LA PROTECTION DU SECRET COMMERCIAL AUX USA - LA REVOLUTION DU DTSA

Philippe Girard-Foley

Avocat à la Cour (Paris)

Affiliate Member Law Institute Victoria (Australia)

LL.M. University of Pennsylvania

Une révision générale des pratiques commerciales s'impose avec urgence pour toutes les sociétés françaises en relation d'affaires avec les Etats-Unis, y compris les PME et ETI, à la suite de l'entrée en vigueur du DTSA. L'emploi du terme "révolution" ne parait nullement exagéré dans la mesure où la loi *Defend Trade Secrets Act* ("DTSA") signée le 11 mai 2016 par le President Obama et entrée immédiatement en vigueur est largement considérée par les commentateurs comme l'avancée législative en ce domaine la plus considérable depuis le *Lanham Act* de 1946. Conçu pour répondre aux nouveaux risques générés par les progrès technologiques facilitant l'espionnage industriel et commercial, le DTSA crée un droit pour les plaignants du secteur privé à introduire une instance en matière civile devant les tribunaux fédéraux, introduit une possibilité de saisie "*ex parte*" ainsi que d'autres dispositions visant toutes à amener le secret commercial au même niveau de protection que les autres branches de la propriété intellectuelle: marques, brevets et droit d'auteur.

1. La situation antérieure au DTSA

1.1. Jusqu'à l'adoption du DTSA, la protection du secret commercial reposait uniquement sur les lois d'état. 47 états et le *District of Columbia* (*Washington DC*) disposent d'une loi élaborée sur le modele du *Uniform Trade Secrets Act* ("UTSA"), mais chacun selon sa propre version. Il en résultait des disparités entre lois et jurisprudence d'état quant à des données aussi fondamentales que la définition du secret commercial ("*trade secret*"), celle de sa violation ("*misappropriation*") et les recours ("*remedies*") à la disposition des victimes. Dans les deux autres états, New York et Massachusetts la protection du secret commercial reposait uniquement sur la *common law*.

1.2. Au niveau fédéral, le "vol" de secrets commerciaux "*theft of trade secrets*" était qualifié de délit fédéral ("*fédéral crime*") par la Loi sur l'Espionnage Économique ("*Economic Espionage Act*") de 1996 tel que modifiée par le "*Foreign and Economic Espionage Penalty Enhancement Act*" de 2012. Des mesures civiles pouvaient ainsi être prononcées, telles qu'une ordonnance valant mise en demeure ("*injunctive relief*") mais l'action devant les juridictions civiles fédérales n'était ouverte qu'au procureur général ("*U.S. Attorney General*").

1.3. Pour les parties privées, une action devant les juridictions fédérales nécessitait de faire reconnaitre la compétence des tribunaux fédéraux par la démonstration d'une diversité (le litige devant impliquer plusieurs états du fait des parties ou de son objet) ou en tentant de lier la demande à une procédure distincte bénéficiant de la compétence fédérale. Dans tous les cas, cette preuve était difficile à établir.

2. Les avancées du DTSA

2.1. L'avancée essentielle réalisée par le DTSA consiste, par rapport à la situation antérieure telle qu'exposée ci-dessous, à ouvrir l'action civile devant les juridictions fédérales aux parties privées.

2.2. En outre, le DTSA améliore les capacités de défense des victimes de captation ou violation de secret commercial en ce qu'il:

- fournit des définitions claires et homogènes des concepts fondamentaux;
- introduit des mesures "*ex parte*"; et
- contient des dispositions plus favorables que certaines lois d'état non seulement au niveau des principes mais aussi à celui de la procédure. Par exemple, dans la version du UTSA adoptée dans l'état de Californie, le demandeur est tenu d'identifier dans le détail le secret commercial réputé être violé avant toute mise en oeuvre de la procédure ("*prediscovery trade secret identification*"), ce que le DTSA exige seulement en vue d'une saisie "*ex parte*".

