Guide pratique

La protection des informations sensibles des entreprises

3e édition - mars 2019

Commission Réforme publique et simplification

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.

Les entreprises détiennent de nombreuses informations ayant une valeur économique. Dans un contexte concurrentiel mondialisé, ce capital immatériel permet à l'entreprise de se démarquer de la concurrence, de se développer et de s'adapter aux besoins multiformes et évolutifs du marché.

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.

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 quelques éléments de réponse et des solutions concrètes afin d'aider les entreprises à protéger leurs informations sensibles et à faire valoir leurs droits.

Bonne lecture !

Gilles de Bagneux

Président du comité
de la Commande publique

Yves Blouin

Président du groupe de travail
Protection des créations techniques

La protection des informations sensibles des entreprises en quelques mots

Ce guide comprend 11 chapitres qui traitent des points suivants :

> Les informations peuvent être confidentielles, relever ou pas du secret des affaires, constituer ou pas des données personnelles (chapitre I).

> Dans tous les cas, il est important que l'entreprise commence par **identifier les informations sensibles** qu'elle détient, qui peuvent être de différents ordres : techniques, commerciales, financières, stratégiques, etc., voire les signaler comme telles (chapitre II).

> **La loi sur le secret des affaires** confère à ces informations une protection contre les obtentions ou divulgations illicites, et il faut s'assurer que les conditions en sont remplies (chapitre III).

> Il est recommandé de se ménager la preuve de la détention de ces informations, en réalisant des « **dépôts privés** » (chapitre IV).

> En interne, l'entreprise veillera à impliquer et **sensibiliser le personnel**, à limiter l'accès à certaines informations le cas échéant, et à sécuriser les systèmes d'information et d'intranet (chapitre V).

> Vis-à-vis de son environnement, il est important de protéger ses informations sensibles par des **accords de confidentialité**, en veillant aux questions de périmètre, de durée et de réciprocité (chapitre VI).

> Certaines innovations ou créations pourront bénéficier **d'un droit de propriété intellectuelle tel qu'un brevet** – avec un choix stratégique entre secret et brevet, et avec la question du savoir-faire – (chapitre VII), ou encore **d'un droit d'auteur** par exemple pour des dessins et modèles (chapitre VIII).

> En cas de **commande publique**, les textes prévoient un principe de confidentialité des offres, tant lors de la passation qu'à l'occasion de l'exécution des marchés (chapitre IX).

> Les **entreprises chargées d'une mission de service public** font l'objet d'un encadrement législatif particulier, qui les oblige à communiquer certaines informations au public, mais prévoit des exceptions en matière de secret (chapitre X).

> **Lorsqu'une entreprise est victime d'une atteinte** à la confidentialité de ses informations, elle doit connaître les moyens d'action (poursuite, sanctions) que la loi lui ouvre : ceux relatifs au secret des affaires, les sanctions spécifiques aux salariés et autres sanctions, pénales ou autres, spécifiques à certaines situations (chapitre XI).

SOMMAIRE

I. Quelques définitions

Il existe différents types de données et d'informations qui peuvent alternativement ou cumulativement :

- nécessiter une vigilance particulière ;
- bénéficier d'une protection spécifique ;
- occasionner des contraintes supplémentaires.

Qu'est-ce qu'une information sensible ?

Au sens du présent guide, il s'agit de toute information ayant une valeur économique et stratégique qui constitue une partie du capital immatériel d'une entreprise justifiant un traitement spécifique.

Peuvent constituer une information sensible :

- **une information protégée par le « secret des affaires »** : il s'agit de toute information qui n'est pas généralement connue ou aisément accessible par des personnes familières de ce type d'information en raison de leur secteur d'activité, qui présente une valeur commerciale (effective ou potentielle) du fait de son caractère secret et qui fait l'objet de mesures de protection raisonnables de la part de leur détenteur légitime (art. L. 151-1 du Code de commerce). Le caractère secret désigne toute information couverte par un texte qui en protège le secret ;

- **une donnée personnelle** : toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée »). Une donnée est donc à caractère personnel dès lors qu'elle permet d'identifier ou de rendre identifiable une personne physique, directement ou indirectement, par exemple par référence à un identifiant (adresse IP, numéro de Sécurité sociale, numéro d'adhérent, identifiant professionnel…) ou à un ou plusieurs éléments qui lui sont propres ou qui, combinés, peuvent être rattachés à une personne physique (numéro de téléphone, numéro de plaque d'immatriculation, numéro de série d'un véhicule…)[1].

