



Espionnage industriel : usurpation de données, moyen de défense, sanctions

publié le 14/10/2011, vu 11844 fois, Auteur : [Murielle Cahen](#)

En quoi l'usurpation de données industrielles confidentielles pose-t-elle problème ? Quels sont les moyens de défense actuels contre l'espionnage industriel ? Comment adapter les sanctions à l'usurpation de données immatérielles ? En quoi consiste la proposition de loi sur le secret des affaires ?

I/ La protection contre l'espionnage industriel dans le droit positif

A/ L'inefficacité des articles éparés appréhendant l'espionnage industriel

Aucun texte à portée générale ne vise explicitement la protection des secrets de l'entreprise, quand bien même le droit français semble disposer de moyens de lutte contre l'espionnage industriel.

Ainsi, dans l'hypothèse où le secret d'affaires divulgué repose sur un mode de protection institué par la propriété intellectuelle, à l'instar d'une marque, de dessins et modèles, d'un brevet, ou d'un droit d'auteur, les articles L 111-1, L 112-2, L 335-2 et suivants du Code de la propriété intellectuelle prévoient expressément les recours pour contrefaçon des droits du titulaire.

Les contrats de travail peuvent également contenir des clauses de confidentialité et des clauses de non-concurrence, permettant de sanctionner le salarié qui se livrerait à des activités d'espionnage.

En dehors de ces hypothèses de titres de propriété intellectuelle et clauses de contrat de travail, il est possible pour l'entreprise victime de s'appuyer sur des qualifications pénales classiques, telles que le vol du matériel supportant le savoir-faire de l'article 311-1 du Code pénal, voire l'abus de confiance dans le cadre de relations contractuelles de l'article 314-1 du Code pénal (arrêt de la Chambre criminelle [du 22 septembre 2004](#)).

Des dispositions répressives peuvent encore permettre aux entreprises de lutter contre la fuite de leurs informations protégées, comme l'article 226-13 du Code pénal qui réprime, d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende, la violation du secret professionnel, par [une personne qui en est « dépositaire soit par état ou par profession, soit en raison d'une mission temporaire »](#). Il en est de même du délit de corruption de l'article 445-1 et 2 du Code pénal, constituée si la communication des informations avait pour but de faciliter l'activité des concurrents.

L'incrimination de la violation du secret de fabrication figure, quant à elle, aux articles L. 621-1 du Code de la propriété intellectuelle et L. 1227-1 du Code du travail, qui la sanctionnent par une peine de deux ans d'emprisonnement et 30 000 euros d'amende. Seul ce délit de divulgation du

secret de fabrication peut encore sembler inclure spécifiquement la violation d'un secret industriel.

B/ L'insuffisance de la jurisprudence réprimant l'espionnage industriel.

À la différence du titulaire d'un droit de propriété intellectuelle, le détenteur d'un secret ne dispose pas de l'action en contrefaçon, mais seulement d'une action en responsabilité fondée sur la preuve de la faute de l'usurpateur, au sens des articles 1382 et suivants du Code civil.

Il convient de rappeler que tout professionnel a le droit d'attirer la clientèle de ses concurrents. Toutefois, il devient fautif dès lors qu'il a usé de moyens déloyaux.

Peut donc voir sa responsabilité engagée celui qui appréhende une information confidentielle sans l'accord du détenteur du secret, sur le fondement de la protection contre la concurrence déloyale. La faute du défendeur consiste alors dans l'accès et le détournement des connaissances contre la volonté de leur détenteur, caractérisant l'espionnage industriel, aussi appelé captation du savoir-faire d'autrui (arrêt de la Cour d'appel de Paris du 9 avril 1992).

Une telle protection s'avère cependant insuffisante, et c'est d'autant plus le cas que les réparations accordées ne sont jamais en nature. En effet, on ne trouve que très peu d'arrêts en France prononçant sous astreinte la prohibition de l'utilisation des informations usurpées, à l'inverse des Etats-Unis.

