Les espions d'entreprises

- Renseignement - International -

Date de mise en ligne : mardi 19 dÃ©cembre 2006

Spyworld Actu

Chez Hewlett Packard (HP), géant américain de l'informatique, on n'en revient toujours pas de la chute de la présidente, Patricia Dunn. Comment peut-on reprocher à un chef d'entreprise de vouloir identifier l'auteur de fuites dans son propre conseil d'administration ?

A la direction de la sécurité, au siège de HP France, l'amertume est d'autant plus grande que l'entreprise se targue de grandes vertus déontologiques. Ce n'est cependant pas l'objectif en tant que tel que la justice américaine avait reproché à la direction, mais bien les moyens utilisés pour traquer le coupable. L'agence de détectives privés engagée par HP a, en effet, usé de fausses identités et espionné journalistes et administrateurs suspects. La justice californienne a fini par abandonner les poursuites le 8 décembre en échange d'un versement de 14,5 millions de dollars. La taupe, elle, a été identifiée et priée de quitter le conseil. Mais son départ aura provoqué une crise profonde au sein de la multinationale. Les accusés, quant à eux, risquent cinq ans de prison.

"La démarche de Hewlett Packard était justifiée, mais le groupe aurait dû contrôler les moyens employés pour mettre fin aux fuites", reconnaît un expert en la matière, Alain Juillet, haut responsable de l'intelligence économique auprès du gouvernement français. Selon lui, "les entreprises françaises aussi doivent se protéger des trahisons". De fait, le succès du raid hostile mené, entre janvier et juin 2006, par le géant de l'acier, Mittal, sur le groupe Arcelor devrait beaucoup aux informations livrées par une taupe située au coeur du dispositif adverse.

Au plus fort de la tension entre les deux groupes, le milliardaire indien Lakshmi Mittal connaissait la position exacte du français. Ainsi aurait-il pu ajuster, à plusieurs reprises, sa stratégie et le prix offert pour le rachat des actions convoitées. Durant cette période, confie l'un des administrateurs, la direction d'Arcelor imposa de fortes restrictions en matière de copie de documents et de communication avec l'extérieur. Mais rien n'y fit. Mittal savait tout. Ce sont les services secrets français, invités dans la partie, qui parvinrent finalement à identifier la taupe, un homme d'origine espagnole. La victoire finale de Mittal sur Guy Dollé, le très isolé président d'Arcelor, a garanti à cet informateur une place de choix dans l'organigramme du nouveau groupe, Mittal-Arcelor. Jamais la notion de "guerre économique" entre entreprises n'a paru aussi appropriée qu'aujourd'hui. La sécurité des systèmes informatiques et de télécommunications est désormais intimement liée aux stratégies de conquête de nouveaux marchés et de protection des patrimoines industriels. L'énormité des enjeux financiers interdit toute naïveté.

En cinq ans, le nombre de sociétés de sécurité spécialisées dans le secteur de l'espionnage économique a été multiplié par six. Elles sont aujourd'hui environ 300. Cambriolages, corruption, intrusion informatique, écoutes téléphoniques, sont des activités évidemment illégales mais qui seraient à l'occasion pratiquées, y compris en France.

L'atmosphère de guerre entre entreprises innovantes les a conduites à renforcer leurs protections face aux menaces extérieures, réelles ou supposées. Une "culture du soupçon" s'est établie un peu partout, et ses première victimes sont souvent les salariés eux-mêmes. Ainsi les dirigeants de l'usine Smart France en Moselle ont été poursuivis pour "atteinte à la vie privée", avant d'être relaxés par la cour d'appel de Metz le 23 novembre dernier. Un employé avait découvert dans les toilettes hommes une caméra de surveillance miniaturisée. "Raisons de sécurité", s'est défendue la direction. La cour a estimé que les toilettes étant "le prolongement du lieu de travail", il n'y avait rien à redire.

Le principe de sécurité prévaut désormais sur tout autre argument. Quand le comité d'entreprise de l'usine Colgate-Palmolive, à Compiègne, a découvert cet été que son propriétaire américain allait transférer toute la gestion des courriels électroniques aux Etats-Unis, le prétexte invoqué par la direction a été "l'amélioration de la sûreté informatique". Pour Hervé Grosjean, délégué CGT de l'usine, "c'est une atteinte aux libertés individuelles, puisque nous n'avons aucune garantie que nos droits au caractère privé du courrier seront respectés". La Commission nationale de l'informatique et des libertés (CNIL) a été saisie.

