REVUE DE PRESSE

Une semaine d'espionnage industriel

20 novembre 2011
Semaine 47 / 2011

Edito :

Cette semaine c'est encore l'affaire Renault qui tient le haut du panier dans la presse, qu'elle soit spécialisée ou non. Il faut dire que l'affaire a fait grand bruit avec tous les bons ingrédients d'un polar digne des années 70 ! Service(s) de renseignement, monde économique, fleuron de l'industrie française, barbouzes et donneurs d'ordre obscurs, voilà le plat de résistance. Tout cela pourrait être risible si ce n'est que trois cadres dirigeants avaient été licenciés et que l'affaire avait défrayé la chronique. L'affaire prend une nouvelle tournure cette semaine avec une perquisition menée dans le bureau de l'assistante personnelle de Carlos GOSHN.

Bonne nouvelle par contre pour la sécurisation des actifs et des patrimoines immatériels des entreprises nationales françaises. Et c'est le député CARAYON lui-même qui monte au créneau en déposant une proposition de loi qui vise à sanctionner la violation du secret des affaires. Le célèbre député estime notamment que « *les entreprises ont le droit à une vie privée* » ! Bonne nouvelle en effet lorsque l'on sait que les faits d'espionnage industriel sont souvent commis avec une complicité interne et que les auditorats du travail et autres « Prud'hommes » ont une fâcheuse tendance à secourir le plus faible – l'employé – qui bénéficie lui de toute une batterie de lois et de jurisprudences traitant de la « sacro sainte » vie privée. Une nouvelle affaire « A400M[1] » serait-elle alors gérée différemment avec l'application d'une telle loi ?

Si à l'Est, il n'y a pas grand-chose de nouveau cette semaine, il n'en va pas de même pour le Nord de l'Europe. Un nombre non confirmé (on parle visiblement d'au moins dix crimes informatiques) de sociétés norvégiennes a connu une vague d'attaques informatiques réalisées par une société d'espionnage informatique. La plupart des articles traitant du sujet évoquent encore une fois l'ombre du gouvernement chinois. La Chine serait donc encore derrière ces faits d'espionnage ? Quand je vous disais qu'à l'Est il n'y avait rien de nouveau !

AFL.

[1] Voir nos articles du 8 novembre 2011

REVUE DE PRESSE

Une semaine d'espionnage industriel

20 novembre 2011
Semaine 47 / 2011

L'affaire Renault, ça s'en va et ça revient.

« L'affaire avait été tellement houleuse qu'elle avait entraîné la démission du numéro 2 de Renault, Patrick PELATA. Aujourd'hui, l'affaire d'espionnage chez le constructeur français n'est toujours pas close. » Lire l'article (Turbo.fr)

« Près de neuf mois après l'ouverture de l'instruction sur la tentative d'escroquerie au renseignement dont RENAULT a été victime, de nouvelles perquisitions ont eu lieu mercredi 16 novembre, au plus haut niveau de la direction. » Lire l'article (Usine Nouvelle)

« Le juge d'instruction de l'affaire RENAULT a fait perquisitionner le bureau de Carlos GOHSN. » Lire l'article (France Soir)

Notre avis :

Si la perquisition fait partie de la procédure et qu'elle est une suite normale de l'instruction, il faut quand même avouer que la responsabilité des dirigeants doit être engagée. Après tout, comment ne pas penser que le recrutement de l'ancien directeur de la sécurité n'avait pas été validé par Carlos GOHSN ? Lorsque l'on connaît la « proximité » qui doit exister entre un directeur sécurité – ou sûreté d'ailleurs – et sa direction, il semble légitime que l'entourage direct du dirigeant doit faire l'objet d'investigations particulières.

Cependant, on ne parle plus des sous-traitants ayant réalisé la frauduleuse mission de « collecte » de documents ! Exit aussi les prestataires qui ont trempé ou pas dans la « magouille »...

Une semaine d'espionnage industriel

Le secret des affaires est l'équivalent du secret défense !

« Le député UMP Bernard CARAYON, membre du collectif de la Droite populaire, a déposé jeudi une proposition[2] de loi visant à sanctionner la violation du secret des affaires. Le texte, qui pourrait être examiné dès le mois de janvier, punit d'un an de prison et de 15.000 euros d'amende la divulgation "d'informations économiques" que les entreprises veulent garder secrètes. Une manière de dissuader l'espionnage industriel. L'élu du TARN revient pour leJDD.fr sur sa proposition. » Lire l'article (JDD)

« Le député Bernard CARAYON, appuyé par plus d'une centaine de collègues des bancs de l'UMP, a déposé une proposition de loi qui condamne d'une peine d'emprisonnement le fait de divulguer des "informations économiques" qu'une entreprise souhaite garder secrètes. La presse, qui publie régulièrement des informations et des rumeurs sur les activités et les projets des entreprises, est directement concernée. » Lire l'article (Numerama)

Notre avis :

Comme à son habitude, le député Bernard CARAYON fournit une analyse claire de la situation et tente de voler au secours du patrimoine immatériel des entreprises françaises. Si ce combat est à saluer, il est toutefois dommage de constater que peu d'élus français semblent être concernés par la chose et conscients de la nécessité de protéger les actifs économiques fussent-ils immatériels.