II/ La nécessité d'une défense plus effective contre l'espionnage industriel

A/ La récente affaire Michelin, témoin des limites de la protection

Le Tribunal correctionnel de Clermont-Ferrand par jugement en date du 21 juin 2010 a condamné un ancien salarié de la société Michelin qui avait tenté de vendre des informations obtenues au cours de son contrat de travail à la société Bridgestone, fabricant concurrent de pneumatiques

Sont retenus plusieurs chefs de poursuite qui dressent un panorama des fondements juridiques de protection de l'information et du secret des affaires. Pourtant, compte tenu de la manière dont la société avait piégé son salarié, ce dernier, invoquant la Convention européenne des droits de l'Homme, a soutenu que le procès était inéquitable pour déloyauté dans la collecte de la preuve.

Est d'abord reproché au salarié le délit précité d'abus de confiance, dont dispose l'article 314-1 du Code pénal, qui condamne à une peine de trois ans d'emprisonnement et 375 000 euros d'amende, toute personne ayant détourné au préjudice d'autrui, des biens quelconques, même immatériels, qui lui ont été remis et qu'elle avait acceptés à charge de les rendre.

Est de même reprise la jurisprudence qui applique, aux affaires d'espionnage industriel, les dispositions précitées réprimant la révélation des secrets de fabrique, notamment l'article L. 1227-1 du Code de travail, prévoyant une peine d'emprisonnement de 2 ans et 30 000 euros d'amende, pour tout directeur ou salarié d'une entreprise qui révélerait ou tenterait de révéler un secret de fabrication.

Toutefois, le tribunal clermontois n'a finalement pas admis l'existence d'un secret de fabrique.

Bien que cette récente affaire Michelin témoigne de l'existence de moyens de protection contre l'espionnage industriel, elle fait également apparaître les limites de la protection constituée autour de dispositions éparses, se révélant, qui plus est, peu efficaces au moment de leur mise en œuvre.

B/ Le projet de loi relatif à la protection des informations économiques comme remède ?

Alors que vient d'éclater l'affaire d'espionnage industriel supposé chez Renault, le député UMP du Tarn Bernard Carayon dépose, le 12 janvier 2011, la proposition de loi n°1754 sur le secret des affaires, visant à créer un délit d'atteinte aux informations économiques protégées.

Il s'agit alors d'instaurer des peines suffisamment sévères pour être dissuasives, à l'image de celles que prévoit le Cohen Act américain, de manière à combler les lacunes du droit français.

Le dispositif mis en place au travers de ce projet de loi semble plus efficace, dotant la justice de moyens répressifs importants. En effet elle prévoit en son article 1^{er} de punir « l'atteinte au secret d'une information à caractère économique protégée » par une peine de trois ans d'emprisonnement et 375 000 euros d'amende ; le double si le responsable de la fuite a agi dans « l'intention de nuire » à l'entreprise ou en a tiré un « profit personnel ».

Si des peines plus sévères sont prévues, une définition plus précise quant à l'objet de la révélation incriminée est expressément fournie. En effet, sont qualifiées d'informations à caractère économique protégées, les informations ne constituant pas des connaissances générales librement accessibles par le public, ayant, directement ou indirectement, une valeur économique pour l'entreprise, et pour la protection desquelles leur détenteur légitime a mis en œuvre des mesures en vue de les tenir secrètes.

Sur le plan pratique, serait institué un « confidentiel entreprise », comme il existe un « confidentiel défense ». Les documents techniques ou commerciaux frappés de cette mention verraient leur divulgation constituer une infraction pénale. Les données protégées sont celles dont la divulgation porterait une atteinte grave aux positions stratégiques, au potentiel ou aux intérêts de l'entreprise, méritant donc au même titre que les brevets industriels de voir leur confidentialité protégée.

LIENS CONNEXES :

Loi Loppsi 2 sur la sécurité informatique : http://www.murielle-cahen.com/publications/p_lopsi2.asp

Intrusion dans un système informatique : http://www.murielle-cahen.com/publications/p_intrusion.asp