

## La protection juridique du patrimoine informationnel aux Etats-Unis : le Cohen Act, 1996

Dans son rapport sur l'état de l'Intelligence Economique en France, le député Carayon explique, à juste titre, que la France est privée de système juridique véritablement protecteur du patrimoine informationnel des entreprises.

Certes, on trouve dans notre droit des dispositions éparses pouvant être appliquées dans des situations de vol de secrets d'affaires. Mais le système pêche par l'inexistence d'une protection de l'information en tant que telle, comme c'est le cas aux Etats-Unis.

Auteur :  
Antoine Doury

Les Etats-Unis ont compris la nécessité d'un système juridique cohérent en la matière il y a déjà une dizaine d'années. Outre-Atlantique, l'information est l'objet d'une protection particulière, posée dans l'Economic Espionage Act, ou Cohen Act, de 1996. Celui-ci attribue une valeur propre à l'information, qui devient objet d'un droit exclusif de propriété.

Aux Etats-Unis, la prise de conscience apparaît dès le début des années 90.

Dans un rapport, le FBI indique que 23 pays viseraient activement les secrets de fabrication détenus par l'industrie américaine. La CIA cite la France, Israël, la Russie, la Chine et Cuba comme les pays les plus engagés dans les manœuvres d'espionnage contre la nation américaine. Les services de renseignement expliquent même que les services secrets français auraient avoué avoir régulièrement espionné les hommes d'affaires et politiques étrangers, posant des micros sur les sièges des avions d'Air France ou dans les chambres d'hôtel. Des études, notamment celle menée par l'A.S.I.S, l'American Society for Industrial Security, donnent des chiffres alarmants : on relèverait une augmentation de l'ordre de 320 % des manœuvres d'espionnage économique de 92 à 96.

Les secteurs convoités sont nombreux : aérospatiale, biotechnologie, informatique, systèmes motorisés, transports, télécommunications, énergie, cryptographie, lasers, etc... Mais les manœuvres ne concerneraient pas seulement des informations de haute technologie. Sont également prises pour cibles des informations

d'ordre commercial (fichiers clients, listing prix, données personnelles, projets de développement, coûts de fabrication...). L'Etat réalise que la réaction devient urgente.

À cette époque, les "lawyers" ont critiqué une législation fédérale trop lacunaire sur la question. Au pénal, il n'existe alors qu'une seule loi fédérale incriminant le vol de secret d'affaires. Et celle-ci ne concerne que l'acte d'un personnel d'Etat. (Article 1905 du code pénal US). Pour pouvoir sanctionner le vol de secret d'affaires par une personne non-fonctionnaire, on devait se référer à des textes variés, comme l'Interstate Transportation of Stolen Property Act de 1930, le Federal Mail Fraud (violation des correspondances), ou encore le Wire Fraud.

**"La CIA cite la France, Israël, la Russie, la Chine et Cuba comme les pays les plus engagés dans les manœuvres d'espionnage contre la nation américaine. Les services de renseignement expliquent même que les services secrets français auraient avoué régulièrement espionné les hommes d'affaires et politiques étrangers, posant des micros sur les sièges des avions d'Air France ou dans les chambres d'hôtel."**



Thibault du  
Manoir de Juaye

Avocat au Barreau  
de Paris

[juaye@regards-intelligence-economique.com](mailto:juaye@regards-intelligence-economique.com)

La rubrique dont l'animation m'incombe, au sein de ce nouveau magazine, Regards sur l'intelligence économique, est consacrée au droit. En vérité, cela n'étonnera, personne ! Sa vocation : examiner, numéro après numéro, le rapport entre le droit et l'intelligence économique et évaluer, autant que faire ce peut, dans quelles mesures les pratiques de l'intelligence économique sont licites, ou non.

En effet, l'intelligence économique, outre les interrogations sur la légalité des pratiques, va utiliser le droit comme outil, comme arme. Certains auteurs soutiennent même qu'il existerait des war room juridiques à côté des war room classiques.

Des notions que tout professionnel se doit de connaître et de manier habilement.

À tel point que l'utilisation de cet outil est devenue incontournable, nécessaire, voire même sine qua non au bon déroulement des activités usuelles de l'intelligence économique : sans connaissance du droit privé et public, comment élaborer la stratégie de son entreprise ? et sans connaissance du droit international, comment comprendre celle de ses concurrents américains ou chinois ? Dans le contexte économique international actuel, la bonne appréhension du droit est donc un gage de survie. Tour à tour, nous aborderons donc des thématiques à l'intersection du droit et de l'intelligence économique : les stratégies juridiques d'entreprises, les évolutions juridiques constitutives à la mise en place de politiques d'intelligence économique. Sans oublier les pratiques internationales.

Si, l'IE doit sortir de la nuit, le droit ne doit plus constituer une zone d'ombre !

