L'INTELLIGENCE JURIDIQUE, LE DROIT AU SERVICE DE L'INTELLIGENCE ECONOMIQUE

Dans un contexte de compétition économique globale exacerbée[1] s'est développé depuis plus d'une vingtaine d'années désormais le concept d'intelligence économique qui se définit communément comme étant « *la maîtrise et la protection de l'information stratégique pertinente pour tout acteur économique* »[2].

A ce titre, le projet de loi nommée LOPPSI II[3] est appelé à délimiter les contours de l'activité privée d'intelligence économique qui seraient définis comme « *consistant dans la recherche et le traitement d'informations sur l'environnement économique, commercial, industriel ou financier d'une ou plusieurs personnes physiques ou morales, destinées soit à leur permettre de se protéger des risques pouvant menacer leur activité économique, leur patrimoine, leurs actifs immatériels ou leur réputation, soit à favoriser leur activité en influant sur l'évolution des affaires ou les décisions de personnes publiques ou privées* ».

Afin de répondre à cette démarche pluridisciplinaire visant notamment à protéger le patrimoine informationnel et les secrets d'affaires, l'intelligence juridique, apparue plus récemment[4], peut se présenter comme étant l'ingénierie juridique appliquée à l'intelligence économique.

Pour ce faire, la matière se propose d'offrir à l'entreprise les moyens juridiques adéquats pour se protéger utilement contre les atteintes et les actes de malveillance et plus généralement pour maîtriser les risques juridiques liés aux marchés et à son environnement commercial et industriel, dans un monde toujours plus concurrentiel.

L'objectif louable est ainsi de sécuriser et de faire valoir les droits incorporels et immatériels dont l'entreprise peut se prévaloir. Ce faisant, l'intelligence juridique aborde de manière transversale tous les aspects liés à la structure même de l'organisation de l'entreprise et de ses activités.

En d'autres termes, c'est « *une démarche organisée, au service du management stratégique de l'entreprise, visant à améliorer sa compétitivité par la collecte, le traitement d'informations et la diffusion de connaissances utiles à la maîtrise de son environnement.* »[5]
Le droit est donc indubitablement l'une des composantes essentielle de l'intelligence économique, en voici les principaux ressorts.

[1] D'aucuns parlent ouvertement, à juste titre, de « guerre économique ».
[2] Selon le site officiel : www.intelligence-economique.gouv.fr
[3] Le projet de Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure, adopté en première lecture par l'Assemblée nationale le 16 février dernier, prévoit de soumettre les professionnels à une procédure d'agrément délivré par le ministre de l'Intérieur. Le non-respect de cette obligation serait passible de trois ans d'emprisonnement et de 45 000 euros d'amende (ainsi que de la fermeture de l'établissement se livrant aux activités illégalement).
[4] « L'intelligence juridique, une nouvelle matière en train d'émerger », Paris Entreprises, n°58, novembre-décembre 2002
[5] Bournois F. et Romani P.-J., « L'Intelligence économique et stratégique dans les entreprises françaises », IHEDN, Economica, 2000

LA CONSTITUTION DU PATRIMOINE INFORMATIONNEL, UN CODE DE BONNES PRATIQUES

S'il est admis que 90% des sources sont librement accessibles, qualifiées « d'informations ouvertes », certains secrets d'affaires sont néanmoins à déceler parmi les 10% restant. Or, le droit fixe expressément les limites au-delà desquelles leur transgression devient un acte répréhensible.

Ainsi, pour se conformer à de bonnes pratiques, l'intelligence juridique répertorie dans cette optique de collecte de données stratégiques le cadre légal applicable :

- déclarations à la CNIL concernant la constitution de fichiers personnels,
- règles relatives à la surveillance du personnel de l'entreprise et des moyens matériels mis à disposition,
- utilisation des services d'agences de détectives privés,
- mise en place d'un service de veille économique et juridique,
- introduction d'un procès comme mode d'acquisition d'information,
- utilisation du droit de dénonciation,
- le régime des écoutes et vidéosurveillance,
- statut juridique des entreprises de sécurité,
- établissement d'une liste des agissements prohibés,
- la notion de secret professionnel,
- mise en place de boîtes de dialogue avec les autorités (DRI, impôts) ...

Enfin, n'oublions pas que ce patrimoine informationnel n'est pas seulement constitué de renseignements obtenus à l'extérieur, mais qu'il peut être aussi une création interne de l'entreprise. Il faudra donc veiller à protéger utilement les innovations de cette dernière sous couvert des droits de propriété intellectuelle.

En tout état de cause, et dans tous les cas de figures, un audit juridique préalable se révèlera donc nécessaire pour :

- Mettre en place une veille juridique spécifique,
- Définir le périmètre du patrimoine informationnel de l'entreprise,
- Mettre en place de mesures de protection de données dématérialisées,
- Mettre en œuvre des modes opératoires juridiques de prévention adaptés.