Pour accroître leur sécurité, les entreprises ont placé la cybersurveillance de leurs salariés au coeur du dispositif. Les frontières de leurs libertés individuelles sont désormais débattues sans cesse devant l'instance judiciaire. Pas toujours, heureusement, aux dépens du salarié. La Cour de cassation a ainsi annulé, fin 2001, le licenciement d'un employé de Nikon France au motif que les preuves apportées par l'employeur provenaient de courriels personnels. L'intrusion de Nikon constituait bien une violation de l'espace privé.

Mais l'"espace privé" se réduit comme peau de chagrin. "Si le salarié est informé au préalable qu'il peut être surveillé, que le contrôle se justifie et que celui-ci n'est pas continu", explique Alex Türk, le président de la CNIL, l'espionnage des salariés peut "être légal". Avec 90 personnes seulement, contre 400 en Allemagne, et un rôle purement consultatif, la CNIL a peu de moyens pour empêcher les dérives. "Nous savons qu'il existe un champ de pratiques totalement illégales mais nous n'avons, à ce jour, aucune procédure de ce type en cours", note M. Türk, pour qui la surveillance ne cesse de s'étendre, notamment via la "géolocalisation" des salariés par le biais du GPS.

Chez France Télécom, on explique que "dès qu'il y a suspicion de vol, calomnies, recherche d'images pédophiles ou concurrence déloyale, nous pouvons examiner tous les moyens de communication nous appartenant". Pour l'inspection interne de l'entreprise comme pour la justice, le traçage informatique peut être le moyen légal d'obtenir une preuve recevable. Dans les faits, les entreprises sont souvent conduites à faire appel aux sociétés spécialisées pour mener l'enquête. "Nos clients disposent, légalement, au titre du contrôle de gestion, de l'accès aux outils informatiques et de télécommunication des employés et nous transmettent leur contenu pour mener nos investigations", indique Philippe Legorjus, président d'Atlantic Intelligence, une société de ce type. Certains cabinets d'enquêteurs ajoutent leurs propres méthodes, sur lesquelles les entreprises ferment parfois les yeux, intéressées, comme dans le cas de Hewlett Packard, par le seul résultat. La justice est alors le seul rempart efficace contre ces intrusions.

Chez Hewlett Packard, géant américain de l'informatique, on n'en revient toujours pas de la chute de la présidente, Patricia Dunn. - REUTERS/PAUL YEUNG

Le tribunal de Nanterre a ainsi condamné, début novembre, d'ex-responsables du cabinet Arnoult International pour corruption et recel de violation du secret professionnel. Les agents en question obtenaient illégalement, grâce à une employée du service des réquisitions judiciaires chez France Télécom, des relevés de communications. Elle aussi condamnée, l'employée a indiqué avoir reçu, en contrepartie de sa trahison, deux versements en liquide. Les agents inculpés, des ex-gendarmes, démentent. Leur employeur plaide le malentendu.

Mais, derrière les moyens légaux dont peuvent user, en façade, les enquêteurs privés pour le compte des entreprises, se profile bel et bien une face cachée de l'"intelligence économique", un monde ô combien sous-réglementé. Intrusion informatique, filature, photo, vidéo, enregistrement de conversations, relevé d'immatriculation, vol de courrier, usurpation d'identité, cambriolage, l'arsenal est vaste.

Dans le cadre de luttes de pouvoir ou de conquête de marchés, il est souvent tentant pour les chefs d'entreprise d'y recourir. "C'est souvent, pour eux, une facilité, un gain de temps, une économie sur les frais d'avocat et de banquier et la tentation douteuse de connaître les secrets d'alcôve, pour un résultat souvent médiocre", commente Pierre-Antoine Lorenzi, patron de Serenus Conseil, spécialiste en stratégie d'entreprise et lobbying.

La qualité douteuse de ces enquêtes occultes est apparue en pleine lumière dans l'affaire du groupe chimique Rhodia. Les juges d'instruction chargés de ce dossier ouvert pour "faux bilan" ont découvert incidemment, à l'été 2005, que des enquêtes confidentielles avaient été réalisées par des cabinets privés sur les deux principaux plaignants du dossier, également actionnaires minoritaires de Rhodia - Hugues de Lasteyrie et le banquier Edouard Stern, assassiné dans de troubles circonstances le 1er mars 2005 à Genève.

