contrefaçon

Pour plus d'informations : ***site des Douanes sur la contrefaçon***

- ***Poursuivre les éventuels contrefacteurs***
  (code de la propriété intellectuelle)

La contrefaçon

La contrefaçon est un délit au même titre que le vol et donc passible de sanctions :
• **pénales** (amende pouvant atteindre 300 000 € et une peine de prison de trois ans, 500 000 € et 5 ans de prison si infraction en bande organisée, fermeture totale ou partielle de l'établissement ayant servi à commettre l'infraction…)
• **civiles** (dommages et intérêts versés au titulaire des droits, destruction de la marchandise et du matériel, publication de la décision…)
• **douanières** (Confiscation des objets contrefaisants et des moyens de transport et objets ayant servi à masquer la fraude, amendes …)

Lutte contre la contrefaçon sur internet

Le 20 février 2009, le Secrétaire d'Etat chargé de l'Industrie et de la Consommation a lancé une mission pour lutter contre la contrefaçon sur internet. La mission est chargée, avant l'été 2009, d'élaborer un protocole d'engagements entre plateformes de e-commerce, titulaires des marques et associations de consommateurs.

Quel accompagnement dans la mise en œuvre de votre stratégie de protection industrielle ?

- Pré-diagnostic gratuit pour l'entreprise : Brochure pré-diagnostic de l'INPI
- La compagnie nationale des conseils en propriété industrielle : site de la CNCPI
- L'association des conseils en propriété industrielle : site de l'ACPI
- L'association des avocats de propriété industrielle : site de l'AAPI
- Loi Modernisation de l'Economie : mesures de simplification de la procédure de dépôt de brevets (www.modernisationeconomie.fr)

Sites et documents de référence :

www.inpi.fr // Etudes de cas relatives à la politique de dépôt de brevets dans les PME : www.epo.org // Guide de la propriété intellectuelle dans les pôles de compétitivité : http://www.industrie.gouv.fr/guidepropintel/fiches_pratiques/la_strategie.htm // Portail de recherche d'informations en propriété industrielle : www.plutarque.com // Site de la propriété industrielle et des PME : http://www.pi-r2.org/index.php3 // Site du Ministère de l'Industrie (réglementation, témoignages d'entreprises) : http://www.industrie.gouv.fr/portail/pratique/index_lutte.html // www.unifab.com // www.oseo.fr

PROTECTION DE L'IMAGE DE L'ENTREPRISE

Enjeu :

Toute entreprise peut être victime d'une atteinte à son image. Celle-ci peut être multiforme : dénigrement des produits et services, appel au boycott, mise en cause des dirigeants, diffusion d'informations erronées, utilisation malveillante du nom de l'entreprise, de ses marques, détournement de sa communication (slogans – défiguration du site Internet, mise en ligne d'un faux site...).

Les entreprises sont d'autant plus vulnérables qu'elles interviennent sur des secteurs en prise directe avec les consommateurs.

Ces attaques qui ternissent la réputation de l'entreprise peuvent aller jusqu'à la mise en péril de sa santé économique.

Comment protéger l'image de l'entreprise?

- *Disposer d'une veille spécifique sur la réputation de l'entreprise* (informations erronées – rumeurs – photos – flux Rss…)
- *Agir contre les nuisances relevées*

1. LA VEILLE SUR LA REPUTATION DE L'ENTREPRISE

Organiser la collecte <u>permanente</u> de l'information véhiculée sur l'entreprise :

- Sur Internet :

  - Identifier les **sources pertinentes** : sites de presse –sites d'informations financières –sites des concurrents - blogs (identification des blogs via les moteurs de recherche spécialisés tels <u>Technorati</u>, <u>Blogsearch google</u>, <u>Wikio</u> –sites des ONG (consommateurs – environnement) – réseaux sociaux –sites collaboratifs type Wikipédia –Forums

  - Définition **des mots clés** (avec différentes orthographes) : le nom de l'entreprise, le nom des principaux responsables, les marques, le nom des sociétés concurrentes et de leurs dirigeants... et interrogation régulière des sources identifiées

  - Paramétrage d'alertes via des outils de type <u>Googlealerts</u>, abonnement aux flux RSS des sources identifiées

- Dans la presse nationale (surtout régionale pour les PME) et dans la presse spécialisée

- Via le réseau commercial afin d'identifier et répondre à d'éventuels mécontentements

Renforcer le dispositif de veille lors des périodes plus particulièrement sensibles : sortie d'un nouveau produit – départ d'un collaborateur – restructuration – transmission de l'entreprise…

Contrôler systématiquement les communications écrites de l'entreprise afin de maîtriser tout risque d'interprétation qui serait préjudiciable à l'image de l'entreprise.

Contrôler les sites Web qui pointent vers le site de l'entreprise
A noter que le fait d'établir un lien vers un autre site sans autorisation de ce site peut être considéré comme portant préjudice.

2. AGIR CONTRE LES NUISANCES RELEVEES

Avant d'entreprendre toute action, il est important de s'interroger au préalable sur ***la capacité de nuisance de l'auteur de l'attaque*** *ce qui va déterminer l'ampleur des actions à mettre en place*

Les actions de riposte progressives à mener en fonction de l'ampleur de l'attaque et de sa diffusion :

- Elaborer une stratégie de réponse :
  - Quelles réponses apporter : expliciter pourquoi on est dénigré ? ou pourquoi les informations sont fausses ?...
  - Quelles sont les cibles et qui faut-il par conséquent convaincre ?
- Identifier si possible les auteurs de la nuisance et les contacter pour demander la suppression des propos litigieux et éviter une propagation rapide via Internet
- Contacter les hébergeurs et/ou les éditeurs de sites dont la responsabilité juridique peut-être mise en cause
- Répondre aux informations diffamatoires ou préjudiciables diffusées sur les sites, les blogs, les forums de discussions
- Communiquer en interne de l'entreprise (lever les doutes – définir les messages à véhiculer)
- Utiliser le site Internet de l'entreprise pour démentir les faits et argumenter
- Mettre en place une véritable communication de crise vis-à-vis de l'ensemble des partenaires de l'entreprise et des médias (cf. fiche sur la gestion de crise)
- Entamer une procédure juridique