3. La coexistence des systèmes

Le DTSA n'abolit pas le régime précédent, à la différence de certains autres textes fédéraux relatifs à la propriété intellectuelle qui se substituent à la législation d'état, mais lui superpose une législation fédérale en matière civile sauf en certaines matières où le DTSA écarte le droit de l'état (comme la doctrine de la "divulgation inévitable")

- Il demeure donc possible de choisir entre le système fédéral et celui de l'état concerné, même lorsque les conditions d'application du DSTA sont réunies. Dans certains cas, une loi d'état peut accorder une protection plus large que l'action fédérale, ou dans d'autres cas ce peuvent être des solutions tirées de la *common law* non contraires à la loi d'état s'il en existe une. Seul un examen cas par cas peut permettre de déterminer le régime le plus favorable.
- De même, l'application de la DTSA étant subordonnée à certains critères de diversité, des litiges intervenant purement à l'intérieur d'un état et impliquant des cas de violation simples de secret commercial comme le vol de listes de clients ou de tarifs demeureront soumis aux lois d'état et de la compétence des lois de l'état.

4. Le champ d'application du DTSA

4.1. Le droit à engager une action civile sur le fondement du DTSA est limité aux violations concernant un secret relatif à un produit ou à un service commercialisé ou offert à la commercialisation entre états ou à l'international ("*if the trade secret is related to a product or service used in, or intended to be used in, interstate or foreign commerce*").

4.2. Ce droit est reconnu aux propriétaires ("*owners*") de secrets commerciaux, sans que ce terme soit défini, ce qui ouvre une incertitude quant à l'applicabilité du texte lorsque ladite propriété fait l'objet d'une contestation préalablement ou lors de l'introduction de la demande.

4.3. Pour obtenir la protection du DTSA, le propriétaire doit bien évidemment prouver que le secret dont il allégué la violation constitue un secret commercial ("*trade secret*") au sens de la loi et que celui-ci a fait l'objet d'une violation ("*misappropriation*") au sens de cette même loi.

4.4. La définition du "*trade secret*" est donc d'une importance fondamentale. Elle couvre toute information ("*all forms and types of information*") et peut être de nature financière, liée aux affaires, scientifique, technique, économique, ou d'ingénierie ("*financial, business, scientific, technical, economic, or engineering information*") dès lors que:

- le propriétaire a pris des mesures "raisonnables" en vue de préserver le caractère secret de l'information ("*taken reasonable measures to keep such information secret*"); et
- l'information a une valeur économique distincte, réalisée ou potentielle, prenant son origine dans le fait de n'être ni connue ni susceptible d'être aisément obtenue par des moyens licites par une tierce personne qui tirerait une valeur économique par l'effet de son usage ou de sa divulgation. Cette définition quelque peu alambiquée est typique de la phraséologie de la législation américaine: "*the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information*".

4.5. Ce qu'il est intéressant de noter ici est que la définition ne repose pas sur le concept de valeur intrinsèque de l'information (le législateur aurait pu utiliser le mot "*intrinsic*") mais de valeur distincte ("*independent*"). La valeur n'est pas consubstantielle mais dérive uniquement du profit qui peut être retiré de l'usage ou de la divulgation… avec la conséquence logique que toute information, même anodine *a priori*, peut se voir reconnaitre la qualification de *trade secret*. Une définition potentiellement très large qui doit amener à ne négliger aucune des connaissances accumulées au sein de l'entreprise comme ayant vocation à être protégée au titre du DTSA.

4.6. En d'autres termes, vu sous l'angle de la préservation comme sous celui de l'absence de valeur intrinsèque, il n'existe pas de secret commercial par nature: un *trade secret* n'existe pas en tant que tel, il se crée.

4.7. La définition de la violation ("*misappropriation*") n'est pas moins importante. Il s'agit d'une définition complexe et "en cascade" typique du style de rédaction des lois des Etats-Unis.

Constitue une violation:

(a) l'obtention du secret commercial d'un tiers par une personne sachant ou ayant toute raison de savoir que ledit secret a été obtenu par des moyens illicites

ou

(b) la divulgation ou l'usage non autorisé par le propriétaire d'un secret commercial par une personne qui:

(i) a utilisé des moyens illicites pour se procurer ledit secret, ou

(ii) savait ou avait des raisons de savoir que la connaissance du secret:

- avait été obtenue par des moyens illicites; ou
- avait été obtenue sous condition d'en respecter le secret ou d'en faire un usage limite; ou
- avait été obtenue d'un personne tenue à en respecter la confidentialité;

ou

(iii) savait ou avait des raisons de savoir que l'information constituait un secret commercial et savait que l'obtention dudit secret était le résultat soit d'un accident soit d'une erreur.

4.8. La notion de moyens illicites ("*improper means*") fait l'objet d'une définition, sur le modèle, non pas du texte du UTSA mais de la jurisprudence dérivée de celui-ci.