  Les données personnelles peuvent faire l'objet d'un traitement (collecte, stockage, conservation, utilisation…), sous format numérique ou sous format papier, dès lors qu'elles sont organisées, classées et respectent les conditions fixées par le RGPD ;

- **une donnée non personnelle** : par opposition, toute donnée qui n'est pas à caractère personnel ;

- **une donnée confidentielle** : toute information communiquée, mais pour laquelle il convient de s'assurer que seules les personnes autorisées à la recevoir y ont accès. Celle-ci ne pourra pas faire l'objet d'une divulgation à des tiers non autorisés et pourra même faire l'objet d'un usage restreint, par exemple dans le cadre d'un accord de confidentialité ou d'une clause de confidentialité (cf. chapitre IV, « Se ménager une preuve de la détention des informations et de leur date »).

- **l' « intégrité de la donnée »** qui consiste à s'assurer que la donnée n'a pas été altérée durant sa communication, soit de manière intentionnelle, soit de manière non intentionnelle.

ATTENTION

La confidentialité est parfois obligatoire.

Certaines informations ne doivent pas être divulguées aux tiers (informations sensibles sur le plan concurrentiel). En effet, le droit de la concurrence interdit certains échanges d'informations entre entreprises, en particulier des informations sensibles de marché (exemple : prix ou autres données individuelles et qui ne sont pas généralement connues).

1. Article 4 du RGPD. Pour en savoir plus : guide pratique sur la protection des données personnelles du MEDEF (**www.medef.com/fr/content/guide-pratique-sur-la-protection-des-donnees-personnelles**), guide de la Cnil sur la sécurité des données personnelles (**www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf**), site de la Commission européenne sur les principes du RGPD (**https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr_fr**).

II. Que faire en présence d'une information sensible ?

La première démarche consiste à identifier et à classer les informations selon leur importance. Dans un second temps, il convient de déterminer celles qui nécessitent des mesures de protection spécifiques.

Ce travail doit être mené de concert par plusieurs services de l'entreprise : technique, bureau d'études, juridique, propriété intellectuelle, commercial, financier, etc.

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.**
- **La liste ci-dessous se contente d'énumérer les différents types d'informations susceptibles d'être rencontrées dans la vie d'une entreprise. Elle ne prend pas partie sur leur caractère confidentiel, qui dépendra des circonstances et du choix de l'entreprise.**

1. Quelles sont les informations sensibles susceptibles d'être classées comme confidentielles ?

- **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, données numériques industrielles de machine à machine fournissant des indications sur leur fonctionnement.
- **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, taux de marge, montage juridique et financier, conditions de contrat, assurances, données de performance financière.
- **Les informations stratégiques et organisationnelles** : organigrammes, projets de rapprochements, méthodes et organisations propres à l'entreprise ou au groupement, projets de recrutement, fichiers du personnel, synthèses résultant de la veille stratégique et technologique.

Parmi les informations confidentielles, certaines sont susceptibles de bénéficier de la protection du secret des affaires (cf. chapitre III, « Que vise la protection du secret des affaires ? »).

2. Comment signaler les informations confidentielles ?

Il existe plusieurs possibilités pour identifier et signaler des informations comme étant confidentielles.

À titre d'exemples :

- **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 (cf. chapitre VI, « Protéger les informations par un accord de confidentialité ») ;
- **protéger** l'accès aux informations (cf. chapitre V, « Impliquer le personnel et sécuriser les systèmes d'information et d'intranet »).

ATTENTION

L'indication de la mention « confidentiel » peut s'avérer nécessaire, mais n'est pas toujours suffisante.

En interne, il importe de sensibiliser et d'impliquer les salariés (cf. chapitre V).

En externe, il est recommandé de signer des accords de confidentialité (cf. chapitre VI), 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 (cf. chapitre IV).

Dans le cadre d'une proposition commerciale ou d'un devis, il est fortement conseillé :

- à chaque fois que cela est possible, de conclure un accord de confidentialité avec les clients/partenaires avant la remise de l'offre (cf. chapitre IV) ;
- 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.

Il faut veiller à ne pas communiquer plus que nécessaire pour l'évaluation de l'offre.

