François Haut

Que faire de l'intrus ?

Cette question, effectivement, sied parfaitement à la dernière intervention de ce colloque sur cette forme particulière d'espionnage qu'est l'espionnage industriel.
On pourrait, en effet, estimer à juste titre que le sort destiné à cet intrus fournisse le mot de la fin : démasqué, il ne reste plus qu'à régler son devenir qui ne manquera pas de se matérialiser par une sanction pénale qui le met habituellement hors d'état de nuire.
C'est ainsi, en effet, que l'on aurait pu imaginer ce propos, en mettant en lumière toutes les catégories juridiques de l'arsenal répressif dont dispose le droit français en la matière.
Il se trouve qu'il n'en sera pas exactement ainsi, et ce parce que cet aspect pénal de l'espionnage industriel, comme d'ailleurs de l'espionnage tout court, ne représente ni la seule, ni la meilleure réponse à cette menace.
En effet, on a parlé jusqu'à présent d'espionnage industriel, on va maintenant d'évoquer des questions qui se rapprochent des techniques du contre-espionnage.
Que faire de l'intrus ? Et d'abord, qu'est-ce qu'un intrus ? Le dictionnaire le définit comme quelqu'un qui s'introduit quelque part sans y avoir été invité. L'intrus, c'est donc, simplifions, celui qui a déjà accompli son forfait, ou qui est en train de l'accomplir, **et** qui a été découvert; sans cela, bien sur, on n'est pas informé de l'intrusion. On ne se demandera pas d'ailleurs comment, par quels moyens, cet intrus a été découvert.
Mais découvert ne signifie pas nécessairement appréhendé, intercepté; repéré ne signifie pas non plus que l'intrus, lui, sache que ceux qu'il a pénétré connaissent ses agissements.
Que faire de l'intrus ? C'est une question qui préoccupe, à juste titre, les industriels espionnés ou espionnables.
Qu'est-ce qui est le plus utile ? Empêcher immédiatement l'intrus de nuire à l'entreprise à laquelle il s'est attaqué. Ou au contraire l'utiliser, tout au moins tenter de l'utiliser, consciemment ou à son insu, pour faire pénétrer des informations fallacieuses chez celui qui l'employait ou même obtenir de lui des informations ?
Où est, alors qu'il est posé ainsi, la solution la plus satisfaisante de ce problème ?
L'option qu'on a choisie conduira d'abord à définir la problématique, elle fixera ensuite les limites des solutions juridiques traditionnelles pour montrer enfin le cadre juridique d'autres options.

I- La problèmatique de cette question

Pour ce qui nous intéresse ici, l'intrus, c'est l'espion.
On va donc exposer rapidement, dans ce premier point, les divers types d'acquisition du renseignement, précisément, pour ce qui nous concerne l'espionnage, puis en quoi consistent les mesures de protection qui vont du contre-espionnage à la contre ingérence.
Une centaine d'années avant notre ère chrétienne, le stratège et philosophe chinois Sun Tse écrivait : *"Ayez des espions partout, soyez instruits de tout, ne négligez rien de ce que vous pourrez apprendre…* Comme son propos concernait la guerre, il ajoutait : *Une armée sans agents secrets est un homme sans yeux ni oreilles"*.

Rien n'a changé aujourd'hui et, pour éviter le triste sort dépeint par Sun Tse, celui d'être coupé de l'extérieur ou d'être pénétré, **espionnage et contre-espionnage** sont toujours indispensables, non seulement aux armées, mais aussi aux Etats dans la réalisation générale de leur politique et, dans le contexte qui est aujourd'hui celui d'une guerre économique, aux entreprises.

L'Espion

L'espionnage, c'est l'utilisation d'individus, le recrutement d'agents et la manipulation de personnes. C'est la recherche d'informations qui sont, elles, hautement protégées et que l'on ne peut obtenir qu'à travers des moyens très spéciaux, voire détournés, et c'est un euphémisme.

Il faut savoir que l'espionnage est couteux, en termes de temps et d'énergies. Il nécessite du temps pour identifier et recruter les sources humaines qui pourraient avoir accès à l'information. Il y a exceptionnellement des préparations rapides. Le processus est généralement lent et laborieux et n'est généralement utilisé qu'en dernière extrémité.

L'espionnage c'est l'utilisation de l'homme, avec ses forces, mais aussi -dirais-je surtout ?- avec ses faiblesses pour essayer de savoir ce que les autres veulent cacher. Alors, parler de méthodes serait

superflus, puisque dans ce type de stratégies indirectes, elles sont toutes envisageables et les plus étonnantes ont été rencontrées.

Comme l'espionnage existe, l'une des nécessités des entreprises, comme de l'Etat, est de se protéger.