Constituent un moyen illicite:

- le vol
- la corruption
- la tromperie
- la violation ou l'encouragement à la violation d'une obligation de préservation du secret
- l'espionnage utilisant des moyens électroniques ou autres moyens.

En revanche, la définition exclut expressément toute rétro-ingénierie et méthodes assimilées qui sont considérées comme des moyens légaux d'acquisition ("*reverse engineering, independent derivation, or any other means*").

5. Application dans le temps

5.1. Le DTSA n'a pas d'application rétroactive et ne concerne donc que les actes de violation commis après son entrée en vigueur, soit le 11 mai 2016.

5.2. L'action civile sur le fondement du DTSA est soumise à une prescription de trois ans à compter de la date à laquelle la violation a été découverte ou aurait dû être découverte par l'emploi d'une "diligence raisonnable" ("*reasonable diligence*").

5.3. Dans le cas de violation continue, celle-ci est réputée avoir été commise (et la durée de la prescription avoir commencé à être décomptée) à cette même date ("*a continuing misappropriation constitutes a single claim of misappropriation*").

5.4. Comme souvent, l'application internationale de la loi américaine est conçue de façon extensive, puisque s'étendant (selon une disposition du *Economic Espionage Act* précité non abrogée par le DTSA [U.S.C. § 1837]), à tout acte commis en

quelque lieu que ce soit, donc y compris en dehors du territoire des Etats-Unis, par un citoyen américain ou une entreprise américaine, mais aussi lorsqu'un acte en rapport avec la violation est commis sur territoire américain ("*an act in furtherance of the [misappropriation] was committed in the United States*". Ce dernier critère est bien sûr ouvert à interprétations.

6. La protection des lanceurs d'alerte

6.1. Le DTSA offre une protection aux lanceurs d'alerte ("*whistleblowers*") qui leur garantit l'immunité pour certains de leurs actes contre toute action pénale ou civile fondée sur une loi de protection du secret commercial, que celle-ci se situe au niveau de l'état ou au niveau fédéral ("*under any Federal or State trade secret law*"). Il s'agit par conséquent d'un domaine dans lequel, par exception au reste du texte, la loi fédérale DTSA se substitue à toute disposition contraire des lois d'état.

6.2. Les actes concernés sont:

(a) la divulgation d'un secret commercial;

(b) dans une des conditions requises pour que soit accordée la protection:

- sous forme confidentielle ("*in confidence*") à un agent public ("*government official*") ou un avocat ("*attorney*") dans le seul but de rapporter ou d'enquêter sur la violation présumée d'une loi, ou
- sous le sceau du Palais ("*under seal*") en qualité de pièce produite dans le cadre d'une procédure judiciaire ou assimilée.

6.3. De surcroit, les personnes intentant une action judiciaire dirigée contre une sanction de leur employeur dont ils prétendent qu'elle a été motivée par une dénonciation de leur part ("*retaliation suits*"), peuvent également divulguer le secret commercial concerné, mais uniquement:

(a) à leur propre avocat; ou

(b) dans le déroulement du procès, soit sous forme confidentielle ("*under seal*") soit sur ordre du tribunal.

6.4. Une préoccupation existe au regard de la divulgation auprès d'un agent public, car dès que celle-ci intervient, le propriétaire du secret commercial en perd le contrôle et ne dispose d'aucune autre protection que celle pouvant résulter de lois dont l'objet n'est pas directement celle du secret commercial comme le *Freedom of Information Act*.

6.5. Les "employeurs" ont l'obligation de porter cette immunité à la connaissance de leurs "employés" dans tout contrat comportant une clause relative à l'usage du secret commercial ou de toute autre information confidentielle ("*any contract or agreement with an employee that governs the use of a trade secret or other confidential information*").

L'obligation vise tous les contrats conclus ou modifies mais également complétés par un avenant ("*update*") après le 11 mai 2016, date d'entrée en vigueur du DTSA.

L'immunité peut être mentionnée soit dans le corps du contrat, soit par renvoi dans celui-ci (ou dans une annexe aux contrats existant) à un document externe décrivant la procédure pour la dénonciation des prétendues violations de la loi.

6.6. À cette fin, il est donné du terme "employé" ("*employee*") une définition très large, qui ne se limite pas aux personnes titulaires d'un contrat de travail et placées à ce titre sous un lien de subordination, mais aussi aux consultants et fournisseurs.