III. Que vise la protection du secret des affaires ?

La loi n°2018-670 du 30 juillet 2018 introduit dans le Code de commerce une nouvelle protection pour le secret des affaires. Cette loi prévoit une protection en faveur du titulaire d'une information sensible désigné comme le « détenteur légitime » contre l'obtention, l'utilisation et la divulgation illicites.

1. Définition du secret des affaires

L'article L. 151-1 du Code de commerce **définit le secret des affaires** comme « toute information répondant aux critères suivants :

1. *Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ;*

2. *Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ;*

3. *Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret ».*

2. Obtention/divulgation/utilisation

La protection bénéficie au « *détenteur légitime* » défini comme « celui qui en a le contrôle *de façon licite* » (C. com. art. L. 151-2, 2°).

L'obtention est considérée comme illicite lorsqu'elle est réalisée sans le consentement du détenteur légitime et qu'elle résulte :

- d'un « *accès non autorisé à tout document, objet, matériau, substance ou fichier numérique qui contient le secret ou dont il peut être déduit, ou bien d'une appropriation ou d'une copie non autorisée de ces éléments* » (C. com., art. L. 151-4, 1°) ;
- de « *tout autre comportement considéré, compte tenu des circonstances, comme déloyal et contraire aux usages en matière commerciale* » (C. com., art. L. 151-4,2°).

L'obtention d'une information protégée est licite lorsqu'elle concerne :

- « *une découverte ou une création indépendante* » ;
- « *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, sauf stipulation contractuelle interdisant ou limitant l'obtention du secret* »[2] (C. com., art. L. 151-3).

L'utilisation ou la divulgation sont illicites si :

- elles sont réalisées sans le consentement de son détenteur légitime par une personne qui a obtenu le secret de manière illicite ou qui agit en violation d'une obligation de ne pas divulguer le secret ou de limiter son utilisation (art. L. 151-5).

  Exemple : un accord de confidentialité, une clause de confidentialité voire une clause de non-concurrence, empêchent ou restreignent le droit d'utiliser ou de divulguer ;

- la production, l'offre ou la mise sur le marché, de même que l'importation, l'exportation ou le stockage à ces fins, lorsque la personne qui exerce ces activités savait, ou aurait dû savoir au regard des circonstances, que ce secret était utilisé de façon illicite ou avait été obtenu d'une autre personne qui l'utilisait ou le divulguait d'une façon illicite (C. com., art. L. 151-5, al. 2 et art. L. 151-6).

2. Cf. article L151-2 du Code de commerce.

Exemple : un concurrent fabrique des produits à l'aide d'un plan de fabrication que j'avais confié à mon sous-traitant et que ce dernier lui a transmis en violation d'un accord de confidentialité.

3. Quelles sanctions en cas de violation d'un secret des affaires ?

L'obtention, l'utilisation et la divulgation illicites d'un secret des affaires sont visées par la loi. Le détenteur légitime peut obtenir réparation de son préjudice (cf. chapitre XI, « Faire sanctionner les atteintes à la confidentialité des informations »).

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

Les informations sensibles peuvent faire l'objet de dépôts privés qui permettent de prouver qu'à la date du dépôt, l'entreprise était détentrice de ces informations.

Celui qui s'est ménagé un tel dépôt pourra plus facilement prouver qu'il est le **détenteur de secret des affaires tel que défini par l'article L. 151-2 du Code de commerce** comme « *celui qui en a le contrôle de façon licite* ».

Celui qui peut **prouver la détention antérieure** se place dans une position plus favorable dans le cadre d'un litige concernant une action en violation d'un secret des affaires, en concurrence déloyale ou en manquement à un engagement de confidentialité.

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[3] » en droit français.

ATTENTION

Ces dépôts ne confèrent pas un droit de propriété intellectuelle.

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

1. 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 ;
- en cas de différend, de procéder à l'ouverture de l'enveloppe afin de prouver l'antériorité de sa détention par le déposant.

À NOTER

En format papier, elle ne peut contenir que 7 feuilles A4 (soit 14 pages en recto-verso) ;en format numérique (« e-Soleau »[4]), cette restriction ne s'applique pas. Il est permis d'envoyer des fichiers jusqu'à 300 Mo dans des formats divers.