Eléments de contre-espionnage

Il s'agit pour l'Etat des mesures de tout type destinées à protéger son territoire national compris dans le sens le plus large : installations, travaux de recherche, personnes, informations considérées comme "sensibles"…

On emploie le plus souvent pour désigner la protection ainsi définie, les termes de **contre-espionnage** ou de **contre-ingérence**. On distingue l'ingérence de l'espionnage dont elle est un prolongement. Elle peut être définie comme le fait de s'emparer de certains leviers de commande de l'adversaire ou du concurrent. L'ingérence peut être politique, économique ou culturelle, le but étant toujours soit d'affaiblir, soit d'infléchir la politique de la cible.

• Dans les activités de protection, on distingue traditionnellement des aspects passifs et actifs, **défensifs ou offensifs**, mais la ligne de séparation est floue et difficile à définir.

L'un consiste à **attendre passivement** les mouvements adverses et à contrer des actes hostiles potentiels. En d'autres termes, cela comprend les mesures qui sont prises pour se protéger contre ce que l'adversaire pourrait être susceptible de faire.

Des mesures et activités caractéristiques du contre-espionnage passif consistent en programmes défensifs fondés sur des sources, en contre-mesures techniques de surveillance, en programmes d'information et d'éducation sur la sécurité, en appréciation de la vulnérabilité d'installations sensibles.

En ce qui concerne l'Etat, ces activités passives, quoiqu'indispensables à une bonne sécurité intérieure, ne sont pas suffisantes. C'est pour cela que l'on utilise des **mesures actives** de contre-espionnage.

Moins évidentes pour l'entreprise, elles consistent à entreprendre des actions offensives pour déceler les activités menaçantes des entités hostiles, faire échouer leurs projets, et si possible étendre son contrôle sur eux. Cela peut mener à la manipulation de l'adversaire.

Ainsi conçu, le **contre-espionnage** apparait comme la discipline qui analyse les menaces et qui préconise et met en œuvre les mesures de protection nécessaires, dans le strict respect de la légalité. C'est indispensable pour l'entreprise et ce n'est pas sans soulever des questions pour ce qui est de l'Etat. Cette discipline est , pour l'entreprise, à rapprocher de ce que les anglo-saxons appellent le *"risk management"*.

Ce tableau très sommaire de ce qu'on pourrait appeler le "renseignement d'entreprise" ne serait pas complet si on n'évoquait pas le renseignement ouvert. Il s'agit de l'utilisation des données non protégées, qui ne mettent pas en scène un intrus au sens propre du terme. Cependant, le droit français punit le rassemblement de données dont "la réunion et l'exploitation est susceptible de nuire à la Défense Nationale" (Art. 74 C.P.).

Cette pratique n'entre pas exactement dans notre sujet, mais on va voir que les textes normatifs de notre droit positif cultivent un certain brouillage et que les frontières entre les divers "espionnages" ne sont pas très définies.

II Les limites des solutions traditionnelles

Si l'espionnage industriel ressemble à l'espionnage en général et si la frontière est souvent confuse et difficile à déterminer, il n'en reste pas moins que les solutions juridiques -ou judiciaires- et leurs effets ne sont pas les mêmes.

Eléments du droit pénal de l'espionnage industriel

Il ne s'agit pas de la même qualification juridique.

• Pour le code pénal, dans son article 73, **l'espionnage** est un crime. Il est **commis** contre les intérêts de la défense nationale; il implique la participation humaine directe **d'un étranger** Quand il s'agit d'un français, ce crime est qualifié de trahison (Art. 72 C.P.).

Pour ce qui est de l'espionnage industriel, la qualification n'est pas la même, réserve faite du problème de limites que l'on a évoqué, et qui se concrétise dans l'article 77 du Code Pénal, qui élargit la notion, le pivot étant toujours la défense nationale : "Sera puni… tout Français ou étranger qui, sans autorisation préalable de l'autorité compétente, livrera ou communiquera à une personne agissant pour le compte d'une puissance ou d'une entreprise étrangère, soit une invention intéressant la défense nationale, soit des renseignements, études ou procédés de fabrication se rapportant à une invention de ce genre ou à une application industrielle intéressant la défense nationale."