6.7. Le défaut d'information n'est pas sanctionné en tant que tel, mais indirectement en ce qu'il interdit à "l'employeur" de demander des dommages-intérêts punitifs ou le remboursement des frais d'avocat. Toutefois, on ne peut exclure que la jurisprudence étende la sanction de l'absence d'information au delà de la simple renonciation à ces chefs d'indemnisation jusqu'au rejet pur et simple de toute action contre un "employé" coupable d'avoir violé un secret commercial, ce qui devrait inciter les "employeurs" à mettre leurs contrats en conformité avec le DTSA.

6.8. Ceci souligne à nouveau le difficile arbitrage existant en droit américain entre droit de l'état et droit fédéral. En Californie par exemple, la loi de l'état sur la protection du secret commercial ne

prévoit pas explicitement d'indemnité au profit des lanceurs d'alerte, tout en précisant qu'elle n'a pas pour objet de faire obstacle aux dénonciations de situations illégales. Il peut donc être tentant pour un employeur dans cet état (a) de ne pas fournir a ses employés l'information prévue par le DTSA, (b) en cas de violation d'intenter une action n'incluant pas une demande de dommages-intérêts punitifs et remboursement des frais d'avocats, et (c) d'engager séparément sur la base des mêmes faits et contre les mêmes personnes une action en responsabilité. Ce qui est possible puisque le DTSA n'interdit pas les actions en responsabilité de droit commun ("*tort claims*") pouvant être introduites précisément sur les mêmes fondements de violation aggravée ("*willful and malicious misappropriation*") qui auraient pu servir de base à une action en réparation civile au titre du DTSA si l'obligation d'information des employés avait été respectée. Un tel arbitrage est envisageable en théorie puisque le DTSA ne contient pas l'équivalent de la clause du UTSA (qui prévaut par l'effet de la jurisprudence même dans les états n'ayant pas adoptés cette clause) interdisant les actions distinctes pour les mêmes faits en matière de violation du secret commercial ("*displaces conflicting tort, restitutionary, and other law of this State providing civil remedies for misappropriation of a trade secret*").

6.9. Par ailleurs, seule est concernée la "dénonciation légale" sans que soient affectées les lois interdisant l'accès à l'information par des voies non autorisées, comme le *Computer Fraud and Abuse Act*.

6.10. Une révision des contrats concernés, sinon impérative, est donc très souhaitable, comprenant tout contrat de travail ou de service, tout contrat conclu dans le cadre d'une relation commerciale (distribution, agence, franchise) ou dans le cadre d'une acquisition, contenant une clause se rapportant à la confidentialité des informations ("*confidentiality*"), la non divulgation ("*non disclosure*"), la non concurrence ("*non compete*") et la bonne conduite dans les affaires ("*code of conduct*").

7. Mesures conservatoires *ex parte*

7.1. Le propriétaire d'un secret commercial est désormais autorisé à demander à un tribunal fédéral la saisie d'objets dans la mesure où celle-ci est nécessaire pour empêcher la propagation ou la dissémination d'un secret commercial. Cette demande peut être faite *ex parte*, c'est-à-dire sans information ni présence des détenteurs des objets.

Certaines lois d'état prévoyaient déjà les saisies *ex parte* en matière de violation de secret commercial, mais tel n'était pas le cas du UTSA.

7.2. Le tribunal, toutefois, n'est pas tenu de prononcer la saisie demandée. Il lui revient de décider s'il est justifié de l'accorder, seulement en présence de "circonstances extraordinaires" ("*extraordinary circumstances*") et après s'être assuré que:

(a) il n'existe pas d'autre moyen en droit, telle une simple injonction restrictive ("*restraining order*") permettant d'aboutir au même résultat;

(b) il existe une certitude (et non pas seulement un risque ("*immediate and irreparable injury will occur*") de dommage immédiat et irréparable en l'absence de saisie;

(c) il existe une forte probabilité ("*likely to succeed*") que le demandeur parvienne à prouver tant l'existence du secret commercial que sa violation par la personne visée par la demande de saisie;

(d) ladite personne est effectivement en possession du secret commercial et de l'objet devant être saisi; et

(e) soit seule soit de concert avec des tiers, cette personne, si elle était avertie au préalable de la saisie:

- procéderait à la destruction, au déplacement ou à la dissimulation de la preuve de la violation, ou
- empêcherait le tribunal par tout autre moyen d'y avoir accès.

Il faut en outre que le demandeur décrive avec suffisamment de précision l'objet de la saisie et dans toute la mesure du possible, son emplacement.