> 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 ;

3. Cf. article 613-7 du Code de la propriété intellectuelle.
4. www.inpi.fr/fr/services-et-prestations/e-soleau

- 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 ;
- le coffre-fort numérique, lorsqu'il est utilisé, doit répondre aux exigences fixées à l'article L. 103 du Code des postes et des communications électroniques[5]. Ce service de coffre-fort numérique a pour objet notamment la réception, le stockage, la transmission des documents électroniques exigeant l'intégrité et l'exactitude de leur origine, la traçabilité des opérations effectuées et l'identification de l'utilisateur lors de l'accès au service ;
- 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.

2. Quels documents peuvent faire l'objet d'un dépôt privé ?

Tous types de documents et toutes informations peuvent faire l'objet d'un dépôt privé, par exemple :

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

5. Décret n° 2018-853 du 5 octobre 2018 relatif aux conditions de récupération des documents et données stockés par un service de coffre-fort numérique (JO 7 octobre 2018).

V. 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 (ingénieurs, commerciaux, acheteurs…) et plus particulièrement lorsqu'ils ont accès à des informations sensibles.

a. Comment sensibiliser le personnel ? Règles de conduite

Le personnel doit avoir conscience de ce qui est confidentiel ou qui relève de la protection des données personnelles, ainsi que des précautions à prendre en interne (en cas de perte de clé USB par le salarié, d'utilisation de la boîte mail personnelle non sécurisée…) dans les relations avec les contacts extérieurs afin d'éviter toute divulgation accidentelle. Cette sensibilisation peut se formaliser par les actions suivantes :

- signature d'un engagement de confidentialité notamment dans le cadre d'une clause contenue dans le contrat de travail *qui garde un effet au-delà de l'expiration de ce dernier* ;
- accord collectif ;
- règlement intérieur ;
- élaboration d'une charte informatique ;
- formation interne ;
- diffusion de notes d'information, de service.

À NOTER

Le salarié qui révèle un « secret de fabrique » est passible de sanctions pénales (cf. chapitre XI, « Faire sanctionner les atteintes à la confidentialité des informations »).

b. Cas des personnes extérieures intervenant dans ou pour le compte de l'entreprise (stagiaires, consultants, intérimaires, sous-traitants…)

Ces intervenants doivent faire l'objet de conventions spécifiques assurant la confidentialité des informations et des résultats.

c. En matière de données personnelles

La loi impose la désignation d'un délégué à la protection des données ou Data Protection Officer (DPO) lorsque l'activité principale de l'entreprise consiste en un suivi régulier de données personnelles à grande échelle. Il est en charge de la sensibilisation du personnel et ses coordonnées doivent être communiquées aux collaborateurs.

Par ailleurs, quelle que soit l'activité de l'entreprise, il est recommandé de désigner un référent au sein de l'entreprise chargé de veiller au respect de la loi en matière de données personnelles.

d. Limiter l'accès aux informations sensibles

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

Comment limiter l'accès aux informations les plus sensibles (fichiers rh, projet de r&d, projet de diversification et d'acquisition…) ?

- Serveur compartimenté.
- Fichier verrouillé avec des mots de passe ou par chiffrement (ex : impossibilité d'ouvrir, de lire ou de modifier le fichier).
- Accès restreint aux locaux par badge, clé ou biométrie.
- Liste des personnes habilitées à connaître ces informations. Cette liste peut figurer en annexe d'un accord de confidentialité.

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*[6] ». En application de ce principe, une personne ne pourra accéder à une information sensible que si sa hiérarchie estime qu'elle remplit la condition du besoin d'en connaître[7]. 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.

e. Quand le salarié peut-il divulguer une information sensible ?

Certains textes permettent aux salariés de divulguer des informations sensibles sous conditions :

- **le lanceur d'alerte** : la loi Sapin II du 9 décembre 2016 instaure une protection pour tout salarié qualifié de « lanceur d'alerte »[8] (cf. paragraphe 3, chapitre XI, « Faire sanctionner les atteintes à la confidentialité ») ;

- **le plan de vigilance** : l'article L. 225.102-3, I du Code de commerce issu de la loi devoir de vigilance impose aux grandes entreprises[9] 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.

- **exercice légitime de ses fonctions par le salarié et ses représentants** : l'article L. 151-9 du Code de commerce prévoit que la divulgation de secrets des affaires par les salariés à leurs représentants est **licite** pour autant que cette divulgation soit nécessaire à l'exercice légitime de leurs fonctions.

Dans ces cas, l'employeur ne pourra pas invoquer les mesures mises en place au sein de l'entreprise pour garantir la confidentialité des informations ainsi divulguées.

6. 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.

