Guide pratique

La protection des informations sensibles des entreprises

MEDEF

Pourquoi ce guide ?

Au sein du MEDEF, plusieurs secteurs professionnels ont fait le même constat : il est difficile pour les entreprises de préserver ou de protéger ce qui est pourtant essentiel à leur développement, à savoir leurs créations techniques, leur savoir-faire et plus largement leurs informations stratégiques.

Bien qu'elles n'en aient pas toujours conscience, les entreprises détiennent de nombreuses informations ayant une **valeur économique et stratégique** qui composent leur capital immatériel. Dans un contexte concurrentiel mondialisé, avec des relations commerciales souvent difficiles, ce capital immatériel permet à l'entreprise de se démarquer de la concurrence, de perdurer et de s'adapter aux besoins multiformes et évolutifs du marché.

Compte tenu de leur importance, ces informations sont exposées à de nombreuses menaces, parmi lesquelles figurent les risques de divulgation ou d'usages non autorisés provenant tant de l'intérieur de l'entreprise que de l'extérieur. Ces risques peuvent avoir de graves incidences sur la compétitivité de l'entreprise voire sur sa survie.

Sous la présidence d'Emmanuèle Perron, en 2013, le Comité de la Commande publique du MEDEF s'était saisi du sujet sous l'angle de la confidentialité des offres des candidats à la commande publique pour laquelle une demande de renforcement des textes communautaires avait été formulée[1]. Cette réflexion a finalement bien vite été élargie aux marchés privés qui connaissent la même problématique.

Compte tenu de la transversalité du sujet, le groupe constitué pour travailler sur ce thème a pu bénéficier de la coopération et de l'expertise des membres du Comité de la propriété intellectuelle du MEDEF.

Les rédacteurs de ce guide pratique ne prétendent pas à l'exhaustivité. Dans un domaine où les sources et les outils sont dispersés, ils ont souhaité donner, sous forme de fiches pratiques, quelques éléments de réponse et sensibiliser les entreprises sur ce sujet délicat.

Pourquoi une mise à jour en 2017 ?

Depuis la publication de la première version de ce guide plusieurs textes sont intervenus au premier rang desquels figure la directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 *sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites*, dite directive « *secret d'affaires* ».

Publiée le 15 juin 2016 au Journal Officiel de l'Union Européenne, cette directive prévoit qu'elle doit être transposée par les États Membres dans leur droit interne au plus tard le 9 juin 2018.

Il est apparu nécessaire, sans même attendre cette transposition et quelle que soit l'époque à laquelle elle sera effectuée, de mettre en lumière les principaux apports susceptibles d'impacter le contenu de ce guide.

En effet, il s'agit du prenier texte de l'Union européenne relatif à la protection du secret d'affaires.

Le secret d'affaires couvert par la directive concerne les informations secrètes ayant une valeur commerciale et ayant fait l'objet de dispositions raisonnables pour les garder secrètes.

Au terme de cette directive, les États membres devront prévoir des mesures et des procédures permettant la réparation du préjudice en cas d'obtention, d'utilisation et de divulgation illicites du secret d'affaires afin d'assurer un niveau de protection suffisant et similaire dans chaque État de l'Union.

1. Voir les « *Propositions du MEDEF pour améliorer la protection du secret et des créations techniques des entreprises* » décembre 2010.

Les fiches ont été revues dans un premier temps[2] afin d'intégrer les principaux apports de cette directive.

La révision tient compte également des nouveaux textes issus de la réforme de la commande publique[3], de la réforme du Code civil[4], de la loi « *Sapin II* »[5] et de la loi « *devoir de vigilance* »[6].

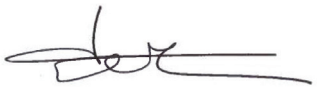
Enfin, une nouvelle fiche a été créée (Fiche n° 8), concernant la publication et les modalités de réutilisation des données des entreprises chargées d'une mission de service public, qui ont été étendues par la loi n° 2016-1321 du 7 octobre 2016 *pour une République numérique*, dite loi « *Lemaire* ».

Gilles de Bagneux

Président du Comité
de la Commande publique

Yves Blouin

Président du Groupe de travail
Protection des créations techniques



2. Une actualisation du guide sera effectuée, le cas échéant, une fois la directive « secret d'affaires » transposée.

3. Opérée par l'ordonnance n° 2015-899 du 23 juillet 2015 et le décret n° 2016-360 relatifs aux marchés publics et par le décret n° 2016-361 du 25 mars 2016 relatif aux marchés publics de défense ou de sécurité ainsi que par l'ordonnance n° 2016-65 du 29 janvier 2016 et le décret n° 2016-86 du 1er février 2016 relatifs aux contrats de concession.

4. Opérée par l'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations.

5. Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

6. Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre.

Table des matières

I. Identifier les données importantes de l'entreprise et signaler les informations confidentielles

La première démarche consiste à identifier et à répertorier les informations nécessitant des mesures de protection.

Cela nécessite un travail à mener de concert avec plusieurs services de l'entreprise : technique, bureau d'études, juridique, propriété intellectuelle, commercial, financier, etc.

Cette étape implique de décrire ces données, à savoir par exemple :

- **les informations techniques et technico-commerciales** : méthodes de conception, idées originales, connaissance des options techniques infructueuses, études spécifiques, savoir-faire, concepts technologiques, projet architectural, solutions innovantes, designs, algorithmes et logiciels, améliorations d'un processus de fabrication, combinaisons de matières pour une application donnée, plans, prototypes, modes de réglage d'un outillage, données d'essai de composants et de solutions techniques, données d'évaluation de fournisseurs, solutions spécifiques pour répondre à un cahier des charges, astuces technologiques permettant la réduction de coûts (consommation, entretien, maintenance), solutions de développement durable ;
- **les informations commerciales** : fichiers clients, fichiers fournisseurs, plans marketing, canaux et méthodes de distribution, résultats d'enquêtes marketing et d'évaluation de produits ;
- **les informations économiques et financières** : contenu des offres et propositions commerciales, prix d'achat et de vente, montage juridique et financier, conditions de contrat, assurances ;
- **les informations stratégiques et organisationnelles** : projets de rapprochements, méthodes et organisations propres à l'entreprise ou au groupement, projets de recrutement, synthèses résultant de la veille stratégique et technologique.

Il y a au moins deux niveaux d'informations : celles qui sont confidentielles et les autres.

Attention : Tout n'est pas confidentiel

Il faut agir avec discernement et ne pas considérer que toute information est confidentielle au risque de décrédibiliser la démarche.

L'article 2, 1) de la directive « *secret d'affaires* » **définit le secret d'affaires** comme « *des informations qui répondent à toutes les conditions suivantes :*

a. elles sont secrètes en ce sens que, dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, 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 ;

b. elles ont une valeur commerciale parce qu'elles sont secrètes ;

c. 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 ».

La démarche d'identification décrite ci-dessus conserve donc tout son intérêt.

Obtention licite d'un secret d'affaires

L'article 3, 1) de la directive « *secret d'affaires* » considère comme licite l'obtention d'un secret d'affaires par l'observation, l'étude, le démontage ou le test d'un produit ou d'un objet qui a été mis à la disposition du public ou qui est de façon licite en possession de la personne qui obtient l'information et qui n'est pas liée par une obligation juridiquement valide de limiter l'obtention du secret d'affaires.

Une fois les informations identifiées comme étant confidentielles, il convient, si nécessaire, de marquer comme telles celles qui revêtent une importance particulière. Ce signalement présente un intérêt tant en interne que vis-à-vis de l'extérieur de l'entreprise.

COMMENT SIGNALER LES INFORMATIONS SENSIBLES ?

- Apposer une mention telle que « confidentiel » sur les documents sensibles (offres, documents techniques, plans…) ainsi que dans les courriers ou courriels qui les accompagnent. Cette mention peut être complétée d'une clause type spécifiant l'usage restrictif qui doit être fait par son destinataire (pour évaluation de l'offre…), sous peine d'engager sa responsabilité.
- Décrire ces informations dans un accord de confidentialité dès lors que cela est possible.

Attention : le marquage peut s'avérer nécessaire mais n'est pas toujours suffisant

En interne, il importe de sensibiliser et d'impliquer les salariés (voir fiche n°3).