7.3. Avant la saisie, le DTSA interdit expressément les copies de documents saisis et exige du tribunal qu'il formule de façon détaillée la façon dont devra se dérouler la saisie, notamment la date exacte de celle-ci et le droit de recourir à la force si les éléments objets de la saisie sont inaccessibles.

7.4. Après la saisie par des policiers fédéraux:

- le ou les objets ainsi saisis doivent être placés sous la protection du tribunal et conservés en un lieu interdisant tout accès physique ou électronique.
- le tribunal doit tenir une audience dans les sept jours suivant la saisie, au cours de laquelle le demandeur devra prouver les éléments de fait et de droit justifiant ladite saisie.

7.5. D'autres dispositions du DTSA ont pour objet d'éviter que la procédure de saisie *ex parte* ne soit utilisée à des fins anticoncurrentielles:

- il est de la responsabilité du tribunal de prendre toutes mesures nécessaires afin d'éviter que la saisie soit connue des tiers.
- une saisie injustifiée ou excessive ("*wrongful or excessive*") peut donner lieu à dommages-intérêts au profit de la personne contre qui elle a été dirigée.

7.6. Toutefois et à l'inverse de certaines législations comme la version du UTSA adoptée comme loi de l'état en Californie, le DTSA n'oblige pas le plaignant à identifier le détail des éléments de secret commercial qu'il allègue avant le début de la procédure de recherche des preuves chez la partie adverse ("*discovery*").

7.7. Le législateur, étant manifestement conscient des difficultés que ces règles pouvaient rencontrer dans leur application, a demandé (dans le chapitre six du DTSA) que soit confié au *Federal Judicial Center* (agence chargée de l'éducation et de la recherche pour les tribunaux fédéraux) de formuler des recommandations ("*best practices*") destinées aux tribunaux en rapport avec les saisies d'information et stockage des secrets commerciaux.

8. L'exclusion de la doctrine de la "divulgation inévitable"

Certaines loi d'état pour la protection du secret commercial autorisent le tribunal à délivrer une ordonnance interdisant l'emploi d'une personne par un nouvel employeur sur la seule base de l'information dont cette personne est détentrice ("*inevitable disclosure*").

Le DTSA écarte cette notion et la remplace par celle de risque effectif de violation ("*threatened misappropriation and not merely on the information the person knows*").

A nouveau, ceci illustre le rapport entre droit de l'état et droit fédéral: il peut être avantageux pour un employeur d'ignorer le DTSA et d'intenter une action fondée sur le droit de l'état dont l'exigence en matière de preuve, alignée sur le critère posé par l'UTSA, est moins contraignant.

9. Sanction et indemnisation de la violation du secret commercial

9.1. Le DTSA n'apporte pas de changement aux sanctions et remèdes pouvant être prononcés par le tribunal, qui demeurent les mêmes que sous le régime du UTSA:

- injonction;
- dommages-intérêts;
- ou alternativement, redevances justifiées en réparation du préjudice effectivement subi ou compensatoires de l'enrichissement sans cause.

9.2. Dans les cas de violation aggravée ("*willful and malicious misappropriation*") le DTSA autorise le tribunal à prononcer:

- le remboursement des frais d'avocats engagés par le demandeur;

- le paiement de dommages-intérêts punitifs d'un montant ne pouvant excéder le double des dommages-intérêts compensatoires.

9.3. Reconnaissant la difficulté que peut rencontrer un tribunal à évaluer le préjudice immédiat, le DTSA l'autorise, dans des circonstances exceptionnelles qui rendraient une injonction inéquitable, à subordonner l'usage futur d'un secret commercial au paiement d'une redevance d'un montant justifié ("*reasonable royalty*") pour une durée ne pouvant excéder la période durant laquelle l'usage du secret commercial aurait pu être interdit.

9.4. Le DTSA ne fait pas que modifier la Loi sur l'Espionnage Economique ("*Economic Espionage Act*") de 1996 modifiée par le "*Foreign and Economic Espionage Penalty Enhancement Act*" de 2012, elle aggrave les sanctions pénales prévues par 18 U.S.C § 1832, la section du chapitre du *United States Code* consacré au droit pénal (*title 18 of the U.S.C. "Crimes and Criminal Procedure"*) qui concerne le vol de secrets commerciaux ("*Theft of trade secrets*").