• Mais, dans la plupart des cas, l'espionnage industriel est un délit, qui inclut le vol, le recel de vol, ou des atteinte à la vie privée.
On laissera de côté ici les infractions de l'article 418 du code pénal qui, bien que se rapportant à l'espionnage industriel, ne concernent pas l'intrusion dans l'entreprise, mais la livraison volontaire de renseignements.
• Quels sont donc ces délits que peut commettre l'intrus.
En fonction de la notion d'espionnage que l'on a exposée précédemment, on retiendra trois éléments qui sont la reproduction de documents, l'enregistrement d'informations et l'appropriation de données informatiques.
• En matière de **reproduction** de documents, quel que soit le procédé utilisé de photocopie ou de photographie, on considérera qu'il s'agit de vol, ou de recel de vol quand il y a des accointances à l'intérieur de l'entreprise. Le risque pour l'intrus est alors de se voir frappé d'une peine d'emprisonnement qui peut aller jusqu'à trois ans, assortie d'une amende qui peut aller jusqu'à 20 000F.
On peut aussi supposer qu'il y ait effraction, qu'elle se produise la nuit; et dans ce cas là, il s'agit d'un vol aggravé sanctionné par l'article 382 du code pénal. Selon les circonstances, l'emprisonnement peut aller jusqu'à 15 ans.
Si l'intrus, dans un sens plus large ici, a reçu ces documents à l'aide d'une complicité intérieure, il est alors coupable de recel. Il est susceptible d'être emprisonné pour une durée qui peut aller jusqu'à 5 ans, peine qui peut être assortie d'une amende généralement forte.
• En matière **d'enregistrement d'informations**, le délit se situe dans le domaine de l'atteinte à la vie privée.
Cela soulève un série de questions quant à la notion de vie privée, qui n'est pas toujours facile de rapprocher de celle d'entreprise. Bien que refusée par la jurisprudence actuelle, peut-être pourrait-on redéfinir l'idée de vie privée de la personne morale, en la rapprochant de la notion de secret professionnel ou de fabrication et de droit de marque ou de propriété.
Sans entrer dans le détail de cette argumentation, qui a toute son importance dans les solutions juridiques à apporter au problème de l'intrus, on considérera ici que l'exploitation d'enregistrements, de sons comme d'images, va entrer dans le cadre des articles 368 du CP et 369 en cas de complicité et pourra être punie d'une peine allant jusqu'à un an d'emprisonnement. Quant à la violation spécifique des communications téléphoniques, qui soulève d'autres questions, elle est prévue par la loi du 10 juillet 1991.
• Reste encore la **fraude informatique**. Ce procédé, que l'on connait aussi sous le nom anglais de *hacking*, qui est loin d'être une distraction d'adolescents, est une forme incontestable d'intrusion. La pénétration illégitime d'un système informatique, que ce soit à des fins de recueil de données, ou de destruction au moyen de ce qu'on appelle aujourd'hui des virus, pose de tels problèmes que la "sécurité informatique" connait un développement considérable.
La loi française tenu compte cette nouvelle donnée et, depuis le 5 janvier 1988, reconnait le caractère spécifique de l'infraction et la punit d'une peine qui peut aller jusqu'à 5 ans dans le cas de "falsification de documents informatisés". Il s'agit des articles 462 et suivants du CP.

Les effets du droit pénal de l'espionnage industriel

Ce qui a été dit jusqu'à présent montre que le droit pénal peut prendre en compte l'espionnage industriel et punit ceux qui s'y adonnent.
Ces punitions se traduisent par des amendes et des peines de prison.
Quand l'intrus est en prison, il est certes hors d'état de nuire, mais il ne sert plus à rien. Pourquoi ?
Quand un Etat met un espion "classique" en prison, a la suite d'une procédure normale, il en fait un élément de négociation. Du fait qu'il est détenteur de la souveraineté, il peut, s'il le désire, quand ses intérêts le commandent, en disposer et s'en servir comme d'une monnaie d'échange.
Concrètement, cela signifie que l'on a assisté, par exemple, à des échanges d'espions, après des négociations au cours desquelles l'Etat détenteur obtenait des avantages. Il pouvait s'agir aussi bien d'espions de son pays que d'autres types d'éléments.
Dans un autre domaine, celui du terrorisme, on a vu le gouvernement français libérer des individus régulièrement et difficilement incarcérés dans notre pays au nom de la raison d'Etat (Annis Naccache).
L'espion est ainsi un otage "légal" et l'on connait bien la puissance de ce moyen de pression.
Rien de cela en revanche pour ce qui est de l'espion industriel. La société-victime qui a pu être à l'origine de son incarcération ne dispose pas de la maîtrise de sa libération.
Elle perd très vite le contrôle de la situation et ce qui peut être une arme entre les mains de l'Etat ne l'est absolument pas pour la société espionnée.

Cela signifie donc que le processus pénal ne présente pas beaucoup d'intérêt en matière d'espionnage industriel.
A cela on fera deux objections. D'une part, l'obtention de dommages et intérêts sera éventuellement possible si l'on a pu localiser le commanditaire de l'intrus et cela peut ne pas être indifférent. Mais, et ce sera l'objet du point suivant, on a intérêt à le faire avant l'intervention du juge.
Deuxième objection, la nuance entre l'espionnage industriel et l'espionnage politique ou militaire est fine, et passer d'un cas de figure à l'autre ne peut pas être écarté.
Il n'en reste pas moins qu'il peut y avoir, pour la société espionnée des solutions autres que le processus judiciaire "normal". A la condition , bien entendu de se placer aussi dans un cadre juridique.