Encore que la France jouit quand même d'une avancée en la matière par rapport à ses voisins directs ! Belgique, Luxembourg, Italie et Espagne font figure de mauvais élèves face à l'Allemagne et au Royaume-Uni dotés d'un arsenal de lois contre l'espionnage.

Le cas de la Belgique pose toutefois un problème de taille puisqu'elle accueille en son sein – et pas uniquement à Bruxelles – de nombreuses entreprises étrangères et nationales qui sont, elles aussi, victimes d'actes d'espionnage économique. Rappelons que l'affaire RENAULT avait eu certaines suites et dossiers connexes sur le sol belge.

A quand un élu belge mettant sur la table les problèmes liés au manque d'outils juridiques pour éviter sinon sévir lorsque l'atteinte à la vie privée de l'entreprise est avérée ?

[2] http://www.assemblee-nationale.fr/13/propositions/pion3103.asp

REVUE DE PRESSE

Une semaine d'espionnage industriel

20 novembre 2011
Semaine 47 / 2011

A l'Est rien de nouveau ! Quoique…

« OSLO - De la défense à l'énergie, les sociétés norvégiennes ont été cette année la cible d'une entreprise d'espionnage informatique sans précédent dans le pays scandinave, a annoncé un service de renseignement norvégien. » Lire l'article (Romandie.com)

Plus d'infos :

Ce n'est pas la première fois que la Chine est montrée du doigt lors d'attaques informatiques ayant pour finalité l'espionnage économique. Il semblerait d'ailleurs que les entreprises chinoises puissent se reposer activement sur les services de renseignement du pays.

Pour rappel, la Chine est dotée d'une organisation du renseignement importante directement placée sous le secrétariat du Parti Communiste. Ainsi *le Département des Investigations* (DIAOCHABU) et le *Département des Affaires Spéciales* (TEWU) ont dans leurs prérogatives le renseignement économique à l'étranger et sur le territoire. A noter aussi que tout ce qui concerne le *renseignement technologique* dépend essentiellement du QINGBAO, le *service de renseignement militaire*.

REVUE DE PRESSE

Une semaine d'espionnage industriel

20 novembre 2011
Semaine 47 / 2011

Brèves :

Des sociétés « télécoms » chinoises espionnent les US

« Une commission de la Chambre des représentants américaine a lancé une enquête sur la menace en termes de sécurité nationale que pourraient poser des entreprises de télécoms basées aux Etats-Unis et appartenant à des Chinois, a-t-elle annoncé jeudi. Pékin est soupçonné de s'appuyer sur ces entreprises pour mener des missions d'espionnage industriel ou militaire, selon le communiqué signé du président de la commission du Renseignement intérieur, Mike ROGERS, et du parlementaire Dutch RUPPERSBERGER. » (Europe 1 & AFP)

Cinq techniques pour percer les secrets de vos concurrents

« Avec de la persévérance et un peu d'astuce, vous pouvez facilement vous transformer en limier du renseignement commercial. A vous de jouer, mais avec prudence... d'autant qu'une nouvelle loi vise à punir l'espionnage industriel. » Lire l'article (Capital.fr)

Cyber-attaque et l'Iran

« On peut penser que les hackers, ces cyber délinquants, sont des personnes isolées qui attaquent, bien souvent pour le défi. En réalite, la cyberguerre, entre états, existe aussi. Espionnage, attentat, Marie VANTCUTSEM vous plonge dans l'envers de la toile. Ecouter (RTBF)

Du hacking en orbite

« Le rapport d'une commission du Congrès US révèlerait, nous apprend Bloomberg, qu'à quatre reprises, des hackers probablement d'origine chinoise, auraient tenté de compromettre l'uplink d'une station de contrôle de satellites d'observation. Un Landsat 7 et un Terra AM-1 auraient ainsi souffert de ruptures de communications durant plusieurs minutes. » Lire l'article (LeMag)

Vous protéger:

Vous désirez connaître l'exposition aux risques d'espionnage industriel de votre entreprise ? Nous vous proposons un diagnostic des risques auxquels vous avez à faire face ainsi qu'une évaluation par rapport à votre secteur d'activités. Contact.

FIN.