L'application de ces textes, pour certains anciens, dépendait du mode de communication de l'information utilisé. Les juristes ne pouvaient se servir de ces textes que si le support de l'information le permettait. Cet état de la législation laissait de nombreuses zones de "non-droit" sur le plan pénal.

Au civil, les citoyens américains pouvaient se prévaloir de la doctrine du Trade Secret. (Droit de la responsabilité civile délictuelle). Cette doctrine était protectrice de la valeur économique de l'information. On pouvait donc sanctionner l'appropriation frauduleuse d'une information (concept de "misappropriation"), sur le fondement de la mauvaise foi ou de la perte de confiance dans son partenaire. Deux modèles coexistaient, construits tous deux sur fondement de la doctrine du Trade Secret : L'Uniform Trade Secret Act (UTSA), applicable dans 37 états, et le Restatement of Torts. L'applicabilité du principe différait un peu selon le modèle, mais le concept était identique. La doctrine du Trade Secret posait une protection civile de l'information en tant que telle, sans condition de matérialisation par un support quelconque. L'information était perçue comme objet de valeur économique, procurant un avantage concurrentiel. Cette valeur était bien entendue relative, car définie par rapport aux acteurs présents sur le marché.

Bien qu'il soit séduisant, ce principe était réduit dans son applicabilité. En effet, les entrepreneurs victimes de vol

**“Arrivant au pouvoir, Clinton déclare que “sa priorité sera la défense des intérêts économiques des Etats-Unis”. La sécurité économique américaine devient dès lors une véritable politique publique. L'administration prend conscience de la nécessité de maîtriser l'information, son partage, l'optimisation de son efficacité.”**

d'information devaient entamer une procédure longue et coûteuse. On estimait alors à 4 ans la durée moyenne d'un procès en la matière. De plus, les preuves d'une acquisition frauduleuse étaient difficiles à apporter. Ainsi, par manque de temps et de moyens, les entrepreneurs ciblés se résignaient à abandonner prématurément leurs poursuites à l'encontre du concurrent mal intentionné, lequel avait d'ailleurs bien souvent intégré le montant d'une sanction potentielle dans ses coûts de production.

Arrivant au pouvoir, Clinton déclare que “sa priorité sera la défense des intérêts économiques des Etats-Unis”. La sécurité économique américaine devient dès lors une véritable politique publique.

L'administration prend conscience de la nécessité de maîtriser l'information, son partage, l'optimisation de son efficacité.

Outre les dispositions en terme d'organisation structurelle de la société de l'information, l'administration émet des dispositions juridiques visant à protéger l'efficacité économique de l'industrie américaine.

De cette réflexion naît le Cohen Act. Cette loi promulguée en 96 à l'initiative de William Cohen, alors Secrétaire d'Etat à la Défense, établit une véritable protection du patrimoine informationnel américain.

Le projet demanda deux ans de préparation. Le législateur consulta notamment les travaux du FBI, travaillant sur l'Economic Counter Intelligence Program lancé en 1994 ainsi que les industriels de l'Aérospatiale et de la Silicon Valley.

L'objet premier de cette loi était la protection du patrimoine informationnel national face à l'espionnage économique public ou mixte, c'est-à-dire l'espionnage par une entité étrangère. Ce n'est qu'au moment du vote que fut ajouté, in extremis, le deuxième volet de la loi, à savoir la protection contre l'espionnage économique privé, c'est-à-dire le vol de secret d'affaires

Dans un premier temps, l'acte vient sanctionner les activités d'espionnage économique par une entité étrangère. C'est l'article 1831 qui en pose le principe. Constituent un acte d'espionnage économique le vol, la reproduction, l'altération, la destruction ou la transmission d'un secret d'affaire, dès lors que l'on agit sciemment, et au profit d'une entité étrangère : que ce soit un gouvernement, une organisation ou un agent particulier. Sont également punis le recel, à savoir la prise de possession d'une information que l'on sait volée, la tentative et la simple préméditation (le simple projet de commettre un vol est répréhensible).

La sanction est, pour une personne physique, une amende maximale de 500 000 \$ et/ou au plus 15 ans d'emprisonnement. Pour une personne morale, la sanction est une amende d'un maximum de 10 millions \$. La sanction est identique quel que soit le stade d'avancement de la manœuvre d'espionnage. Autrement dit, la tentative ou le complot sont aussi sévèrement punis que le vol.

La sanction du vol de secret d'affaires, article 1832, repose sur les mêmes éléments matériels : vol, reproduction,



## La protection juridique du patrimoine informationnel aux Etats-Unis : le Cohen Act, 1996

altération, destruction ou transmission d'un secret d'affaires. L'auteur de l'infraction doit avoir l'intention frauduleuse de détourner un secret d'affaires dans l'intérêt économique d'une entité tierce, et savoir que la perte de l'information nuira à son titulaire. La loi protège tout produit fabriqué pour le marché intérieur ou extérieur ou à vocation à y être mis.