7. Concrètement, chacune des personnes habilitées doit signer un engagement spécifique au projet concerné et doit 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.

8. 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 grave pour l'intérêt général, dont elle a eu personnellement connaissance ».

9. 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.

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

Les terminaux informatiques 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 risque potentiel dans la mesure où des informations confidentielles y 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.

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 (télétravail, déplacements professionnels, utilisation d'un wifi public…).

Dans le cas des données personnelles, le RGPD impose la mise en place de **mesures de sécurité dès la conception**[10] (également appelée « privacy by design »), qui doivent être mises en œuvre par le responsable du traitement.

Dans le cas d'**opérateurs de services essentiels**[11] **et d'importance vitale**, des obligations supplémentaires en matière de cybersécurité s'appliquent.

Dans le cas d'une « obtention illicite » d'un secret des affaires[12] **l'existence d'un système d'information sécurisé** permettra de bénéficier des **mesures de protection et de réparation** prévues par la loi sur le secret des affaires.

Par ailleurs, des textes spécifiques sanctionnent l'accès non autorisé dans les systèmes d'information de l'entreprise (cf. Chapitre XI, « Faire sanctionner les atteintes à la confidentialité des informations »).

10. Voir le guide de la CNIL (**www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles**) et le guide pratique sur la protection des données personnelles du MEDEF (**www.medef.com/fr/content/guide-pratique-sur-la-protection-des-donnees-personnelles**).
11. La liste des services essentiels est fixée par le décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
12. Article L151-1 et suivants du Code de commerce.

VI. 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).

Même si la loi sanctionne le fait d'utiliser ou de divulguer sans y avoir été autorisé des informations obtenues au cours de négociations, il est toujours fortement recommandé de signer un accord de confidentialité[13].

À NOTER

Un accord de confidentialité peut contribuer à faire reconnaître que l'information bénéficie de la protection légale du secret des affaires et constituer une mesure de protection raisonnable pour conserver le caractère secret des informations (art. L. 151-1 et art. L. 151-5 du Code de commerce).

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

Toutes les informations mentionnées dans le chapitre II peuvent faire l'objet d'un accord de confidentialité.

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 des personnes habilitées à recevoir l'information.

13. Article 1112-2 du Code civil en vertu duquel « 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 ».

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

La durée de l'accord de confidentialité peut couvrir :

- la période de négociation ;
- la durée du contrat commercial, auxquelles peut s'ajouter une durée supplémentaire convenue entre les parties.

Auxquelles peut s'ajouter une durée supplémentaire convenue entre les parties.

Il est par ailleurs judicieux de prévoir ce qu'il advient des informations confidentielles à la fin de l'accord (destruction, restitution sur demande…).

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 du codéveloppement d'un produit ou de la réalisation d'un système **> l'accord devrait être réciproque**. À défaut, en cas de litige, on ne peut exclure qu'un juge estime qu'il y a un « *déséquilibre significatif dans les droits et obligations des parties* » ou, au moins, un indice d'un tel déséquilibre[14].

14. L'article L442-6, I, 2° 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 ».

VII. 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[15].

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 que, 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)[16]. 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.

a. 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.

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.

15. Articls L611-1 et suivants du Code de la propriété intellectuelle.
16. Ou dans un organisme étranger.

ATTENTION !

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

b. 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** : **désigne des informations non communiquées.** Certains textes protègent le secret. C'est le cas de la directive « secret d'affaires », transposée en France par la loi du 30 juillet 2018 (voir chapitre III « Que vise la protection du secret des affaires ? »). C'est le cas également de l'article 39 de l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC) annexé au traité de Marrakech ayant institué l'Organisation mondiale du commerce (OMC), qui 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** : **désigne 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 (cf. chapitre VI « Protéger les informations par un accord de confidentialité »).

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 - NDA)* utilisent parfois le terme de « Secret » (Secrecy).

c. 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[17] prévue par le titulaire de ces informations à l'article L. 611-8 du Code de la propriété intellectuelle.

17. 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 à obtenir son transfert.

2. Le savoir-faire est-il protégé ?

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

- *secret, c'est-à-dire qu'il n'est pas généralement connu ou facilement accessible* ;
- *substantiel, c'est-à-dire important et utile pour la production des produits contractuels* ;
- *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*[18] ».

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

- de licences de brevet et de savoir-faire, car le brevet suffit rarement à mettre en œuvre la production ;
- de licences de savoir-faire indépendantes de tout brevet.