En externe, il est recommandé de signer des accords de confidentialité (voir fiche n°4), de rédiger des comptes rendus de réunions de travail (minutes, PV…) qui seront des indices utiles pour déterminer la paternité de telle ou telle information, et de déposer ces informations avant toute transmission (voir fiche n°2).

Dans certaines circonstances, notamment dans le cadre d'offres, la conclusion d'un accord de confidentialité est difficile. En tout état de cause, il faut veiller à ne pas communiquer plus que nécessaire pour l'évaluation de l'offre. En outre, il est fortement conseillé de :

- faire figurer la mention « **confidentiel** » sur les offres, documents techniques et plans qui méritent une confidentialité ;
- d'insérer des **clauses** mentionnant que l'offre et son contenu sont communiqués aux seules fins d'évaluation de l'offre, et rappelant tant la confidentialité de ces éléments que les obligations de non-divulgation et de non-réutilisation qui s'y attachent.

Ces mentions tendront à démontrer la mauvaise foi du destinataire qui aurait détourné ces données, par exemple en les confiant à un autre fournisseur pour l'établissement d'une (meilleure) offre de prix, ou faisant réaliser le projet par un tiers (sous-traitant) sans avoir retenu l'entreprise.

À ce sujet l'article 4, 3) de la directive « *secret d'affaires* » sanctionne l'obtention, l'utilisation et la divulgation d'informations obtenues en **violation d'un accord de confidentialité**, d'une obligation contractuelle ou de toute autre obligation de limiter l'utilisation du secret d'affaires.

II. Se ménager une preuve de la détention des informations et de leur date : « les dépôts privés »

Lorsque des informations techniques sont jugées spécialement précieuses ou stratégiques pour l'entreprise, cette dernière a intérêt à :

- constituer un dossier contenant la description de ces éléments ;
- faire un « dépôt privé », c'est-à-dire un dépôt non réglementé de données.

De telles formalités libres ne procurent aucun droit ni monopole, contrairement au dépôt d'un brevet par exemple. Elles permettent de prouver qu'à la « date certaine » du dépôt, l'entreprise détenait bien les informations pour l'établissement de la preuve de l'antériorité.

Celui qui peut **prouver la détention antérieure** se place dans une position plus favorable dans le cadre d'un litige : action en concurrence déloyale ou en manquement à un engagement de confidentialité (**voir fiche n° 9**).

Celui qui s'est ménagé un tel dépôt pourra plus facilement prouver qu'il est le **détenteur de secret d'affaires tel que défini par l'article 2, 2) de la directive « *secret d'affaires* »** comme « *toute personne physique ou morale qui a le contrôle d'un secret d'affaires de façon licite* ».

Se ménager une preuve de l'ancienneté de la détention permet également, si quelqu'un dépose ultérieurement un brevet, de continuer à exploiter l'invention malgré l'existence de ce brevet – c'est ce qu'on nomme la « possession personnelle antérieure[7] » en droit français.

QUELS SONT LES DIFFÉRENTS TYPES DE « DÉPÔTS PRIVÉS » ?

- **L'enveloppe Soleau** : *il s'agit d'une technique française qui permet, par le dépôt de l'enveloppe à l'institut national de la propriété industrielle (INPI) :*
  - de dater de façon certaine la détention de l'information figurant dans l'enveloppe ;
  - d'identifier le déposant comme étant détenteur de l'information ;
  - et en cas de différend, de procéder à son ouverture afin de prouver l'antériorité de sa détention par le déposant.

  Il ne s'agit en aucune façon d'un titre de propriété intellectuelle.

  Attention, elle ne peut contenir que 7 feuilles A4 (soit 14 pages en recto-verso) et pas de support numérique.

- **Les autres dépôts privés parmi lesquels on peut citer :**
  - le dépôt auprès d'un officier ministériel (huissier ou notaire) dont les actes donnent une date certaine aux dépôts ;
  - l'enregistrement notamment par le dépôt en ligne auprès d'un prestataire spécialisé ou de certaines institutions d'ingénieurs. Certains prestataires certifient la date à l'aide d'un horodatage et d'une signature électronique, d'autres font constater le dépôt par un acte d'huissier ;
  - l'envoi d'un courrier recommandé à soi-même (procédé simple et classique) qui, en cas de litige, pourra être ouvert devant un huissier.
- **L'archivage numérique** : *ces systèmes peuvent être utilisés par les entreprises de manière à fournir la preuve légale d'une date de possession d'une information.*

7. Article 617-7 du Code de la propriété intellectuelle.

QUE PEUT-ON DÉPOSER POUR ASSURER LA TRAÇABILITÉ ?

Tous types de documents et toutes informations, par exemple :

- *plans de fabrication ;*
- *notes de calcul ;*
- *description de procédés ou de savoir-faire ;*
- *études, pré-études ;*
- *cahiers de laboratoire qui permettent à ceux qui innovent de noter leurs activités en cours ;*
- *logiciels et données numériques.*

III. Impliquer le personnel et sécuriser les systèmes d'information et d'intranet

1. Impliquer le personnel

Il est impératif de sensibiliser et d'impliquer le personnel de tous les services de l'entreprise, et plus particulièrement lorsqu'ils ont accès à des informations sensibles. Le personnel doit avoir conscience de ce qui est confidentiel, ainsi que des précautions à prendre dans les relations avec les contacts extérieurs afin d'éviter toute divulgation accidentelle.

Il faut également souligner que la vigilance dans la protection des informations doit aussi s'exercer à l'égard des informations confidentielles reçues par l'entreprise de ses partenaires, clients et fournisseurs.

Les ingénieurs, techniciens et décideurs notamment, doivent être conscients de la valeur des informations qu'ils créent et des informations en leur possession. Cela concerne aussi particulièrement les acheteurs et les équipes marketing et commerciales qui ont à communiquer des informations à leurs interlocuteurs ou au public. Et même si tout n'a pas un caractère confidentiel, de nombreuses informations méritent une protection. Il convient donc d'être vigilant et de ne pas communiquer plus d'informations que nécessaire.

L'accès à l'information peut être réservé ou différencié selon la sensibilité de cette dernière et la catégorie de personnel.

Des **mesures de restriction** peuvent être prévues concernant la diffusion de certaines informations en interne (en fonction du poste occupé dans l'entreprise) et/ou à destination d'interlocuteurs extérieurs.

INFORMATIONS SENSIBLES - QUI A « BESOIN D'EN CONNAÎTRE » ?

Il est possible de créer dans l'entreprise une liste des personnes habilitées à connaître de telles informations. Cette liste peut figurer en annexe d'un accord de confidentialité.

S'agissant des informations **les plus sensibles (concernant par exemple un projet de recherche très important ou un projet de diversification ou d'acquisition)**, il est possible d'imaginer la mise en œuvre d'une protection renforcée par application d'une procédure de « besoin d'en connaître ».

En matière de secret défense, le besoin d'en connaître désigne la « *nécessité impérieuse de prendre connaissance d'une information dans le cadre d'une fonction déterminée pour la bonne exécution d'une mission précise*[8] ».

En application de ce principe, toute personne ne pourra accéder à une information sensible que si sa hiérarchie estime qu'elle remplit la condition du besoin d'en connaître[9]. Par conséquent, seules les personnes habilitées connaissent l'ensemble du dossier. Cela permet de limiter les risques de divulgation d'une information sensible, que celle-ci résulte d'une inattention ou de l'exercice d'une contrainte.

Les **contrats de travail** prévoient généralement des obligations pour le salarié, mais il peut en outre être conseillé de prévoir les instructions dans le règlement intérieur de l'entreprise.

8. Définition issue de l'instruction générale interministérielle sur la protection du secret de la défense nationale, n°1300/ SGDSN/PSE/PSD, du 23 juillet 2010, approuvée par l'arrêté du 30 novembre 2011 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale.

9. Concrètement, chacune des personnes habilitées doit signer un engagement spécifique au projet concerné et être informée des personnes à qui elle peut communiquer des informations concernant ce projet. La liste des personnes habilitées doit être mise à jour en fonction des changements dans l'organisation de l'entreprise et les mises à jour communiquées aux personnes concernées. Une telle procédure, relativement lourde, sera réservée pour les projets les plus sensibles.