La sanction encourue par une personne physique est une amende maximale de 500 000 \$ et/ou de 10 ans d'emprisonnement. Une personne morale risque quant à elle le paiement d'une amende de 5 millions \$.

**“Avec le Cohen Act, la protection du patrimoine informationnel devient réelle. La procédure est moins coûteuse pour l'entrepreneur victime. C'est désormais le Ministère public qui supporte les frais de justice et d'investigation. Elle est également plus rapide.”**

Avec le Cohen Act, les Etats-Unis adoptent un système uniforme de protection pénale du patrimoine informationnel. Pour la première fois, le système pénal consacre le vol de secret d'information à valeur économique sur le modèle du Trade Secret, et vient même compléter la définition du secret d'affaires. L'article 1839 définit le “secret d'affaires” comme suit : le texte protège toute information, quelque que soit sa forme et sa nature, quels que soient le type de support, sans condition de matérialisation, qu'elle soit stockée ou non. L'information est donc protégée en tant que telle. Même immatérielle, elle est l'objet d'un droit exclusif de propriété.

Deux conditions doivent être remplies pour que s'applique le régime de protection : d'une part, le propriétaire



de l'information doit avoir pris les mesures raisonnables pour maintenir le secret. Cet élément définit le secret par rapport au domaine public et pas seulement par rapport aux “intrusions” frauduleuses d'un concurrent. Les commentateurs considèrent ainsi que le propriétaire de l'information, “personne physique ou morale disposant de manière légitime d'un titre ou d'une licence sur lequel repose ledit secret”, doit assurer convenablement la confidentialité des informations essentielles. Par exemple, on estime qu'il doit avertir un salarié de la confidentialité de l'information dont il dispose, comme il doit, à l'inverse, ne communiquer les informations “secrètes” qu'aux seuls salariés qui en ont besoin pour exercer leur fonction. Il doit aussi faire signer des clauses de confidentialité, ou encore conserver les documents secrets sous clé.

Toute information rendue accessible lors d'une conférence de presse ou dans le contenu d'un article perd toute confidentialité, et donc toute protection. Par contre, les commentateurs considèrent que le recueil d'informations éparses, en vue de reformer un secret pourrait être considéré comme la violation d'un secret. Cette thèse n'est cependant pas encore consacrée par la jurisprudence.

L'application de cette notion est sujette à interprétations et débats. On considère que les mesures raisonnables diffèrent selon le secteur d'activité, mais également selon la valeur de l'information, les conséquences potentielles d'un vol.

Pour parfaire l'application de cette loi plus imprécise qu'il n'y paraît, les professionnels ont lancé différents projets visant à inciter les entreprises à anticiper les attaques de concurrents. Le but serait de concrétiser statutairement les mesures raisonnables qu'il convient de prendre. Ils évoquent ainsi le devoir de responsabilisation des cadres vis-à-vis de la confidentialité des informations, les incitant à limiter les délégations de pouvoirs lorsqu'il s'agit d'informations sensibles, et à ne divulguer les secrets qu'aux salariés qui en ont strictement le besoin, tout en les informant de cette confidentialité et en leur expliquant les risques à éviter.

L'entreprise doit cultiver l'esprit de protection du patrimoine informationnel de l'entreprise et mettre en place les mesures standard pour limiter les risques de fuite informationnelle. Ces changements doivent s'accompagner d'une communication claire sur l'importance des attitudes à changer. Les statuts doivent également prévoir des mesures internes de sanctions en cas de défaut de vigilance ou de violation du secret.

D'autre part, l'information doit avoir une “valeur économique propre, actuelle ou potentielle, qui ne consiste pas en des connaissances générales pouvant être facilement et directement constatées par le public”. Autrement dit, ne sont protégées que les informations procurant un avantage concurrentiel certain, et qui ne sont pas accessibles par des moyens communs.

L'application de cette valeur économique laisse, comme pour la notion de “mesures raisonnables”, une grande place à l'interprétation. C'est donc au fil des décisions jurisprudentielles que des précisions seront apportées. Ainsi, le domaine d'application du secret d'affaires est encore flou. La notion de valeur économique propre, par exemple, est très relative. A quel stade d'un projet peut-on considérer que l'information devient

porteuse de valeur économique propre ? De plus, le texte pose comme exception aux informations couvertes par le secret les connaissances générales d'un salarié ("general knowledge, skills or expertise"). Mais où se situe la limite entre le savoir faire acquis par le salarié, et dont il pourra se prévaloir auprès d'une entreprise concurrente, et les informations dites secrètes qui doivent rester dans le patrimoine de l'entreprise ?

