SOULIER BUNCH

Publié le 28 septembre 2016

Soulier Bunch, Cabinet d'avocats d'affaires basé à Paris et Lyon

Lire cet article en ligne

Vers une meilleure protection des secrets d'affaires

La connaissance constitue aujourd'hui la clé de l'innovation et du succès. La protection des secrets de l'entreprise est désormais devenue un enjeu important, la révélation illicite d'informations relatives à l'entreprise étant susceptible de porter atteinte à sa capacité concurrentielle dans un marché où la concurrence s'est exacerbée.

En l'état actuel du droit français, la loi ne protège que partiellement les informations commerciales et savoir-faire des entreprises, et ce, malgré la valeur commerciale considérable que ces informations peuvent représenter. L'expression « secret d'affaires » est pourtant fréquemment employée dans les textes français, législatifs et réglementaires (mentionné dans pas moins de 150 articles codifiés !), ainsi que par la jurisprudence, judiciaire comme administrative, sans être cependant définie ni être encadrée par un régime juridique spécifique.

Faute de texte spécial, le secret d'affaires est donc à l'heure actuelle protégé par un ensemble épars de dispositions, aussi bien sur le plan pénal que sur le plan civil (1).

La directive de l'Union Européenne (UE) 2016/943 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites règle cette problématique (la « Directive »). Elle a été adoptée le 8 juin 2016 par le Parlement européen et par le Conseil de l'UE et doit être transposée par les Etats membres de l'UE avant le 9 juin 2018 (article 19 de la Directive). La question qui se pose alors aux praticiens est de savoir comment sera désormais organisée la protection des secrets d'affaires (2).

1. La protection des secrets d'affaires en l'état actuel du droit français

1.1. En matière pénale

Si le secret d'affaires ne bénéficie d'aucune incrimination pénale qui lui soit dédiée, il se prête néanmoins à l'application de différentes infractions permettant une protection spécifique mais parcellaire sur la base de divers fondements :

- La violation du secret de fabrique : L'article L811-3 du code de la propriété intellectuelle[1] relatif à la violation du secret de fabrique confère une protection limitée qui ne concerne que les employés de l'entreprise et ne vise que les secrets de fabrication (excluant les renseignements d'ordre commercial). Ainsi, l'entreprise ne sera protégée qu'*a posteriori*, dès lors qu'il y aura eu divulgation du secret de fabrique.
- L'espionnage économique, en vertu de l'article 411-6 du code pénal[2], est réprimé s'il profite à une puissance ou à une entreprise étrangère, à condition que les intérêts fondamentaux de la Nation soient menacés.
- Le délit d'intrusion et d'entrave au fonctionnement d'un système automatisé de données[3]est une infraction qui a une portée limitée puisqu'il ne vise que des données contenues dans des systèmes informatiques et suppose qu'une intrusion dans ces systèmes informatiques soit avérée.

Les infractions de droit commun sont également applicables, selon les circonstances :

- Le vol, « la soustraction frauduleuse de la chose d'autrui » (art. 311-1 du code pénal), est une infraction qui s'applique difficilement aux informations, en raison de leur caractère immatériel. Une partie des juridictions refuse ainsi d'appliquer l'infraction de vol aux biens incorporels en dehors de tout vol de support matériel (cd-rom, disque dur…). Cependant, une évolution semble se profiler au travers de quelques décisions isolées qui, bien que n'étant pas des décisions de principe, commencent à privilégier le « vol-reproduction » au classique « vol-soustraction »[4].
- L'abus de confiance[5] suppose une remise préalable du bien détourné. En l'absence d'une telle remise des données confidentielles, l'infraction ne sera pas constituée.

1.2. En matière civile

En marge des actions pénales, les entreprises victimes d'une violation du secret d'affaires peuvent intenter des actions civiles en réparation aux fins d'obtenir le paiement de dommages-intérêts.