DÉFINIR DES « RÈGLES DU JEU » OPPOSABLES AUX SALARIÉS, PAR LE BIAIS :

- *du contrat de travail (notamment d'une clause de confidentialité qui garde un effet au-delà de la fin du contrat de travail) ;*
- *d'un accord collectif ;*
- *du règlement intérieur ;*
- *d'une note de service ;*
- *d'une charte informatique (laquelle devra être annexée au règlement intérieur ou, à défaut, être introduite dans le contrat de travail).*

Attention : le salarié qui révèle un « secret de fabrique » est passible de sanctions pénales (voir fiche n° 9).

Le cas des stagiaires et des consultants non-salariés doit faire l'objet de conventions spécifiques assurant la confidentialité des informations et des résultats. Dans le cas des stagiaires, les relations avec les écoles et universités doivent être organisées pour éviter la divulgation d'informations confidentielles de l'entreprise et permettre la protection des résultats.

Toutefois, ces obligations de confidentialité ont été assouplies par des textes récents, qui permettent aux salariés de divulguer des informations sensibles dans certains contextes.

Ainsi, la loi « *Sapin II* » du 9 décembre 2016 instaure une protection pour tout salarié pouvant être qualifié de *lanceur d'alerte*[10].

Dans ce cas, si le lanceur d'alerte remplit les conditions fixées par la loi, l'employeur ne pourra pas invoquer les mesures mises en place au sein de l'entreprise pour garantir la confidentialité des informations ainsi divulguées.

De même, l'article L. 225.102-3, I du code de commerce issu de la loi « *devoir de vigilance* » impose aux grandes entreprises[11] d'établir un **plan de vigilance** comportant « *les mesures de vigilance raisonnable propres à identifier les risques et à prévenir les atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes ainsi que l'environnement* ». Parmi ces mesures, il doit prévoir un « *mécanisme d'alerte et de recueil des signalements relatifs à l'existence ou à la réalisation des risques* ». Un tel signalement pourra occasionner des révélations de secrets d'affaires, auxquelles l'employeur ne pourra pas s'opposer, dès lors qu'elles s'inscrivent dans le cadre fixé par la loi.

Par ailleurs, l'article 5, c) de la directive « *secret d'affaires* » prévoit que la divulgation par les salariés à leurs représentants est **licite** pour autant que cette divulgation soit nécessaire à l'exercice légitime de leurs fonctions.

10. Ainsi, en vertu de l'article 6 de la « *loi Sapin II* » est qualifié de lanceur d'alerte toute personne physique « *qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit […], ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance* ».

11. En l'espèce, il s'agit des sociétés par actions employant, en leur sein ou dans leurs filiales, au moins 5 000 salariés en France ou au moins 10 000 salariés dans le monde.

2. Sécuriser les systèmes d'information et d'intranet

Tous les utilisateurs de l'informatique à l'intérieur d'une entreprise accèdent à leurs systèmes par l'intermédiaire de terminaux informatiques : ordinateurs, assistants personnels, téléphones intelligents ou mobiles communicants. Quels qu'ils soient, ces terminaux constituent des points d'accès privilégiés au système d'information et leur sécurité doit donc être assurée.

Le développement des **intranets d'entreprise** représente un danger potentiel dans la mesure où des informations confidentielles y figurent ou sont accessibles de manière partagée. La confidentialité des informations sensibles de l'entreprise est mise en danger par le simple libre-accès de ces informations à l'ensemble des salariés. Des limitations dans l'accès à certaines informations sont souhaitables pour que seul le personnel autorisé puisse en avoir connaissance.

Ce danger peut prendre une ampleur particulière en cas d'accès à distance par les salariés à leur poste de travail depuis leur domicile ou un autre lieu. Pour éviter ce risque, l'employeur a la possibilité de prévoir des restrictions d'accès depuis l'extérieur.

Attention : l'intrusion d'un tiers dans les systèmes d'information de l'entreprise peut être sanctionnée pénalement (voir fiche n° 9).

Aux termes de l'article 4,2 de la directive « *secret d'affaires* », **l'obtention d'un secret d'affaires** est considérée comme illicite notamment lorsqu'elle est réalisée par le biais d'accès non autorisé à un document, à un fichier électronique ou d'une appropriation ou copie non autorisée de ces éléments.

IV. Protéger les informations par un accord de confidentialité

Un accord de confidentialité doit être signé le plus en amont possible avant tout échange significatif portant sur des informations sensibles.

Il a pour objet d'interdire la divulgation et l'usage non autorisé d'informations définies comme confidentielles et qui ont été communiquées à l'occasion d'une négociation (phases précontractuelles) ou d'un contrat (phases contractuelles). Dans ce dernier cas, les obligations de confidentialité peuvent être incluses dans le contrat.

Attention

Un accord de confidentialité n'a pas pour objet le transfert ou la cession de droits de propriété intellectuelle ou de savoir-faire. Les entreprises doivent être très vigilantes car on constate que parfois de telles cessions figurent dans un accord de confidentialité.

En outre, il est nécessaire de préciser dans l'accord de confidentialité que celui-ci, une fois signé, prévaut sur toute clause générale (clauses des conditions générales).

L'article 4, 3) de la directive « *secret d'affaires* » prévoit que **l'utilisation ou la divulgation d'un secret d'affaires** est considéré comme illicite notamment lorsqu'elle est réalisée en violation d'un accord de confidentialité ou d'une obligation contractuelle.

Les accords de confidentialité restent donc fortement recommandés.

Attention

En vertu de l'article 1112-2 du Code civil applicable depuis le 1er octobre 2016 « *celui qui utilise ou divulgue sans autorisation une information confidentielle obtenue à l'occasion des négociations engage sa responsabilité dans les conditions du droit commun* ».

1. Quelles informations peuvent faire l'objet d'un accord de confidentialité ?

Toutes les informations mentionnées dans la **fiche n°1** peuvent faire l'objet d'un accord de confidentialité (informations techniques…).

L'accord de confidentialité peut porter sur :

- les informations déjà identifiées et celles qu'il est prévu d'échanger ;
- les développements ou améliorations qui pourront résulter de l'exécution du futur contrat.

L'accord peut viser une liste d'informations/documents donnés ou un type d'informations se rapportant à un projet déterminé. Le champ des exclusions doit également être précisé (informations connues du partenaire ou tombant dans le domaine public).

Dans certains cas, il peut contenir la liste de personnes habilitées à recevoir l'information.

De même, il doit être prévu une obligation de faire respecter la confidentialité par les partenaires (filiales, sous-traitants, fournisseurs).

2. Faut-il prévoir une durée ?

Il faut fixer une durée de l'obligation de confidentialité qui dépendra de la teneur de l'information à protéger.

Il peut s'agir :

- de la durée des pourparlers plus un certain délai ;
- à laquelle peut s'ajouter la durée du contrat commercial plus, le cas échéant, un certain délai.

Si l'accord ne vise que la négociation, l'information, à défaut de mention d'une durée différente, cessera d'être confidentielle dès la fin de celle-ci.

3. L'accord doit-il être réciproque ou unilatéral ?

Tout dépend des flux d'informations qui méritent la confidentialité.

Exemples :

- L'entreprise signe un accord de confidentialité avec son client, afin de lui dévoiler des informations sur un produit futur en cours de développement → **l'accord peut être unilatéral**.
- L'entreprise signe un accord de confidentialité avec son client afin d'échanger des informations en vue d'un co-développement de produit ou de la réalisation d'un système → **l'accord doit être réciproque**.

Attention

En cas d'échanges bilatéraux d'informations, il est recommandé que l'accord de confidentialité soit réciproque. À défaut, en cas de litige, on ne peut exclure qu'un juge en vienne à estimer qu'il y a là un « *déséquilibre significatif dans les droits et obligations des parties* » ou, au moins, un indice d'un tel déséquilibre[12].

12. L'article L. 442-6 du Code de commerce sanctionne le fait de « *soumettre ou de tenter de soumettre un partenaire commercial à des obligations créant un déséquilibre significatif dans les droits et obligations des parties* ».

V. Comment protéger ses innovations ?

1. Le brevet

Le brevet est un titre de propriété industrielle qui protège une innovation technique, c'est-à-dire un produit ou un procédé qui apporte une solution technique à un problème technique donné. Il confère à son titulaire un droit d'interdiction de l'exploitation de l'invention brevetée par un tiers[13].

Pour être brevetable, l'invention doit être nouvelle, impliquer une activité inventive et être susceptible d'application industrielle. Les brevets ne protègent pas les méthodes, les formules mathématiques, les savoir-faire ou les idées en tant que telles, seulement leur mise en œuvre dans des produits ou procédés.