Considérant qu'il pouvait y avoir menaces sur les parties civiles dans l'affaire dont ils avaient à connaître, les juges ont demandé une investigation et découvert que le cabinet Egideria avait bien enquêté sur M. de Lasteyrie pour le compte de Rhodia. Les recherches entreprises dans le même cadre ont également permis de remonter jusqu'à la société Astarte, auteur, pour le compte de Sécurité sans frontières - autre cabinet de sécurité -, de deux rapports sur Edouard Stern. Le premier identifiait ses "adversaires" et analysait les liens entre lui-même, Vincent Bolloré et Albert Frère. Le second proposait une biographie très sommaire de feu le banquier suisse.

Le rapport Stern a été soumis à Thierry Breton, alors président de France Télécom et qui fut, jusqu'en 2002, administrateur et président du comité d'audit de Rhodia. Aujourd'hui ministre des finances, M. Breton a expliqué qu'il avait adressé une fin de non-recevoir à cette mission et qu'aucune facturation n'avait été adressée à France Télécom. Mais les juges ont trouvé la trace d'une facture de 11 960 euros, qui apparaît liée à cette production. Adressée, le 24 février 2005 à France Télécom, la facture a été annulée le 3 mars 2005, c'est-à-dire deux jours après la mort de M. Stern.

"L'essentiel des rapports effectués par ces cabinets privés est constitué d'un tiers d'infos trouvées sur Internet, un tiers de ragots et un tiers d'enrobage", relativise un haut responsable de la police financière parisienne. "Il ne faut pas minimiser, dit-il, la part d'intox et de parasitisme représentée par toutes ces agences qui jouent sur la paranoïa, l'ego et le goût du secret des patrons."

La justice belge, elle, ne prend pas à la légère les agissements des apprentis barbouzes français. Le parquet de Bruxelles a inculpé, le 17 août, le groupe Suez et cinq Français pour "piratage informatique" et "tentative d'interception de communications privées". Cette affaire d'espionnage industriel, surnommée "Electragate" dans les milieux d'affaires franco-belges, a débuté en février 2004 lorsqu'un salarié d'Electrabel a découvert qu'un ordinateur du groupe avait été piraté. Il est apparu, au cours de l'enquête, que, dans la nuit du 19 au 20 février 2004, Richard Guillet, ex-nageur de combat de la DGSE ayant monté sa propre agence de sécurité, s'était introduit, avec deux informaticiens lyonnais, dans les locaux d'Electrabel pour y poser des micros espions dans des ordinateurs.

Interrogés par la justice française, les intéressés ont indiqué avoir agi pour le compte de la société O'Foll Consultant, dirigée par Olivier Foll, ancien directeur de la police judiciaire. Ils agissaient aussi pour le client du cabinet, à savoir le secrétaire général de Suez, Patrick Ouart, et le représentant de Suez au sein du conseil d'administration d'Electrabel, Jean-Pierre Hansen. Il s'agissait simplement, affirment les intéressés, de "tester" la sécurité des installations d'Electrabel, dont Suez était alors actionnaire minoritaire. Pour preuve de leur bonne foi, ils ajoutèrent que c'est M. Hansen lui-même qui introduisit les "espions" dans la place.

Version contestée par le parquet de Bruxelles, qui précise que d'autres faits, telle la copie de disques durs, ne collent pas avec le prétendu "test". L'accusation ne démord pas de sa version, à savoir que Suez espionnait le premier électricien belge dans l'espoir d'en prendre le contrôle. De fait, en 2005, Suez a mis la main sur près de 100 % du capital de cette société. Gérard Mestrallet, PDG de Suez, a été entendu comme simple témoin. Le renvoi de l'affaire devant le tribunal est présentement examiné par la justice belge.

La guerre économique admet cependant des méthodes plus "douces". Au cours de la première phase de l'OPA hostile lancée début 2004 par Sanofi sur Aventis, un avocat d'affaires prend langue avec la direction de Sanofi, présidée par Jean-François Dehecq. L'avocat affirme représenter un cadre anonyme d'Aventis prêt à trahir son camp et à fournir à Sanofi des informations stratégiques, en échange de 5 millions de dollars. M. Dehecq refuse de "démentir ou confirmer cet épisode" au Monde. Mais on sait, par l'intermédiaire d'un de ses anciens collaborateurs, que le PDG a décliné la proposition, qu'il a demandé et obtenu l'identification du "traître" et que, après la fusion, qui a finalement été scellée, l'intéressé a été congédié.

Post-scriptum :

http://www.lemonde.fr/web/article/0...