La licence de savoir-faire consiste à communiquer des informations, conseils, documentations et formations.

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.

Le savoir-faire peut bénéficier de la protection du secret des affaires dans les conditions décrites dessus (cf. chapitre III « Que vise la protection du secret des affaires ? »).

Un savoir-faire spécifique peut être développé par l'entreprise à l'occasion d'un marché ou d'un appel d'offres. Le « Guide pour la qualité des relations clients-fournisseurs » du Médiateur des relations interentreprises avec la direction des Affaires juridiques du ministère de l'Économie, l'INPI et la DGCIS indique : « *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* ».

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 les chapitres I et II) ;
- 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 le chapitre IV) 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.

18. 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 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.

VIII. 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[19] protège en effet toute « œuvre de l'esprit » quelqu'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[20].

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).

1. 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[21].
- Les structures des bases de données[22].

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.

2. Comment prouver la date de la détention des informations ?

Il est conseillé de se ménager la préuve de la date de la détention de ses droits d'auteur en ayant recours par exemple aux dépôts privés (cf. chapitre II « Que faire face à une information sensible ? »).

19. Article L111-1 et suivants du Code la propriété intellectuelle.
20. 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, 1re 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.
21. L'article L112-2 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, relatifs au fonctionnement d'un ensemble de traitement de données.
22. Articles L112-3 et L341-1 et suivants du Code de la propriété intellectuelle.

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

Dans le cadre de la commande publique, la confidentialité fait l'objet de textes spécifiques.

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 : L. 2132-1, L. 2332-1, L. 3122-3, R. 2131-3 et R. 2132-5 du nouveau Code de la commande publique. 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, marché passé selon une procédure adaptée (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 (entreprises de réseaux…) ;
- 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 ;
- 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[23] :

- violerait le secret en matière industrielle et commerciale ou le secret des affaires ;
- 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.

23. 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.

ATTENTION !

Cette obligation de confidentialité demeure quand bien même les candidatures auraient été déclarées irrecevables au sens de l'article R. 2144-7 du décret du 3 décembre 2018 ou quand bien même les offres auraient été déclarées inappropriées au sens de l'article L. 2152-4 de l'ordonnance du 26 novembre 2018 et de l'article R. 2152-1 du décret du 3 décembre 2018. L'acheteur ne doit pas utiliser les éléments confidentiels contenus dans les offres remises par les candidats.

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'informations, 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 contournements :

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 préétudes 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 préétude, 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.

Le prix du marché est-il communicable ? L'acheteur a obligation de communiquer aux personnes qui en font la demande des informations telles que le nom de l'attributaire et le prix du marché. Toutefois, les borderaux de détail de prix ne sont pas communicables.

Conseil d'État, arrêt n° 375529 du 30 mars 2016 : « *au regard des règles de la commande publique, doivent ainsi être regardés comme communicables, sous réserve des secrets protégés par la loi, l'ensemble des pièces du marché ; que dans cette mesure, si notamment l'acte d'engagement, le prix global de l'offre et les prestations proposées par l'entreprise attributaire sont en principe communicables, le bordereau unitaire de prix de l'entreprise attributaire, en ce qu'il reflète la stratégie commerciale de l'entreprise opérant dans un secteur d'activité et qu'il est susceptible, ainsi, de porter atteinte au secret commercial, n'est quant à lui, en principe, pas communicable […]* ».

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 R. 2152-1 du décret n° 2018-1075 du 3 décembre 2018 portant partie réglementaire du code de la commande publique ;*
- *en cours d'exécution du marché, **veiller au respect des dispositions des CCAG relatives à la confidentialité** (art. 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 cocontractant 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 toute hypothèse, l'exercice d'un **recours contentieux**[24] 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[25].*

24. Cf. chapitre IX.

25. 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 ».

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

Les entreprises chargées d'une mission de service public peuvent détenir des informations sensibles. Toutefois, la législation leur impose une obligation de communication à laquelle elles ne peuvent pas déroger, sauf exceptions parmi lesquelles figurent le secret des affaires.

1. 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**[26].

L'article L. 321-3 CRPA issu 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.

Exemple : 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 au format électronique doivent obligatoirement être publiés (art. L. 312-1-1 CRPA), c'est-à-dire mis en ligne, selon un échéancier d'application[27].