Pour que l'invention soit nouvelle il faut qu'au moment de la demande, elle n'ait pas été divulguée – sauf sous couvert d'un accord de confidentialité.

En outre, pour être titulaire d'un brevet, il faut effectuer un dépôt à l'Institut National de la Propriété Industrielle (INPI)[14]. En contrepartie de la protection, l'invention sera divulguée au public : en effet, les dépôts de brevets sont automatiquement publiés au bout de 18 mois.

En cas d'utilisation frauduleuse de l'invention brevetée, son titulaire pourra agir en contrefaçon afin d'obtenir notamment des dommages et intérêts. Le contrefacteur encourt par ailleurs des sanctions pénales.

La protection conférée a une durée limitée à vingt ans, non renouvelable, à compter du dépôt de la demande de brevet.

BREVET OU SECRET ? DES CHOIX STRATÉGIQUES

Le brevet confère à son titulaire un droit exclusif pour l'exploitation de l'invention, sous réserve des droits antérieurs des tiers. Il peut également être valorisé par la concession de licences d'utilisation, procurant ainsi un avantage financier et stratégique au titulaire.

Il présente des inconvénients et contraintes qu'il convient de prendre en compte avant d'opter pour cette protection :

- breveter impose de publier l'invention, qui va donc être connue de tous, en respectant l'exigence légale de « description suffisante ». Mais, le « noyau dur » que constitue le brevet peut s'accompagner de tout un savoir-faire qui n'a pas vocation à faire partie de la description de l'invention et ne fera donc pas l'objet de la publication ;
- le coût du brevet (coût initial et redevances périodiques) est un élément pouvant entrer en ligne de compte. Mais il ne faut pas perdre de vue que le maintien du secret ou de la confidentialité a également un coût, qui tend à augmenter avec le temps ;
- il ne suffit pas de déposer, il faut pouvoir défendre ses droits en cas de litige. Dans ce cas, le titulaire va parfois se trouver contraint, pour défendre ses droits, de fournir de nombreux éléments techniques qui risquent de mettre à mal les éléments confidentiels de l'entreprise.

13. Articles L. 611-1 et suivants du Code de la propriété intellectuelle.

14. Ou dans un organisme étranger.

UNE APPROCHE STRATÉGIQUE CONSISTERA DONC À :

- garder secrètes les informations pendant toute la phase de développement de l'innovation ;
- se poser la question de l'opportunité de breveter les inventions techniques entrant dans l'innovation lorsque celles-ci deviennent suffisamment matures ;
- faire alors le choix du brevet, au prix de la divulgation de l'invention au bout de 18 mois, ou du maintien au secret aussi longtemps que possible, au risque qu'un autre dépose indépendamment un brevet sur une invention similaire ;
- garder secrets les développements ultérieurs au dépôt du brevet, avec l'option de breveter certains d'entre eux.

L'information la plus vulnérable est celle qui ne sera ni brevetée, ni tenue secrète.

a. Secret ou confidentialité, quelle est la différence ?

Bien qu'il n'existe pas de définition valable dans tous les cas, et que ces termes soient le plus souvent employés l'un pour l'autre, on peut proposer la distinction suivante :

- **secret : désignerait des informations non communiquées.** Certains textes protègent le secret. C'est le cas de la directive « *secret d'affaires* ». C'est le cas également de l'article 39 du traité ADPIC (Accord sur les aspects des Droits de Propriété Intellectuelle qui touchent au Commerce) annexé au traité de Marrakech ayant institué l'OMC (Organisation Mondiale du Commerce). L'article 39.2 du traité ADPIC définit les « *renseignements non divulgués* » comme des renseignements secrets, qui ont une valeur commerciale parce qu'ils sont secrets et qui font l'objet de dispositions raisonnables, compte-tenu des circonstances, destinées à les garder secrets. Des renseignements sont secrets si, « *dans leur globalité ou dans la configuration et l'assemblage exacts de leurs éléments, ils ne sont pas généralement connus de personnes appartenant aux milieux qui s'occupent normalement du genre de renseignements en question ou ne leur sont pas aisément accessibles* » ;
- **confidentialité : désignerait des informations communiquées**, mais pour lesquelles on demande à celui qui les reçoit de ne pas les divulguer ou d'en faire un usage restreint – c'est l'objet des accords de confidentialité ainsi que des mentions et clauses de confidentialité (**voir fiche n°4**).

Bien entendu, une information confidentielle suppose d'abord qu'elle soit tenue secrète. Lors de sa communication, on demandera la confidentialité.

Ainsi les accords de confidentialité (*Non disclosure agreement*) utilisent parfois le terme de « Secret » (*Secrecy*).

b. Le brevet malgré la rupture de confidentialité

Celui qui est victime d'une rupture de confidentialité peut toutefois bénéficier d'un brevet, et cela dans deux hypothèses différentes :

- **1er cas : l'information a été divulguée**

  En principe, il n'est plus possible de déposer un brevet puisque l'invention a déjà été divulguée. Toutefois, la loi prévoit que l'information divulguée abusivement n'empêche pas le dépôt d'un brevet, sous certaines conditions.

- **2nd cas : l'information a été utilisée pour déposer un brevet**

  Le brevet obtenu grâce à des informations confidentielles peut faire l'objet d'une action en revendication[15] prévue par le titulaire de ces informations à l'article L. 611-8 du Code de la propriété intellectuelle.

15. Ce titulaire peut, sous réserve d'apporter la preuve de la détention antérieure de l'information, prétendre à revendiquer le brevet, c'est-à-dire, obtenir son transfert.

2. Le savoir-faire est-il protégé ?

En tant que tel, le savoir-faire (*know-how*) n'est pas protégé par un titre de propriété intellectuelle, conférant un « droit exclusif » comme peut le faire un brevet. Dans le domaine technologique, seule l'invention peut faire l'objet d'un tel titre, dans les conditions fixées par la législation sur les brevets. Le dépôt d'un brevet suppose une publication, alors que le savoir-faire peut être maintenu secret.

Au niveau européen, le savoir-faire est défini comme « *un ensemble d'informations pratiques non brevetées, résultant de l'expérience et testées, qui est :*

i. secret, c'est-à-dire qu'il n'est pas généralement connu ou facilement accessible ;

ii. substantiel, c'est-à-dire important et utile pour la production des produits contractuels, et ;

iii. identifié, c'est-à-dire décrit d'une façon suffisamment complète pour permettre de vérifier qu'il remplit les conditions de secret et de substantialité[16] *».*

Le savoir-faire peut bénéficier de la protection du secret des affaires instituée par la directive « *secret d'affaires* » sous réserve d'en respecter les conditions (voir la mise à jour de la **fiche n°1** et l'article 2, 1) de la directive).

L'entreprise aura en général un fond de savoir-faire général, et des manifestations particulières de ce savoir-faire développées à l'occasion de tel ou tel marché ou appel d'offres. L'utilisation par un client d'un savoir-faire sans accord et sans rémunération est considérée comme irrégulière[17]. Les contrats de vente ou de prestation précisent souvent qu'ils n'entraînent pas la cession des droits de propriété intellectuelle et du savoir-faire mis en œuvre. Le risque d'appropriation est limité pour un brevet, car la loi prévoit qu'il ne peut être cédé que sous des conditions bien précises, mais il est bien réel pour le savoir-faire.

Le savoir-faire peut faire l'objet de **licences**, que l'on désigne aussi par « transferts de technologie » :

- souvent, il s'agit de licences de brevet et de savoir-faire, car le brevet suffit rarement à mettre en œuvre la production. Il faut encore que soient communiqués des informations, conseils, documentations et formations, éléments traduisant le savoir-faire ;
- parfois, il s'agit de licences de savoir-faire indépendantes de tout brevet.

SAVOIR-FAIRE : LES BONNES PRATIQUES

La seule véritable protection du savoir-faire est le secret. Pour protéger son savoir-faire, l'entreprise doit :

- identifier le savoir-faire, s'en ménager la preuve, le mentionner dans ses offres et autres documents (**voir fiches n° 1 et 2**) ;
- si des éléments de savoir-faire sont communiqués, ne remettre que ce qui est strictement nécessaire (exemple : des plans d'ensemble et non des plans de détail), faire signer un accord de confidentialité (**voir la fiche n°4**) et veiller à ce que dans les contrats commerciaux, le savoir-faire soit préservé, à moins, le cas échéant, qu'un accord soit négocié avec une contrepartie et à des conditions équilibrées.