Entamer une procédure juridique

Principaux recours juridiques

- **Droit de réponse** (article 6-IV de la loi sur la confiance de l'économie numérique du 21 juin 2004)
- **Diffamation et injures** (art 29 de la loi du 29 juillet 1881 sur la liberté de la presse)
- **Responsabilité éditoriale** des éditeurs et des hébergeurs de site (art 6 de la loi sur la confiance de l'économie numérique du 21 juin 2004)
- **Contrefaçon de marque** (art. L.716-1 code de la propriété intellectuelle)
- Action judiciaire contre le parasitisme dont le **cybersquatting d'une marque** (dépôt de noms de domaines similaires à la marque)
- **Concurrence déloyale – Concurrence parasitaire – Dénigrement**

A noter : afin d'être sûr de choisir la procédure appropriée, il est important de prendre conseil auprès d'un expert juridique.
Il est également nécessaire d'avoir **déposé les noms liés à sa dénomination sociale et à ses marques** dans les différentes extensions (cf. Inpi).

Sites et documents de référence :

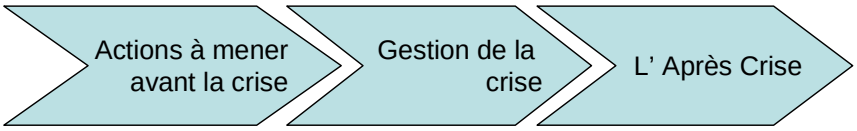
www.clusif.fr (étude sur la maîtrise et la protection de l'information) / www.inpi.fr / www.les-infostrateges.com (dossier sur la e-réputation) / www.journaldunet.com / www.digimind.fr (réputation internet) / www.inhes.interieur.gouv.fr (aide-mémoire sur la maîtrise de la communication de crise) / www.legalis.net (jurisprudence diffamation)

PREPARATION A LA GESTION DE CRISE

Enjeu :

Les entreprises sont exposées à une diversité de risques (économiques, techniques, technologiques, humains, réglementaires, environnementaux, sociaux, informationnels, informatiques, etc.) qu'il n'est pas toujours possible d'anticiper et qui peuvent avoir des conséquences fortement dommageables pour l'entreprise : perte de marchés, perte de savoir-faire, perte de crédibilité….Lorsque survient la crise, l'entreprise doit être en mesure de réagir très vite. Sa capacité de réaction et l'efficacité de son action sont dès lors liées à son degré de préparation. A cette fin, il est indispensable pour l'entreprise d'identifier le plus en amont possible ses vulnérabilités et les menaces associées. Il faut aussi prévoir comment réagir (procédures à mettre en place, moyens humains et matériels à mobiliser, réseaux, information à détenir, plans de communication…).

Comment ?



1. TROIS ACTIONS INDISPENSABLES A MENER AVANT LA CRISE

1 - Identifiez les activités critiques de l'entreprise…

Activités qui doivent être assurées pour ne pas mettre en péril la pérennité de l'entreprise

… et ses vulnérabilités

2 - Constituez votre "boîte à outils d'urgence"

Informations indispensables (annuaires des responsables, plans des lieux, moyens extérieurs mobilisables, etc.)

Plans de continuation de l'activité (liste des premières mesures à prendre, plan de récupération des données informatiques,…)

3 - Formez-vous à la communication de crise

Les facteurs clés de la communication de crise

✓ Nommer un porte-parole préparé à la communication de crise clairement identifié comme la voix officielle de l'entreprise,

✓ Disposer des matériels de communication préparés à l'avance (liste des personnes à contacter – argumentaires…)

✓ Communiquer suffisamment d'éléments factuels afin de réduire les risques d'interprétations, de déformations ou de désinformations,

✓ Ecouter et analyser les réactions aux informations transmises et s'assurer que sa communication est comprise et correspond aux attentes,

✓ Associer l'ensemble des salariés à la sortie de crise par une communication interne spécifique (lever les doutes, indiquer les grands axes de la sortie de crise), à différencier de la communication externe plus axée sur la défense de l'image de l'entreprise.

✓ Adapter en permanence le discours aux évolutions et répercussions de la crise,

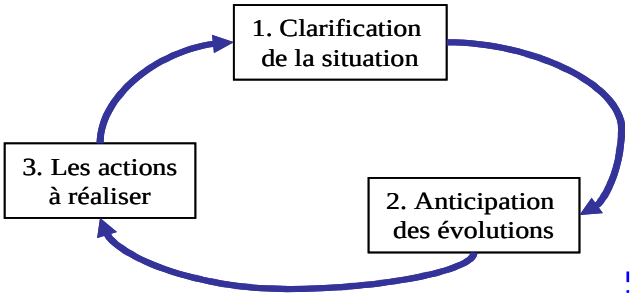
✓ Pour les messages diffusés, veiller à :

- La véracité de l'information (toute information ne doit pas être systématiquement diffusée mais celle qui l'est doit être vraie)
- La cohérence de l'information avec l'image et les valeurs de l'entreprise
- La crédibilité de l'information (prouver ce que l'on avance)

2. LA GESTION DE LA CRISE

Le suivi de ces 3 étapes est indispensable pour prévenir les "mauvaises" réactions prises trop à chaud. Pour autant, face à une crise, l'entreprise doit définir rapidement un plan d'actions et prendre des mesures pour éviter un gonflement de la crise, d'où l'importance de la phase de préparation

Un management en trois temps



A chaque Gestion de crise ses solutions spécifiques

***E**n fonction du type de risque (industriel, économique, informatique…), de l'origine de la crise (naturelle, accidentelle, malveillance, erreur,…) et des acteurs impliqués.*

Les questions à se poser

Clarification de la situation

Comment en est-on arrivé là ?
(historique des événements)

Qui est impliqué ?
(initiateurs, victimes, soutiens, détracteurs)

Quels sont les moyens d'actions et les contraintes pesant sur l'entreprise ?