Cette section du U.S.C. ("Chapter 90 of title 18") vise (en résumé) le fait de voler, s'approprier, dissimuler, copier par tous moyens, recevoir, acheter ou posséder en connaissance de cause un secret commercial en vue d'en tirer profit, ou en vue de causer préjudice à son propriétaire.

Dans la version précédente, la pénalité maximale encourue était de 5 millions US$, dans la version telle que modifiée par le DTSA, cette sanction est portée à la plus élevée des deux sommes: 5 millions US$ ou le triple de la valeur du secret commercial dérobé y compris les frais de recherche, de mise en forme ("*design*") et autres frais de reproduction du secret commercial que la partie coupable aura pu s'épargner.

9.5. En outre, le DTSA dispose que de tels actes peuvent constituer désormais des actes qualifiés d'activités criminelles tombant sous le coup du "RICO" ("*Racketeer Influenced and Corrupt Organizations Act*"), ce qui du reste n'est pas sans conséquence à l'international compte tenu de l'application extra-territoriale de ce texte par les tribunaux américains.

10. Les implications du DTSA et actions à prendre en conséquence

Les implications du DTSA pour les sociétés françaises de toutes tailles en relation d'affaires avec les Etats-Unis sont manifestement étendues et comprennent de multiples ramifications.

10.1. En matière de divulgation du secret commercial, ces sociétés peuvent être concurremment et même simultanément victimes et auteurs d'infraction. Il faut s'assurer à la fois que la protection de ses secrets commerciaux bénéficie des avancées du DTSA mais aussi que la société ne se rend pas coupable, directement ou indirectement par l'intermédiaire de ses partenaires commerciaux, de violation de secret commercial appartenant à un tiers. Une révision des pratiques et des documents est donc indispensable.

10.2. Plus précisément, toute société concernée doit:

- identifier ses secrets commerciaux;
- les valoriser en fonction des différentes hypothèses de perte, violation et utilisation par un tiers à des fins concurrentielles ou contraires aux intérêts de l'entreprise;
- lister et apprécier l'efficacité des moyens de protection existants;
- en cas d'insuffisance, organiser des moyens de détection et de protection efficace;
- concevoir et mettre en place des mesures destinées à empêcher la violation même involontaire de secrets commerciaux appartenant à des tiers;
- intégrer dans tous contrats où celle-ci doit figurer, la clause d'information sur l'immunité des lanceurs d'alerte prévue par le DTSA;
- concevoir et mettre en place des mesures spécifiques aux débuts et fins de contrat;
- concevoir et mettre en place des moyens de répondre immédiatement à toute accusation de violation de secret commercial appartenant à un tiers;

- s'assurer du respect de ses secrets commerciaux et du DTSA et autres textes applicables par les partenaires commerciaux.

10.3. La première étape doit consister à identifier les secrets commerciaux de l'entreprise, sur la base de la définition fournie par le DTSA, qui est très large comme indiqué au paragraphe 3 ci-dessus. Ceux-ci comprennent aussi les secrets commerciaux dont la société est propriétaire en France. L'inventaire en toute hypothèse constitue une démarche salutaire car le secret commercial dans toutes les juridictions n'est protégé par la loi que s'il l'est par son propriétaire, ce qui implique au premier chef d'en connaitre l'existence, le contenu et les limites.

10.4. Le domaine de ce qui au sein de l'entreprise est susceptible de constituer un secret commercial protégé par la loi étant fréquemment sous-estimé, il peut être utile de se référer à la définition donnée dans le DTSA de ce qui constitue "toute forme et type d'information":

- le DTSA fournit la définition suivante, déjà mentionnée au chapitre 3 ci-dessus: information de nature financière, liée aux affaires, scientifique, technique, économique, ou d'ingénierie ("financial, business, scientific, technical, economic, or engineering information").
- le DTSA complète cette définition en précisant qu'elle inclut tout modèle, plan, compilation, dispositif, formule, conception, prototype, méthode, techniques, procédé, procédure, programme ou codes ("*patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes*").
- Le DTSA précise encore que l'élément concerné est susceptible de protection indépendamment de savoir s'il se présente sous forme tangible ou intangible, et qu'il ait été ou non (et s'il l'est, sous quelque forme que ce soit) enregistré/conservé, compilé ou mis en mémoire sous forme physique, électronique, graphique, photographique ou par écrit ("*whether or how stored, compiled, or memorialised physically, electronically, graphically, photographically, or in writing*".

Dans la recherche en interne des secrets commerciaux faisant partie du patrimoine immatériel de l'entreprise, il ne faut donc écarter *a priori* aucun élément ou catégorie d'élément.