16. Article 1er du Règlement 772/2004 du 27 avril 2004 concernant l'application de l'article 81, paragraphe 3, du traité à des catégories d'accords de transfert de technologie. Ce règlement ne vise aucunement à accorder une protection juridique au savoir-faire, mais à définir dans quelles conditions les licences de brevets et/ou de savoir-faire sont licites au regard du droit de la concurrence. On s'y réfère fréquemment car il n'existe pas d'autre définition réglementaire dans les législations communautaires et française.

17. Voir le « *Guide pour la qualité des relations clients-fournisseurs* » de la Médiation des relations interentreprises (avec la direction des Affaires juridiques du ministère de l'Économie, l'INPI et la DGCIS : « L'exploitation de brevet ou de savoir-faire sans l'accord du sous-traitant est interdite par la loi. Les situations où un donneur d'ordre utilise un brevet ou un savoir-faire d'un sous-traitant dans un appel d'offres notamment, sans son accord et sans rémunération, rentrent dans ce cas de figure » (p.19).

VI. Protéger par le droit d'auteur

La protection de certaines informations sensibles de l'entreprise peut également être assurée par les garanties qu'offre le droit d'auteur aux œuvres de l'esprit en droit français.

Le droit d'auteur[18] protège en effet toute « œuvre de l'esprit » quel qu'en soit le genre, la forme d'expression, le support ou la destination, à l'exclusion toutefois des idées et des concepts.

Le droit d'auteur s'acquiert sans formalités, du fait même de la création de l'œuvre. La création est donc protégée à partir du jour où elle est réalisée[19].

Pour bénéficier de la protection par le droit d'auteur, la création doit simplement être originale, c'est-à-dire qu'elle doit porter la marque de la personnalité de l'auteur (cette condition étant appréciée largement dans le cas du logiciel par exemple).

QUELS TYPES DE DONNÉES SENSIBLES DE L'ENTREPRISE PEUVENT RELEVER DU DROIT D'AUTEUR ?

- Tous les écrits présentant un caractère original. Exemple : une plaquette, un site Internet.
- Les dessins et modèles et, à certaines conditions, des objets industriels dits de « l'art appliqué ».
- Les logiciels (codes-sources et codes-objets ou exécutables), y compris les matériels de conception préparatoire[20].
- Les structures des bases de données[21].

Le droit d'auteur confère à son titulaire deux types de droits :

- **le droit moral**, qui permet à son auteur de faire respecter l'intégrité de l'œuvre et de s'opposer à sa divulgation sans autorisation, ou à une divulgation qui la dénaturerait. Ce droit fait l'objet d'une protection perpétuelle. Il est inaliénable ;

- **les droits patrimoniaux**, qui confèrent un monopole d'exploitation économique sur l'œuvre. Leur durée de protection s'achève soixante-dix ans après le décès de l'auteur. Au terme de cette période, l'œuvre entre dans le domaine public.

18. Articles L. 111-1 et suivants du Code la propriété intellectuelle.

19. Remarque sur la diffusion de l'œuvre : le juge considère que « *l'exploitation d'une œuvre par une personne morale sous son nom fait présumer (…) que cette personne est titulaire de l'œuvre* » (Cour de cassation, 1ère chambre civile, 24 mars 1993). La diffusion s'oppose au secret, mais permet au moins de faire présumer qu'on est propriétaire de la création considérée.

20. L'article L. 112-2 du Code la propriété intellectuelle et l'arrêté du 22 décembre 1981 sur l'enrichissement de la langue française définissent les logiciels comme des programmes, procédés et règles, et éventuellement de la documentation, relatif au fonctionnement d'un ensemble de traitement de données.

21. Articles L. 112-3 et L. 341-1 et suivants du Code de la propriété intellectuelle.

Attention

En tout état de cause, pour faire valoir ses droits d'auteur sur une œuvre de l'esprit, il faut pouvoir établir la preuve de la date de la détention (voir fiche n° 2). Il est donc conseillé de s'en constituer la preuve en ayant recours, par exemple à :

- l'enveloppe Soleau ;

- le dépôt privé, on peut citer :

> le dépôt auprès d'un officier ministériel (huissier ou notaire) dont les actes donnent une date certaine aux dépôts,

> l'enregistrement notamment par le dépôt en ligne auprès d'un prestataire spécialisé ou de certaines institutions d'ingénieurs. Certains prestataires certifient la date à l'aide d'un horodatage et d'une signature électronique, d'autres font constater le dépôt par un acte d'huissier,

> l'envoi d'un courrier recommandé à soi-même (procédé simple et classique) qui, en cas de litige, pourra être ouvert devant un huissier.

Pour en savoir

- Agence pour la Protection des Programmes (APP) : **www.app.asso.fr**
- Société des Ingénieurs Et Scientifiques de France (IESF) : **http://home.iesf.fr**
- Société Civile des Auteurs Multimédia (Scam) : **www.scam.fr**
- Bibliothèque Nationale de France (BNF) : **www.bnf.fr**

VII. Assurer la confidentialité des offres dans le cadre des marchés publics et des concessions

1. Un principe général et d'application large

La confidentialité des offres est un principe de droit européen prévu par les dispositions des directives européennes relatives à la passation des marchés publics ainsi qu'à la passation des contrats de concessions (Directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 *sur la passation des marchés publics et abrogeant la directive 2004/18/CE* et Directive 2014/23/UE du Parlement européen et du Conseil du 26 février 2014 *sur l'attribution de contrats de concession*). Ces dispositions ont été reprises dans le droit français aux articles 44 de l'ordonnance n° 2015-899 du 23 juillet 2015 *relative aux marchés publics* et 38 de l'ordonnance n° 2016-65 du 29 janvier 2016 *relative aux contrats de concession*. Il en résulte pour les pouvoirs adjudicateurs et les entités adjudicatrices (autrement dit les acheteurs) l'interdiction de communiquer tout ou partie des éléments contenus dans les offres des candidats aux marchés publics et aux concessions.

CETTE INTERDICTION EST D'APPLICATION GÉNÉRALE ET CONCERNE :

- tous les types de marchés publics (issus des procédures d'appel d'offres, marché négocié, dialogue compétitif, MAPA…), et tous les types de contrats de concession (procédure ordinaire, procédure allégée) ;
- tous les types de pouvoirs adjudicateurs (État, collectivités locales…) et d'entités adjudicatrices ;
- toute offre, qu'elle comporte ou non, une mention de confidentialité.

2. Connaître les textes

Dans le cadre d'un contrat de la commande publique, il faut distinguer entre :

- la passation du marché ou de la concession et ;
- l'exécution du marché ou de la concession.

a. Au stade de la passation des marchés et des contrats de concession

L'acheteur public ou l'autorité concédante ne peut pas communiquer les informations confidentielles qu'il détient dans le cadre d'un marché dont la divulgation[22] :

- violerait le secret en matière industrielle et commerciale ou ;
- pourrait nuire à une concurrence loyale entre les opérateurs économiques notamment par la communication en cours de consultation du montant global ou du prix détaillé des offres.

Cependant, il peut demander aux candidats qu'ils consentent à ce que certaines de leurs informations confidentielles précisément désignées soient divulguées lorsqu'ils sont retenus pour l'exécution d'un marché.

Attention

Cette obligation de confidentialité demeure quand bien même les candidatures auraient été déclarées irrecevables au sens du IV de l'article 55 ou les offres inappropriées au sens du I de l'article 59 : l'acheteur ne doit pas utiliser les éléments confidentiels contenus dans les offres remises par les candidats.