La jurisprudence reconnait que la captation déloyale d'informations sensibles constitue un délit civil. Pour couvrir ces informations, la jurisprudence a recours à la notion de « savoir-faire », le savoir-faire étant défini (par la doctrine et la jurisprudence) comme les « *informations de natures techniques, industrielles ou commerciales, identifiées et substantielles, non immédiatement accessibles au public et transmissibles* ». Cette expression, bien que plus vaste que le secret de fabrique ou le secret professionnel, ne demeure qu'une composante du secret d'affaires.

L'exploitation abusive du savoir-faire d'autrui est le plus souvent sanctionnée par le biais de l'action en responsabilité civile délictuelle qui prend la forme d'une action en concurrence déloyale. La mise en œuvre de cette action suppose de déceler une faute dans le comportement du salarié/concurrent/tiers ayant causé un préjudice à l'entreprise détentrice du savoir-faire.

En dehors de toute intervention contentieuse, il convient de relever que les entreprises peuvent également se prémunir contre les atteintes à leurs secrets d'affaires grâce à certaines précautions contractuelles, limitées toutefois par l'effet relatif des contrats.

Ainsi, en dépit de son importance économique, le secret d'affaires n'est pas, en tant que tel, efficacement protégé par le droit français. Cette situation devrait être comblée par la transposition de la Directive européenne du 8 juin 2016, à tout le moins sur le plan civil. En effet, contrairement à de multiples propositions de lois françaises étant intervenues par le passé (Proposition de loi Carayon en 2011 ou projet de loi Macron en 2014) qui prévoyaient une protection à la fois civile et pénale du secret d'affaires, la Directive ne traite que du volet civil.

2. La protection des secrets d'affaires aux termes de la Directive

2.1. La définition des « secrets d'affaires »

Les « secrets d'affaires » protégés par la Directive sont définis comme étant les savoir-faire et informations

commerciales de valeur, qui ne sont pas divulgués et que l'on entend garder confidentiels (article 2 de la Directive). Cette définition s'inspire directement de l'article 39 de l'accord sur les Aspects des Droits de Propriété Intellectuelle qui touchent au Commerce (ADPIC) de l'Organisation Mondiale du Commerce.

Pour être qualifiées de secrets d'affaires, les informations doivent répondre de façon cumulative aux trois critères suivants :

– « *elles ne sont pas généralement connues des personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou ne leur sont pas aisément accessibles,*

– *elles ont une valeur commerciale parce qu'elles sont secrètes,*

– *elles ont fait l'objet, de la part de la personne qui en a le contrôle de façon licite, de dispositions raisonnables, compte tenu des circonstances, destinées à les garder secrètes* ».

Ainsi, le caractère secret des informations n'a pas à être absolu, il suffit que ces dernières soient méconnues « *des personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question* ». Ce critère posera très certainement des difficultés d'appréciation, notamment s'agissant de savoir qui sont les personnes visées, dans quelle mesure considère-t-on qu'elles ont connaissance des informations en cause et de quelle manière il conviendra de le prouver.

En outre, les entreprises pourront agir efficacement en cas d'atteinte à leurs secrets d'affaires, à condition toutefois de prouver la valeur commerciale des informations qu'elles détiennent mais également, d'anticiper toute atteinte par la mise en place de « *dispositions raisonnables* », destinées à garder les informations en cause secrètes.

La valeur commerciale de l'information peut être effective ou potentielle (14^{e} considérant de la Directive). L'information secrète a une valeur commerciale dès lors que l'atteinte qui lui est portée est susceptible de nuire aux intérêts économiques, scientifiques et techniques du détenteur du secret, mais également à ses positions stratégiques et à sa capacité concurrentielle.

Bien que n'étant pas clairement définies, les « *dispositions raisonnables destinées à garder secrètes* » les informations de l'entreprise, semblent pouvoir, par exemple, consister en la consignation de l'information confidentielle, la rédaction de clauses de confidentialité, la négociation d'accords de non-divulgation ou encore, le contrôle d'accès aux informations ou le cryptage des informations, etc. Le caractère « raisonnable » de ces dispositions peut néanmoins rester sujet à interprétation.