10.5. Il ne suffit pas d'identifier les secrets commerciaux, souvent latents, il est recommandé par surcroit (et ceci aide à les faire sortir de l'état de latence) de leur affecter une valeur. L'exercice n'est pas aisé mais constitue une étape nécessaire, et doit comprendre une évaluation du coût pour l'entreprise de la perte ou de la captation par un tiers du secret, totale ou partielle, selon les different cas de figure envisageables (divulgation à un ou plusieurs concurrents, divulgation auprès de l'industrie à laquelle appartient l'entreprise, divulgation auprès du public en général…).

10.6. Il convient ensuite d'identifier et d'apprécier l'efficacité des moyens mis en oeuvre par l'entreprise elle-même pour protéger ses secrets commerciaux. Ceux-ci sont trop souvent bien maigres, car la prise de conscience de la valeur des secrets commerciaux n'a pas encore vraiment pris forme au sein de nombreuses entreprises notamment françaises. Cette attitude procède généralement d'une préconception selon laquelle le secret commercial n'est pas protégeable: pas protégeable donc pas de valeur, donc pas de mesures de protection…ce cercle vicieux est à briser.

La réforme du DTSA qui met le secret commercial sur un pied d'égalité avec les autres piliers de la propriété intellectuelle que sont les marques, les brevets et le droit d'auteur, devrait alerter les responsables d'entreprises… Se rappeler que la formule du Coca Cola est protégée par un secret de fabrique, pas par un brevet!

10.7. La vulnérabilité de chaque secret commercial doit être examinée dans le détail. La décomposition du risque en ses éléments constitutifs permet de mieux l'apprécier, d'en organiser la défense et de se préparer a demander la protection par l'injonction et/ou l'indemnisation si celui-ci se matérialise.

10.8. Il en résulte logiquement que l'étape suivante doit consister à mettre en oeuvre tous les moyens pratiques disponibles de protection du secret commercial. La meilleure façon de convaincre un tribunal de l'existence et de la valeur d'un secret commercial est de le prendre soi-même au sérieux.

Ces moyens peuvent être des moyens physiques mais sont aussi et surtout des moyens contractuels, et ceci non seulement dans les contrats de travail mais dans tous documents avec les fournisseurs, distributeurs, agents, consultants…etc. Sont concernés non seulement les contrats les plus évidents, comme les contrats de distribution, mais aussi tous ceux portant sur le secret commercial même sans le désigner nommément, comme les accords de confidentialité ("*confidentiality agreements*"), accords de non divulgation ("*non disclosure agreements*"), accords de transfert ou de partage de données confidentielles ("*proprietary information assignment/sharing agreements*") soit isolés soit inclus dans un accord de coopération, de partenariat ou dans un accord de négociation préalable à une acquisition ou une cession.

10.9. Compte tenu de la généralité de la définition du terme "*employee*" dont les limites ne sont pas clairement connues, il est prudent et recommandable d'inclure aussi dans le périmètre de révision les contrats avec les fournisseurs, prestataires de services, partenaires dans une Joint Venture, les offres et documents précontractuels, les accords de non débauchage, les engagements de retour de matériel en fin de contrat…etc.

10.10. La dimension introduite par le travail à domicile ou "télétravail" doit être prise en compte, de même que l'usage partagé d'instruments tels qu'ordinateurs portables et téléphones intelligents, ainsi que l'autorisation expresse ou implicite de l'usage de tels instruments détenus privativement aux fins des besoins de l'entreprise ("*BYOD bring your own device*" plus répandu aux Etats-Unis qu'en France).

10.12. De même qu'aucun secret commercial ne devrait être négligé dans la rédaction de ces documents, de même doit-on s'assurer que la définition en est précise et rigoureuse, ni trop large ni trop vague ce qui ôterait son efficacité à la disposition protectrice.

10.13. Réciproquement, la société doit mettre en oeuvre si elles n'existent déjà ou renforcer dans le cas contraire les mesures visant à empêcher l'acquisition de secrets commerciaux appartenant à des tiers. Cette exigence ne connait pas de limite géographique mais dans la mesure où le marché américain est visé, une attention particulière doit être portée aux exigences du DTSA et généralement de la législation et jurisprudence des Etats-Unis en la matière.