Quelles sont les capacités d'action des acteurs présents ?

Anticipation des évolutions

Comment la crise peut-elle évoluer ?
en fonction des choix probables des différents acteurs et des actions envisagées par l'entreprise (analyse des différents scénarii d'évolution) ?

Quel est le niveau de responsabilité de l'entreprise ?

Quelles sont les conséquences ?
atteinte à l'image vis-à-vis des salariés, des clients, des fournisseurs, des institutions, des investisseurs, dégradation des résultats financiers, dégradation de l'outil de production

Les actions à réaliser

Rechercher les informations manquantes
en fonction des actions mises en œuvre et de leur impact sur l'évolution de la crise

Implication personnelle accrue du chef d'entreprise
garant de l'unité et de la stabilité de l'entreprise et le seul à pouvoir prendre des décisions inhabituelles

Mise en œuvre de la communication de crise
au sein de l'entreprise – avec les acteurs en relation avec l'entreprise – avec les médias
adaptation continue des messages et des cibles de communication

Gestion jusqu'au retour d'une situation normale

3. APRES LA CRISE

- N’oubliez pas d’annoncer le retour à la normale et de remercier vos soutiens (réunions internes, courriers aux fournisseurs, clients, communiqué de presse, etc.)
- Tirez les enseignements de la crise et adaptez votre dispositif de prévention et vos sujets de veille
- Informer le personnel sur la stratégie mise en œuvre pour enrayer les conséquences de la crise sur l’entreprise
- Dans la mesure du possible, valorisez le comportement de votre structure face à l'adversité

Adaptation des dispositifs de veille (concurrentielle, marchés, technologique, juridique, image de marque,…) pour :

✓ Pouvoir détecter le plus en amont possible les menaces et mettre en place des actions préventives avant même la survenue de la crise

✓ Pouvoir agir plus vite dans le cas d’une crise similaire

Sites et documents de référence : www.observatoire-crises.org // www.vigilances.fr

CADRE JURIDIQUE DE LA COLLECTE D'INFORMATIONS

Enjeu :

Lors de la collecte et de la diffusion d'informations, les entreprises sont exposées à un risque de mise en cause de leur responsabilité. L'acquisition et le traitement de l'information s'inscrivent dans un cadre juridique qui repose notamment sur le respect de la propriété intellectuelle, de la vie privée et des libertés individuelles et de la protection des informations sensibles des entreprises.

Comment ?

1- Le traitement et la diffusion d'articles, d'extraits de revues spécialisées ou de toute œuvre originale protégée doivent respecter les règles de la propriété intellectuelle et notamment le droit d'auteur

Certaines informations dites « ouvertes » ou libre d'accès peuvent faire l'objet de protections de type droit d'auteur ou droit de propriété industrielle.
Ainsi, avant toute reproduction d'une image, d'un dessin, d'un modèle ou d'un texte issus d'un support papier ou électronique, il convient de savoir si cette information est libre de droit ou bien doit faire l'objet d'une demande d'autorisation sous peine de constituer une atteinte au droit d'auteur susceptible d'être attaquée pour contrefaçon.

Droit d'auteur :
« Droit de propriété intellectuelle dont la durée s'étend jusqu'à 70 ans après la mort de l'auteur et qui s'acquiert sans aucune formalité de dépôt, du seul fait de la création. Il confère des droits patrimoniaux (droit de reproduction et de représentation) et un droit moral (notamment droit au respect de l'œuvre). Toute création artistique ou littéraire, quel qu'en soit le mérite, peut bénéficier d'une protection au titre du droit d'auteur, si elle est originale »
Source : CNCPI (Compagnie Nationale des Conseils en Propriété Industrielle) - *Articles L111-1 et s et articles L112-2e et s du code de la propriété intellectuelle*

- ***La diffusion de revues de presse*** ou panoramas de presse (assemblages d'articles ou d'extraits d'articles) sur le site Internet de l'entreprise, un forum de discussion, une liste de diffusion ou l'intranet doit faire l'objet d'une autorisation des auteurs et de leurs éditeurs. - Pour plus d'informations : Centre français d'exploitation de la copie (www.cfcopies.com)

2- L'analyse et l'utilisation de données à caractère personnel doivent respecter la vie privée et les libertés individuelles des personnes physiques : les principales dispositions de la loi « Informatique et Libertés »

Les entreprises gèrent de nombreuses informations à caractère personnel (fichiers contenant des données sur les clients, les prospects, les fournisseurs, les personnels, les badges électroniques favorisant le contrôle de passage des visiteurs, du personnel, etc.). La loi n°78-17 du 6 janvier 1978 modifiée en 2004 fixe un cadre à la collecte et au traitement de ces informations afin d'éviter que leur divulgation ou leur utilisation porte atteinte aux droits et libertés ou à la vie privée des personnes concernées.

En cas de non respect de la loi, les entreprises peuvent voir leur responsabilité civile et pénale engagées.

Conditions d'applications de la loi :

Cette loi réglemente la mise en place de traitements automatisés ou non qui comportent des données à caractère personnel (article 2 de la loi).

Un traitement automatisé de données à caractère personnel : il s'agit de toute opération portant sur des informations personnelles, et notamment la collecte, l'enregistrement, l'organisation, la modification, la conservation, la communication, l'effacement et la destruction.

Une donnée à caractère personnel : il s'agit de toute information relative à une personne physique identifiée ou susceptible de l'être, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (ex : nom et prénom, date de naissance, éléments biométriques, ADN etc.).