2.2. La licéité ou l'illicéité de l'obtention, l'utilisation et la divulgation de secrets d'affaires

- **L'obtention, l'utilisation et la divulgation licites de secrets d'affaires**

L'article 3 de la Directive prévoit certaines hypothèses dans lesquelles l'obtention, l'utilisation et la divulgation de secrets d'affaires sont licites. Il s'agit notamment de cas dans lesquels l'obtention du secret d'affaires

procède d'une « *découverte ou d'une création indépendante* » ou encore de toute autre pratique « *conforme aux usages honnêtes en matière commerciale* ».

L'obtention d'un secret d'affaires est également licite lorsqu'elle résulte de l'exercice d'une ingénierie inverse[6] à partir d'un produit licitement en la possession de la personne qui obtient l'information, à condition cependant que cette dernière ne soit pas liée « *par une obligation juridiquement valide de limiter l'obtention du secret d'affaires* ».

L'obtention, l'utilisation ou la divulgation d'un secret d'affaires est également considérée comme licite dans la mesure où elle est requise ou autorisée par le droit de l'Union ou le droit national.

- **L'obtention, l'utilisation et la divulgation illicites de secrets d'affaires**

La Directive définit ensuite dans son article 4 l'obtention, l'utilisation et la divulgation illicites de secrets d'affaires, sachant que ces actes sont toujours accomplis sans le consentement du détenteur du secret d'affaires. Il s'agit notamment « *d'un accès non autorisé à tout document, objet, matériau, substance ou fichier électronique ou d'une appropriation ou copie non autorisée de ces éléments […] et de tout autre comportement qui, eu égard aux circonstances, est considéré comme contraire aux usages honnêtes en matière commerciale* ».

L'utilisation ou la divulgation d'un secret d'affaires est également considérée comme illicite lorsqu'elle est réalisée par une personne ayant obtenu le secret d'affaires de façon illicite, c'est-à-dire ayant agi en violation d'un accord de confidentialité ou d'une obligation contractuelle.

En outre, l'obtention, l'utilisation ou la divulgation d'un secret d'affaires est considérée comme illicite lorsque, au moment de ces actions, une personne savait ou aurait dû savoir que ledit secret d'affaires avait été obtenu d'une autre personne qui l'utilisait ou le divulguait de façon illicite.

Par ailleurs, « *la production, l'offre ou la mise sur le marché, ou l'importation, l'exportation ou le stockage à ces fins de biens en infraction sont aussi considérés comme une utilisation illicite d'un secret d'affaires lorsque la personne qui exerce ces activités savait ou […] aurait dû savoir que le secret d'affaires était utilisé de façon illicite* ».

2.3. Les dérogations apportées à la protection du secret d'affaires

La Directive ne porte atteinte ni à la liberté d'expression et d'information, ni à la possibilité de révélation de telles informations secrètes pour des motifs d'intérêt public (articles 1 et 5 de la Directive). En effet, le droit à la liberté d'information prime sur la protection du secret d'affaires dès lors que le but poursuivi est de protéger l'intérêt public ou un « intérêt légitime » reconnu par le droit de l'UE ou le droit national.

Les journalistes et « lanceurs d'alerte », qui étaient fermement opposés à l'adoption de cette Directive au motif qu'elle portait atteinte à la liberté d'expression et d'information, voient donc leurs revendications prises en compte avec l'instauration de ces dérogations limitant l'effet de la protection. Toutefois, on peut imaginer que

les notions d' « intérêt public » et d' « intérêt légitime » ne manqueront pas de susciter débats et controverses quant à leur interprétation.

D'autres dérogations sont apportées à la protection du secret d'affaires afin notamment de respecter au mieux la liberté du travail et « la mobilité des travailleurs » (article 1.3 de la Directive).