LA PROTECTION DES SECRETS D'AFFAIRES, UNE NECESSITE ECONOMIQUE

Une fois bâti, ce patrimoine informationnel, constitué de pratiques commerciales et de secrets d'affaires, est dès lors censé procurer à son titulaire un avantage économique déterminant sur ses concurrents ; en revanche, toute atteinte ou divulgation d'une donnée stratégique – le cas le plus symptomatique étant l'espionnage – peut se révéler particulièrement destructeur.

Le droit permet donc également de mettre en place au sein de l'entreprise un mode de protection adapté à son organisation structurelle pour palier cette vulnérabilité. Au-delà des mesures de protection technique, numérique et biométrique, et à défaut d'une législation spécifique, tous les pans du droit seront ainsi être mobilisés pour assurer la sécurité du patrimoine immatériel.

Sans vouloir établir un inventaire à la Prévert, citons les principaux traits qui devront être utilement combinés pour se révéler efficaces :

- En droit des sociétés, on peut notamment citer des dispositions statutaires à destination des associés telles que les clauses d'agrément en vue de filtrer les nouveaux entrants qui pourraient ainsi accéder à certaines informations privilégiées dans le cadre de l'exercice de leur droit de communication ou d'expertise de gestion, des clauses de non-concurrence pour éviter de voir un ex-partenaire développer une activité similaire à l'appui des fichiers de l'entreprise, des seuils d'alerte comme en matière d'OPA… Les pactes peuvent aussi définir et compartimenter les droits d'accès.
- En droit commercial, dans les accords et contrats de distribution ce sont des clauses spécifiques, d'exclusivité, de non débauchage, qui seraient négociées en vue d'éviter de voir un homme clef être recruté par un partenaire économique, voire un concurrent et de non-concurrence dont le périmètre devra être bien délimité notamment dans le temps et l'espace, mais aussi des protocoles de confidentialité dédiés ainsi que des chartes de bonne conduite et de loyauté, incontournables dans un schéma de franchise. Il importe que ces dispositions contractuelles soient particulièrement bien rédigées.
- En droit économique, outre la protection des droits immatériels et intellectuels tels que enregistrement de marques, dessins et modèles et brevets, mais aussi de bases de données, logiciels … , en termes de recherche et développement il est nécessaire de recourir à des conventions particulières précisant le périmètre de confidentialité, la propriété des droits en découlant et leur protection ainsi que leur utilisation par chaque partie. Cela est notamment essentiel dans les contrats industriels de production à façon ou de sous-traitance.
- En droit des nouvelles technologies, il conviendra par exemple, de mettre en place une charte de bonne conduite et de loyauté avec les partenaires extérieurs pour la conservation sécurisée des donnés externalisées ou de procéder, en interne, à un compartimentage des données essentielles et à un accès limité avec mots de passe et login.
- En droit social, il est possible de définir des clauses de confidentialité et de bon usage des outils informatiques insérées dans les contrats de travail et de mettre en œuvre une charte informatique. En fonction de la qualité du salarié, et de son niveau de responsabilités, le contrat devra être adapté en conséquence et comprendra diverses clauses spécifiques, mentionnant par exemple les outils informatiques auxquels il aura accès ou qui lui sont confiés avec les dispositions relatives à leur utilisation et à

leur conservation. La charte aura, pour sa part, vocation à s'appliquer à tout le personnel et répond aux normes du règlement intérieur dont elle pourra être un additif. Elle devra préciser, entre autres choses, les sanctions en cas de non-respect des obligations, énoncer les règles d'utilisation des ressources numériques, les modes et procédés d'utilisation des outils informatiques, les méthodes de sauvegarde... jusqu'à limiter l'accès à Internet et l'utilisation de la messagerie. Le tout dans le respect des règles contraignantes du droit du travail.

Si ces mesures non exhaustives prises par l'entreprise pour mettre ses données et informations sensibles à l'abri d'un vol ou d'un détournement sont indispensables, elles n'offrent jamais une garantie totale tant le facteur humain est la première cause de fragilité.

LES VOIES DE RECOURS :
REPLIQUER ET REPARER L'HEMORRAGIE

Dans l'hypothèse où l'entreprise est titulaire d'un droit de propriété intellectuelle, comme vu ci-dessus, elle pourra utilement introduire un recours en contrefaçon[6] qui se résout habituellement en dommages et intérêts destinés à réparer le préjudice subi, à défaut de sanction financière dissuasive et hors recours pénal admis en cette matière. Cette procédure spécifique vise également à interdire l'usage desdits droits au contrefaisant, sous astreinte.