Les obligations du responsable du traitement :
Le responsable du traitement de données à caractère personnel est (…) la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. Il doit :

- Déclarer à la Commission Nationale de l'Informatique et des Libertés (CNIL), préalablement à leur mise en œuvre, les traitements automatisés et non automatisés (dans certains cas s'agissant de ces derniers) de données à caractère personnel.
- Assurer la sécurité et la confidentialité des données enregistrées,
- Informer les personnes concernées de leurs droits (droit d'accès, de rectification et de radiation, droit d'opposition)
- Se soumettre aux contrôles et vérifications de la CNIL.

Les 5 principes clés à respecter :

- Le principe de finalité (usage déterminé et légitime)
- Le principe de proportionnalité et de pertinence des données
- Le principe d'une durée limitée de conservation des données
- Le principe de sécurité et de confidentialité des données
- Le principe du respect des droits des personnes

➢ ***Pensez à désigner un correspondant informatique et liberté (CIL)*** *à la CNIL. Cette désignation vous exonère de déclaration et le CIL contribuera à une bonne application de la loi. Toutefois, la désignation du CIL n'emporte aucune exonération de responsabilité pour le responsable du traitement.*

➢ ***Le non respect des dispositions de la loi Informatique et Liberté est passible d'une amende*** *de 300 000 euros et de 5 ans* ***d'emprisonnement*** *pour le responsable du traitement des données à caractère personnel (art. 226-16 à 24 du code pénal). En cas de reconnaissance de la responsabilité pénale de l'entreprise en tant que personne morale, les amendes sont quintuplées et les peines peuvent aller jusqu'à la dissolution (art 131-38 et 39 du code pénal).*

3- Actes et comportements également répréhensibles :

- L'enregistrement des paroles audio ou images vidéo à l'insu de l'intéressé
- L'intrusion volontaire ou involontaire dans un système informatique et l'utilisation de l'information à des fins de dénigrement
- Le vol d'information dans l'entreprise (y compris dans les poubelles situées dans les locaux de l'entreprise)
- La corruption active et/ou passive en France et à l'étranger
- L'usurpation ou l'usage de fausses identités
- La simulation de rachat d'une entreprise ou la mise en œuvre de fausses procédures juridiques pour obtenir des informations sensibles …

4- Les bonnes pratiques à utiliser dans le cadre de la collecte d'informations

- Rappeler (par exemple, par la signature d'une charte) aux collaborateurs impliqués dans la collecte d'informations, le respect des règles déontologiques et notamment en matière de :
  - droit d'auteur,
  - d'utilisation des fichiers papier ou électroniques contenant des données à caractère personnel,
  - de recours à des pratiques légales excluant l'obtention d'informations par toute pression morale ou financière ou par l'emploi de fausses identités.
- Faire signer des engagements de « bonnes pratiques » aux prestataires en intelligence économique auxquels l'entreprise recourt (cf. à titre d'exemple la charte éthique sur le site de la FEPIE - Fédération des Professionnels de l'Intelligence Economique – www.fepie.com).

Sites et documents de référence www.cnil.fr // www.clusif.fr // www.cncpi.fr // http://droit.org **//** Le Droit de l'intelligence économique, Thibault du Manoir de Juaye, LexisNexis, 2007

CADRE JURIDIQUE DE LA DIFFUSION D'INFORMATIONS A DES AUTORITES ETRANGERES

Enjeu :

Les entreprises françaises sont fréquemment sollicitées par des autorités étrangères afin d'obtenir des informations dans le cadre de procédures administratives ou juridictionnelles. Ces informations parfois sensibles sont protégées par la loi du 26 juillet 1968. De même dans la mise en œuvre de la procédure américaine du C-TPAT (export vers les Etats-Unis), les entreprises peuvent être assistées par le service des douanes.

Comment ?

1. **La loi du 26 juillet 1968** (loi n°68-678) relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères dans le cadre de procédures administratives ou judiciaires.

Ces requêtes explicites et officielles, qui ne relèvent pas de procédés illégaux tels que l'espionnage économique, peuvent néanmoins porter sur des informations sensibles pour les entreprises elles-mêmes (procédés de fabrication, savoir-faire particulier, fichiers commerciaux...) et pour la collectivité nationale dans son ensemble (informations relatives aux technologies de souveraineté, risque de dissémination).

Les grands principes de la loi

- En dehors du champ d'application d'une convention internationale, d'une loi ou d'un règlement spécifique, il est interdit à toute personne physique ou morale de répondre à une demande de renseignements visant à diffuser des informations de nature à constituer une menace notamment à l'égard de la souveraineté, de la sécurité et des intérêts économiques essentiels de la France ou permettant de constituer des preuves dans le cadre d'une procédure juridique ou administrative étrangère.
- Obligation d'informer le ministre des affaires étrangères (*lettre AR, Ministère des affaires étrangères et européennes – Direction juridique – Sous-direction du droit international et du droit communautaire*)
- Possibilité d'informer également le ministre de la justice ou le ministre de l'économie ou le ministre dont relève l'activité exercée par les entreprises qui transmettront les informations au ministre des affaires étrangères.
- Sanctions pénales : 6 mois d'emprisonnement et / ou une amende de 18 000 euros.

2. **La procédure C-TPAT** (Customs-Trade Partnership Against Terrorism)

Objectif : procédure d'agrément mise en place aux Etats-Unis après les attentats du 11 septembre 2001 afin de sécuriser la chaîne logistique d'importation des marchandises sur le territoire américain. Les importateurs agréés bénéficient de formalités de dédouanement allégées sur le plan des contrôles de sécurité permettant une réduction significative des délais de livraison.

Cible : toutes les entreprises qui exportent régulièrement vers les Etats-Unis peuvent potentiellement être sollicitées par leurs clients américains.

Processus : l'importateur américain demande à être agréé par la douane américaine et propose alors à ses fournisseurs étrangers de se soumettre à un audit (mené à partir d'un questionnaire type) de sa chaîne de logistique et de mettre en place au besoin un plan d'amélioration de la sécurité. Dans ce cadre, des visites sur site peuvent être réalisées par les services douaniers américains. La participation à ce programme n'est pas obligatoire.