2.4. Les mesures judiciaires pouvant être mises en œuvre en cas d'atteinte aux secrets d'affaires

Au plus tard le 9 juin 2018, les Etats membres devront avoir mis à la disposition des « détenteurs de secrets d'affaires », contrôlant un secret d'affaires de façon licite, des « mesures, procédures et réparations nécessaires pour qu'une réparation au civil soit possible en cas d'obtention, d'utilisation et de divulgation illicites de secrets d'affaires ». Ces mesures devront respecter le principe de proportionnalité, être justes et équitables, effectives et dissuasives et elles ne devront pas être inutilement complexes, coûteuses ou longues à mettre en place (article 6 de la Directive).

- **Les mesures provisoires et conservatoires**

Les autorités judiciaires compétentes des Etats membres pourront ainsi prononcer, à la demande du détenteur de secrets d'affaires, des mesures provisoires et conservatoires, telles que :

– la cessation ou l'interdiction de l'utilisation ou de la divulgation du secret d'affaires à titre provisoire,

– l'interdiction de produire, d'offrir, de mettre sur le marché ou d'utiliser des biens en infraction, ou d'importer, d'exporter ou de stocker des biens en infraction ou encore,

– la saisie ou la remise des biens soupçonnés d'être en infraction (article 10 de la Directive).

Pour éviter les abus, l'article 11 de la Directive permet aux autorités d'exiger du demandeur qu'il fournisse tout élément de preuve de nature à justifier, avec un degré de certitude suffisant, la conviction qu'un secret d'affaires existe, que le demandeur en est le détenteur et que le secret d'affaires a été obtenu, utilisé ou divulgué de façon illicite. Cet article contraint les autorités judiciaires à prendre en compte un certain nombre d'éléments, tels que le comportement du défendeur, les conséquences de l'utilisation ou de la divulgation illicite ou encore la valeur du secret d'affaires ou les intérêts des tiers.

Les Etats membres devront, par ailleurs, veiller à ce que les autorités judiciaires puissent, en lieu et place des mesures précédemment citées, subordonner la poursuite de l'utilisation illicite alléguée d'un secret d'affaires à la constitution de garanties destinées à assurer l'indemnisation du détenteur de secrets d'affaires. En revanche, la divulgation d'un secret d'affaires en échange de la constitution de garanties n'est pas autorisée (article 10 de la Directive).

- **Les injonctions et mesures correctives**

En plus des mesures précédemment citées, en présence d'une décision judiciaire rendue au fond constatant

qu'il y a eu obtention, utilisation ou divulgation illicite d'un secret d'affaires, les autorités judiciaires compétentes pourront ordonner la destruction ou la remise au demandeur de tout ou partie de tout document, objet, matériau, substance ou fichier électronique qui contient ou matérialise le secret d'affaires.

En outre, les autorités compétentes pourront adopter des mesures correctives telles que :

– le rappel des biens en infraction se trouvant sur le marché,

– la suppression du caractère infractionnel du bien,

– la destruction des biens en infraction ou leur retrait du marché.

En cas de retrait des biens en infraction du marché, le détenteur de secrets d'affaires pourra demander à ce que ces biens lui soient remis ou demander leur remise à des organisations caritatives.

Ces différentes mesures seront mises en œuvre aux frais du contrevenant, à moins que des raisons particulières ne s'y opposent (article 12 de la Directive).

- **Les dommages et intérêts**

Les autorités judiciaires pourront également condamner le contrevenant au paiement de dommages et intérêts (article 14 de la Directive). Pour en fixer le montant, ces autorités pourront prendre en considération « *tous les facteurs appropriés tels que les conséquences économiques négatives, […] le préjudice moral* », ou bien « *fixer un montant forfaitaire de dommages et intérêts, sur la base d'éléments tels que, au moins, le montant des redevances ou droits qui auraient été dus si le contrevenant avait demandé l'autorisation d'utiliser le secret d'affaires en question*».

