

Extrait du Spyworld Actu

<http://www.spyworld-actu.com/spip.php?article14400>

Espionnage industriel : la tentation sécuritaire

- Intelligence économique -



Date de mise en ligne : lundi 31 janvier 2011

Spyworld Actu

Espionnage industriel, vol de brevets ou de technologies, cybercriminalité, enlèvement d'expatriés, mais aussi fraudes, pots-de-vin versés aux salariés, les entreprises sont menacées aussi bien par la grande criminalité que par la petite délinquance.

Le risque de malveillance est élevé : lors d'une enquête réalisée en 2009 par le cabinet Pricewaterhouse Coopers, une entreprise européenne sur quatre déclarait avoir été victime d'une fraude au cours de l'année écoulée, et plus d'une fois sur deux celle-ci impliquait des salariés.

Le Financial Times observait le 12 janvier que "la plus grande vulnérabilité de la plupart des entreprises, comme l'affaire Renault semble le montrer, est leur propre personnel". Elles ne doivent donc pas se protéger seulement des prédateurs externes - le plus souvent d'autres entreprises -, mais aussi de leurs propres collaborateurs qui pourraient accepter non seulement d'être corrompus, mais aussi de corrompre.

ETHIQUE DES AFFAIRES

La première responsabilité des entreprises est de se comporter en toutes choses conformément à l'éthique des affaires. Les articles d'Anne Sachet-Milliat, Ludovic François et Mathieu Pellerin, publiés dans le numéro "Spécial éthique" de la revue Sécurité et Stratégie (juillet-septembre 2010), viennent opportunément rappeler la difficulté de l'exercice.

En réalité, l'entreprise n'a, à proprement parler, ni morale ni éthique, mais seulement "des objectifs et un bilan" (André Comte-Sponville, *Le capitalisme est-il moral ?*, Albin Michel, 2004).

Etre vertueux relève donc de la responsabilité individuelle. En conséquence, pour qu'il y ait de la morale dans l'entreprise, les dirigeants doivent être eux-mêmes exemplaires, puis agir positivement sur le comportement de leurs salariés. Le but est de prévenir toute pratique délictueuse de leur part, fût-elle réalisée au profit de l'entreprise.

Les spécialistes en intelligence économique montrent que le travail de renseignement mené à cette fin, s'il ne relève pas de l'espionnage proprement dit, recourt trop souvent à des manipulations ou à des mensonges.

REGLES DEONTOLOGIQUES CLAIRES

La gestion des ressources humaines et le management doivent donc édicter et diffuser des règles déontologiques claires et réalistes, informer sur les risques encourus au plan pénal en cas de faute, intégrer des cas "éthiques" aux formations, etc.

L'affaire Kerviel a rappelé à quel point le contexte organisationnel conditionne les comportements, et combien il est nécessaire d'expliquer les règles et de les intégrer à l'animation quotidienne des équipes. Au-delà, comment chacun peut-il agir face à un problème délicat ?

Des outils existent, tel le "public disclosure test" : il s'agit pour tout professionnel confronté à un cas de conscience de se demander comment il se sentirait si l'action qu'il s'apprête à faire était rendue publique ; pourrait-il l'assumer ? Cette politique existe chez Renault, qui a nommé un "déontologue", assisté d'un comité au niveau du groupe.

Elle n'assure pourtant pas une protection totale. Ce constat a amené certains dirigeants à élaborer des dispositifs de

Espionnage industriel : la tentation sécuritaire

surveillance de certains collaborateurs, impliqués dans des dossiers sensibles ou stratégiques.

Mais privilégier la sécurité au détriment de la confiance pose d'autres problèmes : comme dans la société, il est impératif de bien encadrer ces dispositifs sécuritaires.

Post-scriptum :

<http://www.lemonde.fr/idees/article...>