Rôle de la Direction Générale des Douanes et Droits Indirects (DGDDI)

La DGDDI est informée des prévisions de déplacement des auditeurs auprès d'entreprises françaises et a **mis en place une procédure d'accompagnement** des déplacements des agents des douanes américaines.

Il s'agit généralement d'un agent du Pôle d'Action Economique (PAE) de la direction régionale des douanes, spécialisé dans les contacts avec les entreprises. Son rôle est de s'assurer, par sa présence physique, que l'audit se déroule selon le questionnaire-type. En outre, cet agent est à même, en raison de sa spécialisation, de jouer un rôle de conseil en matière de procédures douanières adaptées aux besoins spécifiques de l'entreprise auditée.

Les entreprises sollicitées par leurs clients américains en vue d'obtenir une certification C-TPAT peuvent également informer de manière spontanée leur direction régionale des douanes de rattachement.

Sites de référence : www.legifrance.gouv.fr // www.douane.gouv.fr // www.mdeie.gouv.qc.ca/ctpat // www.cbp.gov/xp/cgov/trade/cargo_security/ctpat

LE DISPOSITIF PUBLIC D'INTELLIGENCE ECONOMIQUE
(Administrations centrale et déconcentrée)

Genèse :

Le rapport du Commissariat général du Plan intitulé « Intelligence économique et stratégie des entreprises », souvent connu sous le nom de « rapport Martre » (1994) avait notamment souligné l'importance de l'Intelligence économique pour les entreprises et le retard de la France dans ce domaine. Un « Comité pour la Compétitivité et la Sécurité Economique » avait été constitué en 1995 auprès du Premier ministre puis est tombé en désuétude.

Un nouvel élan a été donné lorsqu'en janvier 2003 le Premier ministre a demandé au député Bernard Carayon de "dresser un état des lieux sur la façon dont notre pays intègre la fonction d'intelligence économique dans son système éducatif et de formation, dans son action publique et au sein du monde des entreprises" et de l'assortir de recommandations. En juin 2003, le député a remis son rapport intitulé "Intelligence économique, compétitivité et cohésion sociale", assorti de 38 propositions concernant la stratégie de l'Etat dans le domaine de la recherche et de l'innovation, la défense économique, la politique d'influence, la formation, et la mise en œuvre de l'intelligence économique territoriale.

Ses recommandations ont inspiré, fin 2003, la création d'un dispositif interministériel chargé de mettre en œuvre une politique de l'IE en France.

Qui ?

1. Le dispositif national

- **Un groupe interministériel permanent**

Le Haut Responsable à l'Intelligence Economique (HRIE) « anime un Groupe interministériel Permanent pour l'Intelligence Economique » (GPIE) qui élabore des projets ou des recommandations à l'usage du gouvernement et des administrations compétentes selon un plan d'action arrêté au plus haut niveau de l' Etat**.** Pilote d'un **dispositif souple et réactif** placé auprès du Secrétaire général de la Défense nationale (SGDN), le HRIE rend compte de son action à un comité directeur présidé par le Directeur de cabinet du Premier ministre et composé des Directeurs de cabinet des ministères concernés.
Le HRIE a proposé plusieurs actions, transposant l'essentiel des propositions formulées par le rapport CARAYON, telles que :

- La mise en place de structures (délégation ou services) d'IE dans les ministères clés ;
- La définition d'un périmètre stratégique du patrimoine scientifique et technique (14 secteurs identifiés) ;
- La création de trois fonds d'investissement spécialisés et d'un dispositif financier dédié à aider les " jeunes pousses innovantes " ;
- La définition d'un référentiel de formation à l' I E pour l'enseignement supérieur et le lancement d'une réflexion structurée sur l'insertion de modules d' I E dans les divers cursus.

Enfin, les travaux du GPIE s'appuient sur certains textes réglementaires, comme le décret réglementant les relations financières avec l'étranger (décret n° 2005 - 1739 du 30-12-2005 paru au J O n° 304 du 31-12-2005) qui impose une autorisation préalable du Ministre de l'Economie pour les investissements étrangers dans certains secteurs d'activité susceptibles d'intéresser l'ordre public, la sécurité publique ou la défense nationale et en conséquence jugés stratégiques.

- **Des ministères mobilisés**

La plupart des départements ministériels se sont progressivement dotés de structures ou ont confié à un service la coordination de leurs actions d'intelligence économique.

a) Le ministère de l'Intérieur déploie des Schéma régionaux stratégiques de l'IE

A la faveur des premiers Schémas régionaux stratégiques d'intelligence économique expérimentés en 2004 et 2005 dans quelques régions, la politique d'intelligence économique a rapidement acquis une dimension territoriale permettant d'initier des actions de sensibilisation des PME et d'assurer la protection et le suivi régional des entreprises sensibles. La conduite du dispositif territorial a été confiée au Ministère de l'Intérieur qui a généralisé par circulaire du 13 septembre 2005, complétée par la suite par celle du 8 août 2008, la démarche d'intelligence économique à l'ensemble des régions métropolitaines. Des plans triennaux ont été sollicités par la Ministre de l'Intérieur.

b) Les ministères économique et financier se sont dotés d'un dispositif transverse et territorial d'intelligence économique

La circulaire ministérielle du 21 mars 2007 (Journal Officiel du 10 mai 2007) a mis en place au sein des deux ministères économique et financier, une structure transversale à vocation opérationnelle : le Service de coordination à l'Intelligence économique (SCIE) dirigé, depuis août 2006, par un Coordonnateur Ministériel à l'Intelligence Economique (CMIE). Ce service, rattaché au Secrétariat Général commun aux Ministères de l'Economie et du Budget, s'appuie sur un réseau de 22 chargés de mission régionaux à l'intelligence économique (CRIE), placés auprès des Trésoriers - Payeurs Généraux de région. Une évolution est toutefois en cours, les CRIE devant être rattachés aux futures Directions régionales des Entreprises, de la Concurrence, de la Consommation, du Travail et de l'Emploi (DIRECCTE) dont la mise en place est en cours dans 5 régions (Aquitaine, Franche-Comté, Languedoc-Roussillon, Provence-Alpes-Côte d'Azur, Rhône-Alpes) dès 2009, pour être généralisée aux autres régions d'ici 2010.