A défaut de disposer de tels droits privatifs, le demandeur devra alors intenter une action en concurrence déloyale dans les conditions retenues par les tribunaux et dégagées par la doctrine[7].
A cet égard, l'atteinte au patrimoine informationnel la plus fréquente est celle du salarié indélicat qui fait usage de secrets enregistrés chez son employeur à des fins personnelles[8] à moins qu'il ne les mette en œuvre chez un concurrent[9]. De même, le débauchage de salariés[10] est souvent sanctionné à la condition toutefois de démontrer que le nouvel employeur avait effectivement l'intention de s'approprier les secrets du concurrent. Enfin, le détournement de fichiers commerciaux alimente un contentieux abondant[11].

Si ces ripostes se veulent efficaces, elles ont cependant essentiellement vocation à réparer le préjudice sous une forme financière, souvent difficilement quantifiable, sans autre effet dissuasif[12], si le défendeur n'est pas en outre insolvable. La voie pénale pourrait dès lors se révéler plus décisive et immédiate. Or, à l'exclusion des cas particuliers d'atteinte aux intérêts stratégiques de l'état, il n'existe que très peu de textes qui sanctionnent précisément l'atteinte et la divulgation du patrimoine informationnel, le vol en étant a priori exclu.

En effet, le vol se définit par la soustraction frauduleuse du bien dans l'actif de la victime, et son transfert corrélatif dans le patrimoine du voleur ; tel n'est pas le cas pour une copie numérique car les donnés initiales demeurent dans le patrimoine de la victime. En outre, les tribunaux ont très longtemps été réticents à reconnaître le vol de données dématérialisées, ne retenant que la disparition de biens incorporels expressément attachés à un support matériel.
A cet égard, la Cour d'appel de Paris[13] a, en 1992, estimé que : « *des transferts qui portent exclusivement sur des données immatérielles,* (...) *ne sauraient entrer dans le champ d'application* [du vol] (...) *; qu'il est, en outre, manifeste que ces opérations de copiage, n'ayant entraîné aucun transfert dans la possession des données informatiques, ne sauraient être à elles seules constitutives d'une soustraction* ». Cette jurisprudence était constante à l'exception de vols reconnus de temps-machine.
La Cour de cassation a pour la première fois retenu la qualification de vol de données informatiques, en 2003, énonçant que « *le fait d'avoir en sa possession,* (...) *sans pouvoir justifier d'une autorisation de reproduction et d'usage du légitime propriétaire, qui au contraire soutient que ce programme source lui a été dérobé, caractérise suffisamment la*

[6] Par exemple : article L 111-1, L 112-2, L 335-2 et suivants du Code de la propriété intellectuelle
[7] On doit au doyen Roubier (Roubier P., Le droit de la propriété industrielle, t. I, éd. Sirey, 1952, n° 110) une classification des moyens concurrentiels déloyaux sous quatre rubriques : les moyens de confusion, le dénigrement, la désorganisation interne d'une entreprise rivale,et, enfin, la désorganisation générale du marché.
[8] Cass. Com. 8 janvier 1979, CA Paris 21 juin 1989
[9] CA Paris 27 septembre 2000, Cass. Com.19 décembre 2000
[10] Cass. Com. 19 novembre 1991, CA Paris 15 janvier 1997, Cass. Com. 30 janvier 2001
[11] Cass. Com 20 octobre 1998, Cass. Com. 30 janvier 2001
[12] Le droit positif français ne prévoit pas de dommages et intérêts « punitifs », ou amende civile.
[13] CA Paris, 13e ch. A, 25 novembre 1992

soustraction frauduleuse de la chose d'autrui et la volonté de s'approprier les informations gravées sur le support matériel »[14]. Cette décision demeure néanmoins isolée et discutée.
C'est pourquoi les juristes sont particulièrement attentifs au traitement qui sera réservé à la proposition de loi CARAYON relative à *la protection des informations économiques* visant à introduire dans le Code pénal le délit d'atteinte « au secret d'une information à caractère économique protégée ».
Ce texte audacieux prévoit de punir d'un an d'emprisonnement et de 15.000 euros d'amende le fait « *pour toute personne non autorisée par le détenteur ou par les dispositions législatives et réglementaires en vigueur, d'appréhender, de conserver, de reproduire ou de porter à la connaissance d'un tiers non autorisé une information à caractère économique protégée*. »
Un tel dispositif offrirait sans conteste un outil supplémentaire au service de l'intelligence juridique.

Olivier de MAISON ROUGE
Avocat au Barreau de Clermont-Ferrand
DEA de Droit des Affaires – Docteur en Droit
Enseignant ESC CLERMONT
32 Avenue Julien 63000 CLERMONT-FERRAND
Tel : 04.73.19.43.19 / Fax : 04.73.93.07.97
Mail : odemaisonrouge@orange.fr

[14] Cass. Crim., 9 septembre 2003