III Le "bon usage" de l'intrus.
Vous l'avez repéré, vous le connaissez, l'intrus est là. Que faire ?
C'est ici que l'on se place dans le cadre intellectuel du contre-espionnage. Mais attention, vous ne disposez pas des mêmes moyens que l'Etat et ce que vous ferez peut, faute de précautions, se retourner contre vous.
le cadre juridique
La marge de manoeuvre dont on peut disposer est relativement étroite.
On supposera que votre entreprise est protégée par des moyens techniques, mais aussi par des moyens humains et que votre intrus est pris sur le fait.
L'article 73 du code de procédure pénale dispose que *"dans le cas de délit flagrant puni de peine d'emprisonnement* -c'est le cas de figure que nous avons envisagé- *toute personne a qualité pour en appréhender l'auteur et le conduire devant l'Officier de police judiciaire le plus proche."*
Le texte ne prévoit pas de délai précis pour ce qui est de cette conduite mais il va de soi qu'il est bref. Rien à voir avec le temps de la garde à vue dont dispose l'Etat. Reste que ce délai existe et qu'il faut tenter de le mettre, au maximum, à profit.
Cette petite marge doit permettre d'obtenir une confession spontanée de l'intrus. Attention à toute violence et toute intimidation abusive qui ne manquerait pas de se retourner contre vous soit sous la forme d'un contre-chantage, soit sous la forme d'une plainte reconventionnelle au pénal.
Cette confession spontanée n'a d'intérêt que si on en a la trace et l'un des moyens les plus commodes est l'enregistrement.
Attention là encore car l'enregistrement sans consentement peut aussi se retourner contre vous sur la base de l'article 368 du CP. D'où encore une précaution, faire écrire à l'intrus, d'une écriture calme révélant le moins de tension possible une autorisation d'enregistrement de ses propos dans laquelle il reconnait l'effraction et exprime son consentement pour ménager le droit à la preuve.
Le cadre stratégique
Cette situation de l'intrus n'est guère enviable car il va droit à la condamnation. Mais on a dit que ce n'était pas la meilleure solution pour l'industriel.
Une possibilité réside alors dans la manipulation.
Il s'agit de tenter de persuader l'espion, fort des arguments dont on dispose, d'abandonner ses prétentions initiales et de se retourner contre celui qui l'emploie. On ne s'étendra pas sur les moyens de persuasion, mais ceux-ci nécessitent une part de collaboration de l'intrus; ce sont ici les personnalités et les circonstances qui dicteront les résultats.
Dans l'absolu, les stratégies industrielles de l'entreprise considérée s'en trouveront d'autant confortées.
Mais il ne s'agit en aucune manière de se placer soi même dans une situation qui puisse être répréhensible: les inconvénients dépaseraient de loin les avantages.
En revanche, utiliser des procédés que l'on connait sous le terme d'origine russe de désinformation,
Beaucoup mieux, l'hypothèse d'une manipulation que se fera à l'insu de l'intrus. Là, le cadre juridique n'est bien-sur plus le même car aucun lien n'existe entre l'entreprise et l'intrus et dans cette hypothèse, la sécrité est plus grande.
On est parti de l'idée que l'intrus n'existe qu'à partir du moment où il a été repéré. On peut imaginer alors de le "désinformer" en l'alimentant d'informations soigneusement sélectionnées ou altérées. Là encore les procédés sont connus et on ne s'étendra pas sur leur nature.
Mais attention. Trois réserves ou trois précautions s'imposent : la véritable information a-t-elle été correctement protégée; l'information modifiée a-t-elle atteint sa cible; en a-t-on tiré les bonnes conséquences.

Pour conclure ce propos, on soumettra deux réflexions.
La première concerne la sécurité de l'entreprise en génétral. Rien de ce qui vient d'être ditn'est possible si on n'a pas donné à son entreprise une éducation et une conscience de la sécurité. Dans la sérénité, sans paranoïa, elle sont indispensables. Une seconde rélfexion portera sur l'importance de la connaissance et la nécessité qu'il y a à la protéger dans le contexte général d'une concurrence économique qui s'apparente à une guerre.
Dans cette ambiance de conflit à basse intensité, chacun est concerné, chaque emplyé, chaque citoyen; Les nuances sont de moins en moins évidentes et l'idée de frontière, dans tous les sens du terme, entre pays comme entre matières, secrètes ou non, perd de son sens. Le droit se brouille quelque peu et il ne faudrait pas que ce soit l'intrus qui en profite.