L'article 7.2 de la Directive dispose que le demandeur qui engage une procédure judiciaire abusivement ou de mauvaise foi peut notamment se voir condamné, à la demande du défendeur, à régler à ce dernier des dommages et intérêts.

Il est à noter également que la Directive, en son article 8, impose aux Etats de fixer un délai de prescription aux demandes et actions ayant pour fondement un secret d'affaires, lequel ne pourra excéder 6 ans.

En réalité, ces mesures ne permettent pas de véritablement sanctionner le contrevenant, il s'agit simplement de réparer le préjudice subi par le détenteur de secrets d'affaires dont les droits ont été atteints. Les auteurs de la Directive n'ont ainsi pas souhaité introduire des dommages et intérêts punitifs mais il reste possible pour les Etats membres, au moment de la transposition du texte, d'ajouter des sanctions pénales par exemple, de manière à dissuader plus amplement les atteintes aux secrets d'affaires.

2.5. La confidentialité des procédures contentieuses et des mesures de publicité

La mise en œuvre des différents moyens d'action des détenteurs de secrets d'affaires dont les droits seraient atteints ne doit pas faire courir de risques de publicité néfaste ou de divulgation d'informations sensibles et

confidentielles. Afin d'éviter ces risques, l'article 9 de la Directive fixe un certain nombre de règles visant à protéger la confidentialité des secrets d'affaires au cours des procédures contentieuses.

Les Etats membres de l'UE devront ainsi veiller à ce que toute personne participant à une procédure judiciaire relative à l'obtention, l'utilisation ou la divulgation illicite d'un secret d'affaires, ou ayant accès à des documents faisant partie d'une telle procédure, ne soient pas autorisée à utiliser ou divulguer un secret d'affaires que les autorités judiciaires compétentes ont, en réponse à la demande dûment motivée d'une partie intéressée, qualifié de confidentiel.

Les autorités compétentes peuvent, sur demande motivée de l'une des parties, prendre des mesures de restrictions d'accès aux documents versés aux débats mais aussi aux audiences et à leur retranscription ; une version non confidentielle des audiences, dans laquelle les informations sensibles sont supprimées, peut alors être mise à la disposition des personnes concernées.

En outre, en vertu de l'article 15 de la Directive, les mesures de publicité résultant de la décision qui aura été rendue doivent protéger le caractère confidentiel du secret en cause.

2.6. Conclusion

La Directive vient harmoniser au sein de l'UE la protection civile du secret d'affaires en permettant aux entreprises européennes de se protéger contre l'obtention, la diffusion ou l'exploitation d'informations confidentielles à vocation commerciale et de dimension stratégique. Une avancée indispensable pour l'Union Européenne dont la protection parcellaire et inégale selon les Etats n'était pas de nature à protéger de manière satisfaisante les entreprises contre les pratiques illicites qui entament leur compétitivité.

[1] « *Le fait pour tout directeur ou salarié d'une entreprise où il est employé, de révéler ou de tenter de révéler un secret de fabrique est puni de deux ans d'emprisonnement et de 30.000 euros d'amende* »

[2] « *Le fait de livrer ou de rendre accessibles à une puissance étrangère, à une entreprise ou organisation étrangère ou sous contrôle étranger ou à leurs agents des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts fondamentaux de la nation est puni de quinze ans de détention criminelle et de 225 000 euros d'amende* »

[3] « *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 euros d'amende* » (art. 323-1 du code pénal)

[4] Crim. 4 mars 2008, no 07-84.002 ; Crim. 20 mai 2015, no 14-81.336

[5] « *Le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien*

quelconque qui lui ont été remis et qu'elle a acceptés à charge, de les rendre, de les représenter ou d'en faire un usage déterminé » (art. 314-1 du code pénal)

[6] L'ingénierie inverse consiste à obtenir le renseignement secret en démontant ou en observant un produit mis à la disposition public.