Ici, les commentateurs estiment que doit être sanctionnée l'obtention de connaissances spécifiques relatives à un produit, mais non l'expérience personnelle, qui fait partie du "patrimoine du salarié". Ici encore, la portée du texte reste incertaine et il appartiendra à la jurisprudence de préciser quelles connaissances ne peuvent être exploitées par un salarié au profit du concurrent.

L'article donne une liste non exhaustive des informations protégées, celle-ci ayant vocation à s'étendre avec l'apparition de nouveaux vecteurs d'information. Avec le Cohen Act, la protection du patrimoine informationnel devient réelle. La procédure est moins coûteuse pour l'entrepreneur victime. C'est désormais le Ministère public qui supporte les frais de justice et d'investigation. Elle est également plus rapide. De plus, le Ministère public a les moyens et pouvoirs de prendre toute mesure pour préserver le secret, respectant seulement une condition de proportionnalité entre les mesures à prendre et la valeur potentielle du secret. Les auteurs estiment qu'il existe désormais une présomption de confidentialité de l'information, et que, dès l'ouverture de la procédure, et jusqu'à l'issue du procès, l'information en question doit rester protégée.

La disposition bénéficie d'un large champ d'application territoriale. L'acte répréhensible tombe sous le coup de la loi dès lors qu'un élément de l'infraction a été commis sur le territoire américain. De plus, tout citoyen ou entité américaine est punissable, et ce même si

**“Même si le système pénal américain est très avancé en matière de protection de l'information au niveau microéconomique, la notion de secret d'affaires est difficile à cerner avec exactitude, tant il est difficile de préciser ce qu'est une information confidentielle.”**

aucun élément matériel n'a été réalisé sur le sol américain. D'application large, la disposition pose néanmoins problème au sujet du piratage informatique.

Ainsi, l'exigence d'une intention de profit économique exclut de toute sanction les hackers qui agissent par défi et non pour revendre l'information et en tirer un quelconque profit.

“L'American Espionage Act”, dont on peut saluer l'exhaustivité, est néanmoins sujet à différentes critiques. Outre les imprécisions en matière de définition du secret d'affaires et la place laissée à l'action jurisprudentielle dans sa détermination, dont il est question précédemment, la loi ne met pas à l'abri de certaines activités telles que le Reverse Engineering, dissection d'un produit fini pour en découvrir le secret de fabrication. Ainsi, non titulaire d'un brevet, CocaCola Inc prend le risque qu'un concurrent découvre la formule de fabrication de son produit. Si le secret était découvert, le concurrent aurait le droit de reconstituer un produit équivalent.

De même, la loi ne protège pas du “Parallel Development”, qui est l'action d'obtenir la même information, mais par une démarche propre. Dans ce cas, le concurrent a tout à fait le droit de procéder à la commercialisation du produit, car là encore aucun brevet ne fut déposé.

Même si le système pénal américain est très avancé en matière de protection de l'information au niveau micro

économique, la notion de secret d'affaires est difficile à cerner avec exactitude, tant il est difficile de préciser ce qu'est une information confidentielle.

Cette grande souplesse quant au contenu de l'information protégée laisse encore de grandes incertitudes quant à la nature des actes sanctionnés. Il appartient aujourd'hui aux juges de préciser cette notion. Pourtant, la jurisprudence tarde à apporter des réponses aux éléments problématiques du Cohen Act.

Tout d'abord car les cas où l'article 1832 fut appliqué ne portent que sur des situations claires, sans équivoque, et où les preuves furent faciles à apporter. Il semble que l'administration américaine ne se risque pas encore à prendre position sur les notions encore imprécises comme celle de “mesures raisonnables” ou de “connaissances générales”.

Par ailleurs, les sanctions prises, notamment les amendes, furent minimales. Ainsi, dans le cas Four Pillars, l'information volée était le résultat de 50 millions \$ de Recherche Développement.

Le commanditaire de l'acquisition frauduleuse fut condamné au paiement de 250 000 \$.

Pour finir, il est intéressant de constater le décalage entre la mise en pratique du Cohen Act et sa vocation première. Alors qu'en 1996, la motivation principale était la protection contre l'espionnage économique par des puissances étrangères, dont on dénombrait alors près de 600 cas selon le FBI, il apparaît qu'aucune décision prise sur fondement du Cohen Act ne porte sur de telles activités.

En somme, aucune décision n'a été rendue à partir de l'article 1831. Peut-être devrions-nous réfléchir aux raisons de ce mutisme juridique pour le moins surprenant.

Tout aussi exemplaire que soit la dynamique américaine en matière de protection juridique du patrimoine informationnel de l'entreprise, il convient de tenir compte de ses limites pour, à notre tour, enfin éclaircir la vaste zone d'ombre qu'est notre droit du secret des affaires. ☉