Les principaux objectifs du SCIE sont, dans le cadre de sa participation aux missions de régulation économique de l 'Etat, de veiller à :

- La protection des entreprises constituant le patrimoine économique national stratégique ;
- La mise en œuvre de dispositifs d'intelligence économique dans les pôles de compétitivité ;
- L'appropriation par les entreprises (PMI / PME) de démarches d'intelligence économique ;
- La mise en place d'une capacité d'anticipation sur des sujets revêtant des enjeux forts pour l'économie française.

c) Ce processus s'est progressivement étendu à d'autres Ministères

Si les Ministères des Affaires Etrangères et de la Défense disposaient déjà de dispositifs d'intelligence économique, le processus s'est étendue progressivement à d'autres départements ministériels (Recherche ; Agriculture ; Ecologie, Energie, Développement durable et Aménagement du territoire…).

2. Le dispositif dans les régions

- **L'intelligence économique appliquée aux territoires**

Dans les régions, on trouve différents services de l'Etat agissant dans le champ de l'IE :

- Les administrations déconcentrées des administrations économique et financière (CRIE, futures DIRECCTE qui rassembleront notamment les DRIRE, les DRCE, les DRCCRF…, Directions Régionales des Douanes et Droits Indirects) ;
- Les autres administrations (SGAR, gendarmerie, DRRI).

Les services de l'Etat travaillent en collaboration et partenariat avec les établissements publics présents localement (INPI, OSEO…) mais également avec les autres acteurs locaux impliqués dans la mise en œuvre de démarches d'IE :

- Les collectivités territoriales, et en particulier les Conseils régionaux ;
- Les chambres de commerce et d'industrie et les chambres des métiers et d'artisanat ;
- Les universités et les grandes écoles, les fédérations et associations professionnelles…

- **Les schémas régionaux d'intelligence économique**

Suivant les préconisations du ministère de l'Intérieur, les Schémas régionaux s'articulent autour d'une structure de direction et de deux instances de déclinaison des volets offensif et défensif de l'IE (dans le Nord - Pas de Calais, précurseur en la matière, le Schéma régional stratégique de l' IE a été mis en place en février 2005 à l'initiative du Préfet de région).

- **Exemples de programmes d'actions**

* Sensibilisation des entreprises (PME) et de leurs partenaires dont les Pôles de compétitivité, aux volets offensif et défensif de la démarche de l'IE (Ubifrance pour les informations en matière d'exportation);

* Organisation et participation aux actions de communication sur l'IE (colloques, forums, débats …) ;

* Accompagnement des actions collectives et appels à projets portant sur l'IE et sur la sécurité de l'information et des systèmes d'information (une action particulière a été développée en direction des pôles de compétitivité concernant la sécurisation des plateformes numériques d'échanges d'informations) ;

* Veille sur les entreprises sensibles conjointement avec les autres services de l'Etat concernés ;

* Actions de sensibilisation et de formation à la propriété industrielle ;

* Mise en place progressive d'actions partenariales avec l'Ordre des experts comptables ;

* Concours à la mise en place de portails régionaux de l'IE (ex : Lorraine, Poitou Charentes …) ;

* Suivi d'initiatives d'IE émanant des collectivités territoriales, de groupements professionnels (ex : portails de veille de VIGILANCES en Nord - Pas de Calais ; DECILOR en Lorraine ; COGITO en Alsace, Basse Normandie…).

Dans ce cadre, les CRIE jouent un rôle de premier plan par les initiatives et les actions qu'ils déploient avec l'ensemble des parties prenantes au schéma régional.

Sites et documents de référence : site du HRIE : www.intelligence-economique.gouv.fr // Ministère de l'intérieur : www.interieur.gouv.fr // INPI : http://www.inpi.fr // OSEO : www.oseo.fr // Site régional Poitou-Charentes consacré à l'intelligence économique : fiches pratiques (www.ie-poitou-charentes.fr/?tg=oml&file=articles.ovml&ecran=3&article=135) // ACFCI : www.acfci.cci.fr/innovation/actualites.htm#ie //

LES DISPOSITIFS D'INTELLIGENCE ECONOMIQUE AUTRES QUE CELUI DE L'ETAT

(Collectivités territoriales – chambres de commerce – associations professionnelles…)

Enjeu :

Composante majeure des stratégies régionales de développement économique, les schémas régionaux d'intelligence économique recouvrent, outre l'action des services de l'Etat, celle d'autres institutions et organismes : collectivités territoriales, réseau consulaire, pôles de compétitivité, organisations professionnelles, agences locales de développement…

Ces collectivités et organismes initient et développent, seuls ou en partenariat avec d'autres acteurs publics, parapublics et/ou privés, des programmes dédiés à l'intelligence économique ou intégrant certaines de ses thématiques (veille, sécurité informatique, management de l'information et des connaissances…).

Qui ?

1. Les collectivités territoriales

Les collectivités territoriales (principalement les Conseils régionaux, dans certains cas les Conseils généraux et les Communautés d'agglomération) participent progressivement et de plus en plus activement au développement de démarches d'intelligence économiques.