22. Article 44 de l'ordonnance n° 2015-899 du 23 juillet 2015 *relative aux marchés publics* et article 38 de l'ordonnance n° 2016-65 du 29 janvier 2016 *relative aux contrats de concession*.

b. Au stade de l'exécution des marchés

La confidentialité des offres est régie, en France, par l'article 5 des différents Cahiers des Clauses Administratives Générales (CCAG), intitulé « *Confidentialité - Mesures de sécurité* » :

« *5. 1. Obligation de confidentialité :*

- *5. 1. 1. Le titulaire et le pouvoir adjudicateur qui, à l'occasion de l'exécution du marché, ont connaissance d'informations ou reçoivent communication de documents ou d'éléments de toute nature, signalés comme présentant un caractère confidentiel et relatifs notamment aux moyens à mettre en œuvre pour son exécution, au fonctionnement des services du titulaire ou du pouvoir adjudicateur, sont tenus de prendre toutes mesures nécessaires, afin d'éviter que ces informations, documents ou éléments ne soient divulgués à un tiers qui n'a pas à en connaître. Une partie ne peut demander la confidentialité d'in- formations, de documents ou d'éléments qu'elle a elle-même rendus publics ;*
- *5. 1. 2. Le titulaire doit informer ses sous-traitants des obligations de confidentialité et des mesures de sécurité qui s'imposent à lui pour l'exécution du marché. Il doit s'assurer du respect de ces obligations par ses sous-traitants ;*
- *5. 1. 3. Ne sont pas couverts par cette obligation de confidentialité les informations, documents ou éléments déjà accessibles au public, au moment où ils sont portés à la connaissance des parties au marché* ».

Cette obligation de confidentialité est fondamentale et son respect doit être garanti aux entreprises.

3. Être conscient des « dérapages »

Malgré l'existence d'une réglementation en principe protectrice, on déplore en pratique de trop nombreux détournements :

Exemples de pratiques illégales

- **Exemple 1** : L'entreprise H., PME de 48 personnes, fabrique des treuils et autres appareils de levage professionnels. Elle répond à des consultations en décrivant des propositions techniques précises. Elle a constaté, à plusieurs reprises, que les solutions techniques développées dans ses offres sont intégralement reprises sans son autorisation lors de consultations diverses lancées ultérieurement à la remise de celles-ci. Cette entreprise dépose peu de brevets mais réalise des innovations au fil des consultations, en trouvant chaque fois des solutions techniques originales permettant d'adapter les solutions techniques aux besoins de ses clients potentiels. Pour ce faire, outre ses produits standards, elle s'est dotée d'un département ingénierie spécialisé dans l'étude, l'implantation et l'intégration de treuils sur mesure. Les fréquents détournements dont elle est victime nuisent à son développement et annihilent ses investissements technologiques.

- **Exemple 2** : La société P. produit divers équipements nécessaires à la construction de ponts. Elle consacre beaucoup d'efforts et d'investissements en pré-études afin de réaliser un équipement répondant au cahier des charges précis du client, compte tenu de contraintes particulières à chaque affaire. Elle a récemment été consultée sur la base de ses propres plans, c'est-à-dire que le client ayant lancé un nouvel appel d'offres n'a pas hésité à réutiliser sa pré-étude, en enlevant son nom, afin de consulter à nouveau un panel de fournisseurs potentiels, espérant obtenir des offres moins chères sur cette base.

- **Exemple 3** : L'entreprise T., bureau d'ingénierie spécialisée dans le bâtiment, a déployé d'importants efforts humains et technologiques pour développer des solutions innovantes en matière de performance énergétique afin de répondre aux exigences du « Grenelle de l'environnement ». Elle a répondu à un marché public pour des bâtiments et mis en avant notamment ses solutions innovantes en matière de réduction de consommations d'énergie. La procédure a été déclarée infructueuse puis le marché

à nouveau relancé. L'entreprise T. a eu la mauvaise surprise de s'apercevoir que le maître d'ouvrage avait récupéré ses solutions techniques pour les intégrer dans les documents de cette nouvelle consultation.

4. Avoir les bons réflexes dans le contexte spécifique des marchés publics et des concessions

Sans préjudice des bonnes pratiques évoquées dans le présent guide (de l'identification des informations sensibles à la protection par un brevet en passant par l'implication du personnel), les entreprises peuvent exiger l'application stricte des dispositions évoquées ci-dessus. En effet, on constate trop souvent que les acheteurs publics ne prennent pas toute la mesure de l'obligation de confidentialité des offres faute de connaissance suffisante des textes applicables.

LES ENTREPRISES PEUVENT PAR EXEMPLE, DEMANDER LE RESPECT DE LEURS DROITS DE LA FAÇON SUIVANTE :

- *dans l'offre initiale ou en cours de procédure, si un doute émerge quant au respect de l'obligation de confidentialité,* ***préciser les éléments de l'offre qui sont confidentiels****. Attention néanmoins à ce que l'offre ne soit pas qualifiée d'irrégulière car incomplète au sens de l'article 59 du décret n° 2016-360 du 25 mars 2016 relatif aux marchés publics ;*
- *en cours d'exécution du marché,* ***veiller au respect des dispositions des CCAG relatives à la confidentialité*** *(article 5) lorsque ces dernières s'appliquent au marché concerné (ce qu'il convient de vérifier au préalable; c'est généralement le cas en pratique). En cas de méconnaissance de ces dispositions par le co-contractant du titulaire du marché, il pourra être envisagé d'enclencher la procédure facultative de règlement des différends prévue par les différents CCAG (en saisissant le Comité consultatif de règlement amiable des litiges) ;*
- *en toutes hypothèses, l'exercice d'un* ***recours contentieux***[23] *est également envisageable. Le non-respect de cette obligation de confidentialité par l'acheteur public, qui engage sa responsabilité, est sanctionné par le juge qui peut être conduit, le cas échéant, à annuler le marché*[24].

23. Voir la **fiche n° 9**.

24. Voir, pour une illustration en matière d'offres dématérialisées : Cour administrative d'appel de Paris, 20 mars 2012, CNAVTS, requête n°11PA02323 : « *la méconnaissance de l'obligation de confidentialité des candidatures et des offres constitue un manquement de nature à avoir eu une incidence déterminante sur le choix de l'attributaire justifiant l'annulation du contrat* ».

VIII. Entreprises privées ou publiques chargées d'une mission de service public

a. Obligation de communication

Le Code des Relations entre le Public et l'Administration (CRPA) prévoit que **les administrations, sont tenues de communiquer les documents qu'elles détiennent liés à leurs missions de service public, à l'exclusion des documents comportant des données à caractère personnel**[25].

Attention

L'article L. 321-3 CRPA issue de la loi « *Lemaire* » prévoit que les documents communicables sont réutilisables librement et gratuitement, à la seule exception des données sur lesquelles des tiers détiennent des droits de propriété intellectuelle.

Au sens de l'article L. 300-2 CRPA, sont qualifiées « ***d'administrations*** » l'État, les collectivités territoriales, ainsi que les autres personnes de droit public ou les personnes de droit privé chargées d'une mission de service public.

Exemples : entreprises chargées de l'exploitation d'un réseau de distribution d'eau, de la collecte des déchets, de l'énergie, des transports publics, de la restauration scolaire, etc.

Au sens de ce même article, sont considérés comme des « ***documents administratifs*** » tous les documents produits ou reçus dans le cadre de la mission de service public, y compris les bases de données et les données présentant un intérêt économique, social, sanitaire ou environnemental. Depuis la loi « *Lemaire* », **les codes sources** des logiciels sont considérés comme des documents administratifs soumis à l'obligation de communication.

L'article L. 311-9 du CRPA détaille les modalités de communication des documents administratifs, étant précisé que, depuis la loi « *Lemaire* », tous les documents existant en format électronique doivent obligatoirement être publiés (article L. 312-1-1 CRPA), c'est-à-dire mis en ligne, selon un échéancier d'application[26].

b. Exceptions

La loi dispense toutefois de l'obligation de communication certains types de documents :

- **documents non communicables** (article L. 311-5 CRPA) : ceux dont la communication porterait atteinte au bon fonctionnement des pouvoirs publics ou à un intérêt général, y compris, depuis la loi « *Lemaire* », à la sécurité des systèmes d'information des administrations ;
- **documents communicables seulement à l'intéressé** (personne concernée par l'information – article L. 311-6 CRPA) : notamment ceux dont la communication porterait atteinte au secret en matière commerciale et industrielle « *lequel comprend le secret des procédés, des informations économiques et financières et des stratégies commerciales ou industrielles et est apprécié en tenant compte, le cas échéant, du fait que la mission de service public est soumise à la concurrence*[27] ».

25. Article L. 311-1 CRPA

26. Article 8 de la loi « *Lemaire* ».

27. **Les documents couverts par le secret en matière commerciale et industrielle (site de la CADA)**.

Si l'information non communicable peut être séparée ou occultée dans le document, celui-ci est communicable sous cette condition (article L. 311-7 du CRPA).