10.14. Ensuite, la société doit intégrer dans tous les documents concernés (contrats de distribution, agence, franchise, consultant…etc., donc tous les types de contrats cités au paragraphe précédent, et *a fortiori* contrats de travail le cas échéant y compris par exemple avec des VIE) une mention de l'immunité de lancement d'alerte prévue par le DTSA.

10.15. S'agissant des relations avec les employés au sens strict, il est essentiel que la société mette en place des procédures (comprenant mais ne se limitant pas à des documents contractuels) visant à protéger dans les conditions légales les secrets commerciaux en rapport avec les entrées et sorties de personnel ainsi que les changements d'affectation ayant pour objet de rapprocher un employé de la source de secrets commerciaux ("*on-boarding and off-boarding*"). Plus généralement, une formation à intervalles réguliers serait souhaitable, ainsi que des entretiens de sortie ("*exit interviews*") si ceux-ci ne sont pas déjà en place. Le comportement de l'employé après la cessation de fonctions ne peut être négligé, dans le respect de l'intimité de celui-ci et des conditions de la loi, par exemple sous forme de rappels de ses obligations post-emploi ("*obligations reminders*"). Même en l'absence d'employés directs (si la société n'a pas de filiale aux Etats-Unis) cette précaution doit être étendue par voie contractuelle avec les distributeurs, agents et consultants aux employés respectifs de ceux-ci ayant accès ou pouvant avoir accès aux secrets commerciaux.

10.16. Il est important de prendre en considération sous cet angle défensif l'état de la technologie, qui facilite grandement la captation de secret commercial (délibérée ou accidentelle) notamment en fin de contrat (qui peut être un contrat de travail mais aussi un contrat de consultant, de distributeur ou d'agent) et prévoir une procédure en conséquence.

C'est d'ailleurs cette évolution technologique qui a été à l'origine du DTSA, ou plutôt son appréciation dans un document de 2013 du gouvernement des Etats-Unis intitulé "*Administration Strategy on Mitigating the Theft of U.S. Trade Secrets*" qui a mis l'accent sur l'élévation du risque en découlant pour la préservation des secrets commerciaux et a conduit progressivement le Congrès vers la rédaction puis l'adoption du DTSA.

10.17. La société doit avoir mis en place un mécanisme lui permettant de répondre rapidement et efficacement à toute accusation par un tiers de violation de son secret commercial. Ceci doit comprendre des moyens permettant de démontrer, en cas de menace de saisie *ex parte*, que des mesures alternatives et moins dommageables peuvent également convenir.

10.18. Parallèlement et en complément des mécanismes de défense, la société doit mettre en place des procédures lui permettant de détecter les violations de ses secrets commerciaux ou, à défaut, d'être en mesure de démontrer avoir fait preuve de la "diligence raisonnable" faute de quoi, selon le DTSA, le délai de prescription court à partir de la violation elle-même et non pas de sa découverte ou présumée découverte.

Dans la pratique, une société ne peut se contenter d'avoir mis en place des documents contractuels convenablement rédigés, elle doit aussi s'assurer que l'accès à ses secrets commerciaux au quotidien par ses consultants, distributeurs, agents, partenaires de *Joint Venture* et le cas échéant employés est géré de façon rigoureuse, de préférence sur la base de procédures préétablies comportant des échéanciers d'auto-vérification.

10.19. Enfin, elle doit s'assurer que ses partenaires commerciaux (consultants, distributeurs, agents, franchises…etc.) ont eux-mêmes pris les mesures adéquates visant à assurer;

- la protection des éléments de secret commercial qui leur auront être transmis de façon confidentielle; et
- le respect du DTSA et généralement de la législation américaine en matière de respect du secret commercial.

En conclusion, le DTSA est non seulement un texte générateur de nouveaux droits et de nouvelles obligations, il est également un texte qui rappelle et souligne opportunément la valeur du secret commercial en tant qu'actif incorporel de l'entreprise. Comme la marque, le brevet et dans une moindre mesure (dans certaines juridictions, comme la Chine et les États-Unis) le droit d'auteur, il n'existe pas sans mesures destinées à le protéger, et devient ainsi le quatrième pilier de la propriété intellectuelle.

Le secret commercial peut être efficace s'il est géré correctement, or il s'agit d'un mode de protection moins onéreux que le brevet ou même le certificat d'utilité: là ou il est possible, l'effort pour le protéger en vaut la peine, d'autant que les États-Unis ne sont pas le seul marché où s'applique le principe du "secret commercial protégé par la loi si protégé par son propriétaire", d'autres pays comme la Chine font de même.

P. G-F.