L'implication des collectivités territoriales s'effectuent de plusieurs façons :

- Les Schémas Régionaux d'Intelligence Economique (SRIE), initiés par les Préfets de région, intègrent comme partie prenante les Conseils régionaux (Nord-Pas de Calais, Ile-de-France…)

Par exemple, dans le cadre du SRIE de la région Nord - Pas de Calais, le Conseil régional a partiellement financé, avec l'Etat (DRIRE) et la Chambre Régionale de Commerce et d'Industrie, une action sur la « sécurité de l'information dans les PME » en 2007

- Les Schémas Régionaux de Développement Economique (SRDE) : les Conseils régionaux peuvent dans ce cadre initier et déployer un programme ou des actions ponctuelles d'intelligence économique (Bourgogne, Champagne-Ardenne…)

Un dispositif régional d'intelligence économique en faveur des entreprises a été introduit dans le SRDE de la région Champagne-Ardenne

- Sans être engagée dans l'une ou l'autre des ces actions collectives, la collectivité appuie financièrement des actions ciblées de promotion, de diffusion ou de communication sur l'intelligence économique (financement d'aide à la veille, mise en place de portails régionaux d'intelligence économique…)

Parmi les portails régionaux dédiés à l'intelligence économique, on peut par exemple citer ceux du Poitou-Charentes (www.ie-poitou-charentes.fr/), de la Lorraine (www.decilor.org) ou de la Basse Normandie (www.basse-normandie.net)…

Les collectivités peuvent également s'impliquer dans des opérations interrégionales. C'est le cas par exemple du programme Cybermassif 2010 (développement de la sécurité des systèmes d'informations et initiation d'une démarche d'Intelligence Economique dans les entreprises du Massif Central ; www.cybermassif2010.com) qui réunit, aux côtés d'autres partenaires publics et privés (CCI, les DRIRE…) plusieurs collectivités territoriales : le Conseil régional du Languedoc Roussillon, les Conseils généraux de l'Allier, la Corrèze, la Haute-Loire, la Lozère et du Puy de Dôme, les Communautés d'Agglomération de Brive, de Clermont-Ferrand,de Montluçon, de Moulins, de Riom et de Vichy et les Communautés de Communes de la Haute Vallée d'Olt et de Tulle.

En 2005, le Conseil régional Nord - Pas de Calais et Lille Métropole Communauté Urbaine (LMCU) ont conclu avec l'ADIT une convention destinée à faire bénéficier huit filières du programme intitulé EurADIT de formation et d'accompagnement opérationnel des entreprises de ces secteurs.

2. Les Chambres de commerce et de l'industrie

Le réseau consulaire est une composante majeure du dispositif d'appui au développement économique et concourt activement dans les régions aux schémas et programmes d'intelligence économique.

Les chambres régionales et locales (www.acfci.cci.fr/annuaire/repertoire.asp) ainsi que les Agences Régionales d'Information Stratégiques et Technologiques (ARIST ; www.acfci.cci.fr/innovation/Aristcoord.htm) apportent aux entreprises aide et conseils en matière d'intelligence économique. Elles peuvent notamment :

- Les orienter sur la stratégie et la méthode (rôle du système d'information, impact des technologies, sécurité…) faciliter le montage de leur action avec des programmes d'aide ; diagnostiquer et financer des expertises ;
- Aider à valider des idées nouvelles, imaginer des nouveaux produits, découvrir de nouveaux savoir-faire ;
- Compléter leurs sources d'informations sur les concurrents, les évolutions technologiques, les brevets…

Les actions du réseau consulaire, réalisées en partenariat (Etat, collectivités territoriales, acteurs privés) ou non sont nombreuses : publications, élaboration de supports de sensibilisation et guides (par exemple la CCI Lyon : « guide pratique de la recherche d'informations sur Internet », www.lyon.cci.fr/site/document/2007060512512356_0/AE-juillet-aout2007.pdf), mise en place de formations à l'intelligence économique (par exemple les sessions de formation mises en place depuis 2008 par la CCI de Morlaix dans le Finistère), organisation de conférences / ateliers / séminaires (par exemple, les « Journées de l'innovation et de l'intelligence économique » organisées par le réseau consulaire d'Ile de France), mises en place ou participation à la mise en place de portails dédiés à l'intelligence économique et plateformes de veille (www.portail-intelligence.com/ ; www.veillestrategique.champagne-ardenne.cci.fr/ ; www.ie-poitou-charentes.fr …)

Au niveau national, l'**Assemblée des Chambres Françaises de Commerce et d'Industrie** (ACFCI ; www.acfci.cci.fr/innovation/intelligence_eco.htm), avec les chambres régionales du commerce et de l'industrie, participe à l'élaboration de la doctrine des Chambres en matière d'intelligence économique et à la diffusion d'outils et de pratiques d'intelligence économique pour les entreprises

Parmi les nombreuses actions de l'ACFCI, on peut par exemple mentionner la mise en place d'un Univers Netvibes consulaire consacré à l'intelligence économique (www.netvibes.com/ie-crci#ActualiteIE) qui est une plateforme de veille portant sur l'actualité des différentes composantes de l'IE et de ses principaux acteurs et qui présente les liens vers les différents portails consulaires d'intelligence économique mis en place par les CCI et les CRCI.

3. Les autres structures relais du développement régional

- **L'Institut National de la Propriété Industrielle** (INPI ; www.inpi.fr/fr/l-inpi/ou-nous-trouver/a-paris-et-en-region.html) : les Délégations régionales de l'INPI mettent leurs informations dans le domaine de la propriété industrielle au service des projets d'entreprises. L'INPI délivre les titres de propriété industrielle (brevets, marques, dessins et modèles et en assure la publication) et participe à l'élaboration et à la mise en œuvre des politiques publiques dans le domaine de la propriété industrielle et de la lutte anti-contrefaçon.
- **OSEO** (www.oseo.fr) : les 22 directions régionales d'OSEO (www.oseo.fr/notre_mission/nos_equipes_en_region) ont pour mission de financer et d'accompagner les PME, en partenariat avec les banques et les organismes de capital - investissement, dans les phases les plus décisives du cycle de vie des entreprises. OSEO innovation apporte aux innovateurs et aux entrepreneurs des services d'ingénierie et d'accompagnement, dans le cadre d'une approche globale (appui aux projets collaboratifs, accompagnement personnalisé, aide financière à l'innovation…)
- **L'Agence de Diffusion de l'Information Technologique** (ADIT ; www.adit.fr) dispose de plusieurs représentations en France (Lille, Paris, Caen, Strasbourg, Poitiers…). A Lille par exemple, l'ADIT Nord - Pas de Calais développe ses services, dans le cadre du programme EurADIT (www.adit.fr/euradit/public/index.php), auprès des entreprises des filières textile, bio-santé, ferroviaire, production aquatique, en liaison avec les pôles de compétitivité de la région ;