Par ailleurs, l'article L. 311-4 du CRPA prévoit que les documents administratifs sont communiqués sous réserve des droits de propriété littéraire et artistique (voir la **fiche n° 6**).

Si la demande de communication de documents fait l'objet d'un contentieux judiciaire, le caractère contradictoire de la procédure exige en principe la communication à chacune des parties des éléments du dossier. Toutefois, cette exigence est exclue en ce qui concerne les documents dont le refus de communication est l'objet même du litige[28].

QUE DOIT-ON FAIRE ?

Les entreprises concernées doivent analyser chaque document, donnée ou base de données produits ou reçus dans le cadre de leur mission de service public, afin de déterminer s'ils sont communicables ou s'ils rentrent dans un des cas d'exception, notamment s'ils contiennent un secret en matière commerciale ou industrielle.

28. Voir en ce sens : Conseil d'État, sect., 23 décembre 1988, n° 95310, Banque de France c. Huberschwiller ; Cour administrative d'appel de Paris, 7 novembre 2003, n° 01PA01566, M. et Mme L.-C.

IX. Faire sanctionner les atteintes à la confidentialité des informations

Si, malgré les précautions prises pour protéger l'information sensible de l'entreprise, celle-ci constate des manquements, il reste la possibilité d'exercer des actions contentieuses.

La directive « *secret d'affaires* » impose aux États membres de mettre en place une série de mesures destinées à constater, faire cesser et indemniser les atteintes au secret d'affaires[29].

Dans l'attente de sa transposition, différents outils ou procédures judiciaires, décrits ci-dessous, peuvent être utilisés.

Attention

Les principes du procès équitable et de la loyauté des débats limitent fortement la prise en compte du secret des affaires. Le débat contradictoire organisé au cours des procédures judiciaires implique la communication, par chacune des parties, d'éléments de preuve qui contiennent parfois des informations confidentielles.

Toutefois, l'article 9 de la directive « *secret d'affaires* » prévoit une protection du caractère confidentiel des secrets d'affaires dans le cadre d'une procédure judiciaire qui met en cause précisément un secret d'affaires et qui est applicable à toutes les parties prenantes à la procédure.

Par ailleurs, l'article L. 483-2 du Code de commerce issu de l'ordonnance n° 2017-303 du 9 mars 2017 *relative aux actions en dommages et intérêts du fait des pratiques anti-concurrentielles* prévoit la possibilité de préserver le secret des affaires (huis clos, communication ou production partielle de pièces…).

Les modes alternatifs de résolution des litiges, comme la médiation ou l'arbitrage[30], présentent un intérêt certain dans la mesure où les tiers n'y ont pas accès, assurant ainsi une meilleure confidentialité aux parties.

1. La révélation du secret de fabrique par le salarié

Le cas spécifique du secret de fabrique[31] protège, en France, tout procédé de fabrication offrant un intérêt pratique et commercial mis en œuvre par un industriel et tenu caché par lui à ses concurrents qui avant la communication qui leur a été faite ne le connaissaient pas[32].

Afin de bénéficier des dispositions protectrices de la législation, il faut que la technique en cause réunisse quatre conditions cumulatives : elle est secrète, industrielle, originale et propre à l'entreprise.

Le fait de révéler ou de tenter de révéler un secret de fabrique est puni de deux ans d'emprisonnement et de 30 000 € d'amende. Toutefois, cette règle ne s'applique qu'aux salariés.

29. Articles 10 à 15 de la directive « *secret d'affaires* ».

30. Le décret n°2011-48 du 13 janvier 2011 portant réforme de l'arbitrage a modifié l'article 1464 du Code de procédure civile consacrant le principe de confidentialité de l'arbitrage en droit interne.

31. Articles L. 621-1 du Code de la propriété intellectuelle et article L. 1227-1 du Code du travail.

32. Cour appel Paris, 13 juin 1972, pourvoi rejeté par Cass. Crim., 20 juin 1973 : Ann. propr. ind. 1974. 85.

En outre :

- seule la communication est sanctionnée et non l'utilisation à des fins personnelles ;
- seul est visé le secret industriel, mais le secret commercial, comme par exemple un fichier clients, n'est pas concerné ;
- la divulgation doit émaner d'un salarié. Si elle provient d'un associé, d'un actionnaire ou d'un tiers, l'infraction n'est pas constituée ;
- il faut prouver l'intention frauduleuse.

2. La sanction disciplinaire en cas de faute lourde du salarié

La faute lourde est définie comme celle commise par le salarié dans l'intention de nuire à l'employeur ou à l'entreprise. La faute lourde emporte des conséquences graves (privation des indemnités de préavis et de licenciement et de l'indemnité compensatrice de congés payés). En outre, ce type de faute permet d'engager la responsabilité pécuniaire du salarié et de fonder une action en dommages et intérêts contre ce dernier.

Toutefois, le **lanceur d'alerte** est désormais protégé par loi « *Sapin II* » du 9 décembre 2016, qui interdit de sanctionner un salarié pour avoir signalé une alerte dans le respect des conditions fixées par la loi (article L. 1132-3-3 du Code du travail modifié). Cette protection est également prévue à l'article 5 de la directive « *secret d'affaires* » en vertu duquel, la protection des secrets d'affaires ne s'étend pas aux cas où la divulgation d'un secret d'affaires sert l'intérêt public, dans la mesure où elle permet de révéler une faute, un acte répréhensible ou une activité illégale directement pertinents.

3. La responsabilité contractuelle/délictuelle

Le droit des contrats[33] permet de sanctionner certains comportements fautifs des partenaires avec qui l'on est en relation contractuelle voire en négociation.

Comme il a été rappelé dans la **fiche n° 4**, l'article 1112-2 du Code civil, applicable depuis le 1er octobre 2016, stipule que « *celui qui utilise ou divulgue sans autorisation une information confidentielle obtenue à l'occasion des négociations engage sa responsabilité dans les conditions du droit commun* ».

Lorsque le contrat a été conclu, l'entreprise méconnaît son obligation d'exécuter de bonne foi un contrat si elle recourt à des renseignements obtenus dans le cadre de ces relations pour adresser des propositions à des tiers et obtenir un marché.

De même, les parties engagées dans une négociation précontractuelle sont tenues d'une obligation de bonne foi et ne peuvent, à la rupture des pourparlers, détourner les informations communiquées à l'occasion des négociations, même si aucune clause de confidentialité n'a été stipulée, sous peine d'engager sa responsabilité civile. Il est recommandé de prévoir un accord de confidentialité, qui confortera l'engagement.

Quand un accord de confidentialité a été signé, le manquement aux obligations qu'il contient engage la responsabilité contractuelle de celui qui est auteur du manquement.

On pourra soit demander l'application de la pénalité mentionnée dans l'accord, soit à défaut demander la réparation du préjudice.

33. L'article 1231-1 du Code civil qui pose le principe de la responsabilité contractuelle. L'article 1104 du même code prévoit l'obligation de bonne foi dans l'exécution des contrats.

4. La concurrence déloyale

La plupart des pays admettent la possibilité d'agir en responsabilité civile, et spécialement en concurrence déloyale en cas de préjudice résultant de l'appropriation et de la réutilisation abusive d'informations, mais selon des règles pouvant être très différentes d'un pays à l'autre – même au sein de l'Union européenne, au sein de laquelle le droit sur ce point n'est pas harmonisé[34].

En France, l'existence d'une concurrence déloyale est jugée selon les règles générales de la responsabilité civile délictuelle[35] et donne lieu à une jurisprudence abondante.

L'action permet de sanctionner certains comportements contraires au devoir de loyauté dans la relation de concurrence, alors même que la victime des agissements ne peut se prévaloir d'aucun droit privatif (par exemple un brevet, des dessins et modèles ou un droit d'auteur, auquel cas, elle pourrait agir en contrefaçon).

La victime peut engager la responsabilité civile délictuelle du fautif, (de l'auteur de la divulgation ou de l'utilisation à son profit du secret d'affaires) afin d'obtenir des dommages et intérêts. Pour pouvoir mettre en œuvre cette action, les conditions de la responsabilité civile doivent être remplies, à savoir une faute, un préjudice et un lien de causalité entre les deux. La réunion des preuves nécessaires au succès de cette action peut parfois s'avérer difficile.