- **Les Chambres des Métiers et de l'Artisanat** : ce réseau structuré au niveau départemental, régional et national (http://212.43.237.181/cferm/annuaires/portail/index.html) participe, en partenariat avec d'autres acteurs publics ou privés, à des démarches d'intelligence économique comme en témoigne par exemple la mise en place dès 2002 par la Chambre de Métiers et d'Artisanat d'Annecy d'une démarche d'intelligence économique reposant notamment sur le développement un outil de veille (www.adbs.fr/regions/IMG/doc/CR_veille_CMA74.doc) ou bien encore la participation de la Chambre régionale des métiers et de l'artisanat de Poitou-Charentes à la création du portail régional consacré à l'intelligence économique (www.ie-poitou-charentes.fr)
- L'**Agence française pour le développement international des entreprises** (Ubifrance ; www.ubifrance.fr) : cet établissement public, industriel et commercial offre aux entreprises souhaitant exporter ou s'implanter à l'étranger des informations réglementaires, commerciales…

4. Les organisations et groupements de professionnels

- **Les pôles de compétitivité** (www.competitivite.gouv.fr): compte tenu du caractère stratégique et très sensible de leur patrimoine informationnel, les pôles de compétitivité ont vocation à mettre en place rapidement des dispositifs d'intelligence et de sécurité économiques opérationnels et performants
- Les **Clubs de la Sécurité Informatique** (www.clusif.asso.fr/fr/clusir/): relais régionaux du Club de la sécurité informatique français (CLUSIF), les CLUSIR ont pour vocation de faciliter les échanges relatifs à la sécurité informatique entre tous les acteurs économiques du tissu régional, faire prendre en compte la réalité des risques et améliorer la sécurité de l'information dans les entreprises
- Les **associations de prestataires de services d'intelligence économique** : l'association EVEIL EURO NORD dans le Nord Pas de Calais, www.eveil-euronord.org/ ; l'association ADIESA en région Centre, www.adiesa.net/ ; l'association Vigilances, www.vigilances.fr …)
- La **Fédération des Professionnels de l'Intelligence Economique** (FEPIE ; www.fepie.com/) est une association regroupant au niveau national des professionnels de l'intelligence économique. Sa mission est de structurer, organiser, encadrer les activités d'intelligence économique
- Le **Mouvement des entreprises de France** (MEDEF ; www.medef.fr/medias/upload/75808_FICHIER.pdf)
- La **Confédération Générale des Petites et Moyennes Entreprises** (CGPME ; http://www.cgpme75.fr/index.php?module=sspages&id=7)
- Certaines associations régionales membres des **Dirigeants et Commerciaux de France** (DCF : www.dcf-france.fr/asso-chateauroux/page6.php) comme dans la région Centre (en mars 2007, le Ministère de l'Economie, des Finances et de l'Industrie représenté par le Trésorier Payeur Général du Loiret et de la région Centre et l'association Centre des Dirigeants Commerciaux de France ont signé une convention de partenariat portant sur des sessions de sensibilisation –formation-action- à la démarche d'intelligence économique en région Centre)
- L'**Ordre des Experts Comptables** (www.intelligence-experts.fr) : en ce qui concerne l'intelligence économique et financière, les experts-comptables ont développé une méthode d'identification des facteurs de vulnérabilités ressortant des comptes annuels des entreprises, en vue de les aider à saisir les opportunités de développement à partir d'une vielle intelligente de collecte et maîtrise d'informations.

GLOSSAIRE DES SIGLES UTILISES

ACFCI	Assemblée des chambres françaises de commerce et d'industrie
ADIT	Agence de diffusion de l'information technologique
ARIST	Agence régionale d'information stratégique et technologique
C (R) CI	Chambres (régionales) de commerce et de l'industrie
CGPME	Confédération générale des petites et moyennes entreprises
CLUSIF	Club de la sécurité de l'information français
CLUSIR	Club de la sécurité de l'information régional
CMIE	Coordonnateur ministériel à l'intelligence économique
CNIL	Commission nationale de l'informatique et des libertés
CREDOC	Centre de recherche pour l'étude et l'observation des conditions de vie
CRIE	Chargé de mission régional à l'intelligence économique
DCF	Dirigeants et commerciaux de France
DCRI	Direction centrale du renseignement intérieur
DCSSI	Direction centrale de la sécurité des systèmes d'information
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes
DGDDI	Direction générale des douanes et droits indirects
DGTPE	Direction générale du trésor et de la politique économique
DIRECCTE	Direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi
DPSN	Direction de la planification de sécurité nationale
DRCCRF	Direction régionale de la concurrence, de la consommation et de la répression des fraudes
DRCE	Direction régionale du commerce extérieur
DRDDI	Direction régionale des douanes et droits indirects
DRIRE	Direction régionales de l'industrie, de la recherche et de l'environnement
FEPIE	Fédération française des professionnels de l'intelligence économique
GPIE	Groupe interministériel permanent pour l'intelligence économique
HRIE	Haut responsable à l'intelligence économique
IE	Intelligence économique
INHES	Institut national de hautes études de sécurité
INPI	Institut national de la propriété industrielle
MEDEF	Mouvement des entreprises de France
OMPI	Organisation mondiale de la propriété intellectuelle
SCIE	Service de coordination à l'Intelligence économique
SGAR	Secrétariat général pour les affaires régionales
SGDN	Secrétaire général de la défense nationale
SRDE	Schéma régional de développement économique
SRIE	Schéma régional d'intelligence économique
SSI	Sécurité des systèmes d'information

Service de coordination à
l'intelligence économique