5. L'abus de confiance

La victime d'une atteinte peut agir sur le fondement de l'abus de confiance, sanctionnée aux articles 314-1 et suivants du Code pénal. L'abus de confiance correspond au « 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 ». La faute constitutive du délit d'abus de confiance résulte du détournement d'informations confidentielles à la suite d'une remise préalable de ces informations. Plusieurs décisions[36] ont donné lieu, sur ce fondement, à des condamnations avec peines d'emprisonnement, des membres du personnel ayant conservé ou tenté de vendre des informations confidentielles de leur entreprise.

6. L'intrusion dans les systèmes d'information (loi Godfrain)

L'atteinte aux informations confidentielles peut résulter de l'intrusion volontaire d'un tiers dans les systèmes d'information protégés de l'entreprise. Lorsque les protections mises en place se sont révélées inefficaces, l'entreprise peut faire sanctionner cette intrusion pénalement. En effet, l'article 323-1 du Code pénal sanctionne « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* ».

Ainsi, toute pénétration ou tentative de pénétration dans un système informatique par une personne n'ayant pas le droit d'y accéder est incriminable, (la peine pouvant aller jusqu'à deux ans d'emprisonnement et 60 000 € d'amende).

L'article 323-3 du Code pénal sanctionne « *le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende* ».

34. Une étude commandée par la Commission européenne a mis en évidence de telles disparités – Voir *Study on Trade Secrets and Parasitic Copying (Look-alikes)* - MARKT/2010/20/D – 23 septembre 2011.

35. Article 1240 du Code civil.

36. Voir par exemple, TGI Clermont-Ferrand, ch. Corr. 21 juin 2010 ; TGI Versailles, ch. Corr. 18 décembre 2007.

L'étendue de ce texte a été élargie à plusieurs reprises et notamment par la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

7. Le vol d'information

Les juges ont souvent refusé de considérer l'appropriation de données ou d'informations comme du vol au sens du Code pénal, de sorte que l'on ne pouvait pas sanctionner ce comportement. Cependant, certaines décisions[37] ont, depuis quelques années, admis l'existence de vols de données informatiques, notamment en cas de simple copie de données informatiques. Il serait donc possible de chercher à sanctionner l'appropriation d'informations confidentielles sur le fondement du vol.

8. Les manquements aux règles spécifiques aux marchés publics et concessions[38]

La méconnaissance par un acheteur public du principe de confidentialité des offres peut être sanctionnée par le juge administratif territorialement compétent.

Au stade de la passation des marchés publics et des concessions, il existe plusieurs types de recours offerts aux candidats s'estimant lésés[39].

Au stade de l'exécution du marché, le même juge se référera aux stipulations contractuelles applicables (notamment le CCAG).

37. La jurisprudence considère tout d'abord que le vol d'information doit être accompagné du vol du support matériel de ladite information (Cass. Crim. 12 janvier 1989, n°87-82.265). Elle admet ensuite (dans certains cas), que l'information puisse faire l'objet d'un vol, indépendamment de son support (Cass. Crim. 4 mars 2008, n°07-84.002). Elle a enfin admis implicitement que le téléchargement d'informations sur un site à la suite d'une faille de sécurité de celui-ci représentait bien une « soustraction » et donc caractérisait un vol de données (Cass. Crim. 20 mai 2015, n°14-81.336).

38. Voir également la **fiche n°7**.

39. Pour plus de précisions, se référer à la fiche technique de la direction des Affaires Juridiques du ministère de l'Économie intitulée : « **Les recours contentieux liés à la passation des contrats de la commande publique** ».

Références et bibliographie

Rapports et colloques

- AIPPI, Association Internationale pour la Protection de la Propriété Intellectuelle, GRAPI (Groupe Rhône-Alpes de l'AIPPI) La protection des secrets d'affaires par les droits de Propriété Intellectuelle et le Droit de la concurrence déloyale, 17 mars 2010.

- Colloque de L'IRPI, Institut de recherche en propriété intellectuelle, Approches stratégiques de la propriété industrielle, éditions LexisNexis, Paris, 26 novembre 2010.

- Colloque PROMETHEUS, La protection juridique des informations à caractère économique - Enjeux et perspectives, Assemblée Nationale, 18 octobre 2010.

- DGCIS, Direction Générale de la Compétitivité, de l'Industrie et des services, L'innovation dans les entreprises – Moteurs, moyens et enjeux, mai 2011.

- HOGAN LOVELLS international LLP. *Report on Trade Secrets for the European Commission*, MARKT/2010/20/D, 23 septembre 2011.

- MATHON, C. La protection du Secret des Affaires : Enjeux et propositions – Mission du Haut Responsable chargé de l'Intelligence économique, 17 avril 2009.

Articles et ouvrages

- Breese, P. Stratégies de propriété industrielle - Guide des entreprises innovantes en action, Dunod, 2002.

- Cordier G. Un point-clé des accords de confidentialité : le contrôle par le communicant des informations communiquées, Revue *LexisNexis Jurisclasseur Communication* – Commerce électronique, avril 2008.

- Dumas, R. Transparence du patrimoine et protection du secret des affaires, Revue Lamy droit des affaires n°68, février 2012.

- Hagel, F. Protection des secrets d'affaires : enjeux et repères, Cahiers de droit de l'entreprise n°1, janvier-février 2012.

- Hagel, F. Secret et droits de propriété intellectuelle – Un tour d'horizon, Revue Lamy droit de l'immatériel, n°53, octobre 2009.

- Lemaire, C. La protection du secret des affaires devant le Conseil de la concurrence : une évolution bienvenue, JCP, éd. E, no 1161, 2006.

- Noëlle Lenoir, *La protection des secrets d'affaires, un droit fondamental du marché intérieur consacré à la directive 2016-943 du 8 juin 2016, Revue Lamy droit des affaires*, n°120, novembre 2016.

- Jean-Christophe Galloux, *L'adoption de la directive sur les secrets d'affaires*, Revue trimestrielle de droit commercial et de droit économique, Dalloz, janvier-mars 2017, page 59.

- *Le secret des affaires*, dossier par Jean-Claude Marin, procureur général près la Cour de cassation, La Semaine Juridique Entreprise et Affaires n° 35, 1er septembre 2016, 1454.

Sites Internet et divers

- Ministère de l'Économie
  Guide de la propriété intellectuelle dans les pôles de compétitivité

- INPI, Institut National de la Propriété Intellectuelle
  Enveloppe Soleau

- RESEAU C.U.R.I.E., Cahiers de laboratoire
  Valorisation, transfert de technologie et innovation issue de la recherche publique

- LEPAGE, A. et al.
  Le droit de savoir, Rapport 2010 de la Cour de Cassation

- CADA
  Commission d'Accès aux Documents Administratifs

- MEDEF
  Propositions du MEDEF pour améliorer la protection du secret et des créations techniques des entreprises, Décembre 2010.

Remerciements

L'élaboration de ce guide s'inscrit dans le cadre des actions engagées par le Comité de la Commande publique de la commission Droit de l'entreprise du MEDEF.

Le MEDEF tient à remercier les experts du Comité de la propriété intellectuelle de la commission Innovation du MEDEF pour leur expertise ainsi que les membres du groupe de travail Protection des créations techniques du Comité de la Commande publique qui ont contribué à la rédaction de ce guide, en particulier :

Yves Blouin
Président du groupe de travail protection des créations techniques du MEDEF
Responsable juridique, direction des Affaires Juridiques et Fiscales
Fédération des Industries Mécaniques - (FIM)

Emilie Choux
Juriste, direction des Affaires juridiques du MEDEF
Rapporteur du groupe de travail

Tiphaine Fritz
Juriste, direction des Affaires juridiques
Fédération Nationale des Travaux Publics - (FNTP)

Annabelle Huet
Chargée d'études, législation et affaires européennes
Union des Transports Publics et ferroviaires - (UTP)

Jérémy Simon
Chef de projet France 2020 - (MEDEF)

Françoise Vergriète-Matringes
Présidente de la Commission des Marchés Publics
Syndicat de l'industrie des technologies de l'information - (SFIB)

MEDEF
55, avenue Bosquet
75007 Paris
Tél. : 01.53.59.19.19

www.medef.fr

Contact :
Emilie Choux
echoux@medef.fr

Dépôt légal : juin 2017 - Tous droits réservés - N° ISBN : 978-2-86658-192-3