2. Exceptions

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

- **les documents non communicables** (art. 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 ;
- **les documents communicables seulement à l'intéressé** (personne concernée par l'information – art. L. 311-6 CRPA) : notamment ceux dont la communication porterait atteinte au secret des affaires[28] « *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*[29] ».

26. Article L311-1 CRPA.
27. Article 8 de la loi Lemaire.
28. Dénommé « secret en matière commerciale ou industrielle » avant l'adoption sur le secret des affaires.
29. Les documents couverts par le secret en matière commerciale et industrielle (site de la Cada).

ATTENTION !

En cas de doute, il convient de contacter l'administration qui détient le document et, en l'absence de réponse, de saisir la Cada.

Si l'information non communicable peut être séparée ou occultée dans le document, celui-ci est communicable sous cette condition (art. 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 (cf. Chapitre VI).

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[30].

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 cas d'exception, notamment s'ils contiennent un secret des affaires.

30. 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.

XI. 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.

1. La violation du secret des affaires

Sont interdites l'obtention, l'utilisation ou la divulgation illicite d'un secret des affaires (cf. chapitre III).

Le titre V du livre 1er du Code de commerce contient un chapitre intitulé « Des actions en prévention, en cessation ou en réparation d›une atteinte au secret des affaires », article L. 151-1 et suivants de ce Code.

En cas d'atteinte à un secret des affaires, la victime pourra intenter une **action en responsabilité civile.**

Les sanctions et mesures judicaires sont calquées sur celles applicables en matière de contrefaçon (issues de la directive européenne « propriété Intellectuelle »[31]).

Deux séries de mesures judiciaires sont prévues par la loi :

a. Prévenir et faire cesser les atteintes au secret

La victime peut demander au tribunal d'interdire l'utilisation ou la divulgation du secret ainsi que la production, la vente, la mise sur le marché et le stockage de produits fabriqués à l'aide d'un secret des affaires. Le tribunal peut également interdire l'utilisation d'un produit ou fichier et ordonner le rappel, la destruction du produit ou du fichier numérique concernés.

L'auteur de la divulgation ou de l'utilisation peut demander à échapper à ces mesures s'il est de bonne foi et que de telles mesures lui causeraient un dommage disproportionné, mais le tribunal fixe alors une indemnité à verser au détenteur légitime, au moins égale aux redevances qu'il aurait dû lui payer s'il avait eu une licence.

Le décret n° 2018-1126 du 11 décembre 2018 précise les mesures provisoires ou conservatoires pouvant être ordonnées (art. R. 152.1 et suivants du Code de commerce).

b. Obtenir des dommages et intérêts

L'auteur de la violation pourra être condamné à verser des dommages et intérêts en réparation du préjudice subi. Le tribunal doit prendre en compte :

- les conséquences économiques (manque à gagner, perte d'une chance) ;
- le préjudice moral ;les bénéfices réalisés par le responsable de l'atteinte, y compris les économies d'investissements intellectuels, matériels et promotionnels.

Le tribunal peut préférer une somme forfaitaire tenant compte notamment des droits qui auraient été dus si l'auteur avait obtenu une autorisation (licence) d'utiliser le secret.

Le tribunal peut ordonner la publication du jugement (art. L. 152-6 et L. 152-7).

31. V. directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004 relative au respect des droits de propriété intellectuelle.

À NOTER

L'article L. 153-2 du Code de commerce prévoit **une protection du caractère confidentiel des secrets des affaires dans le cadre d'une procédure judiciaire** qui met en cause un secret des affaires et qui est applicable à toutes les parties prenantes à la procédure, dans les conditions ci-après.

Le juge peut déterminer des pièces qu'il considère comme couvertes par le secret des affaires (ou susceptible de l'être, dans leur existence ou leur contenu). Toute personne qui y a accès (y compris les dirigeants légaux et représentants des entreprises) est tenue à une obligation lui interdisant toute utilisation ou divulgation de son contenu. Les avocats ne sont pas en principe tenus à cette confidentialité.

L'obligation de confidentialité perdure après la fin de la procédure, à moins que la juridiction ait décidé qu'il n'existe pas de secret des affaires ou si les informations ont entre-temps cessé de constituer un secret des affaires ou sont devenues aisément accessibles, et que cette décision ne peut plus faire l'objet d'un recours.

*Les **modes alternatifs de résolution des litiges**, comme la médiation ou l'arbitrage[32], présentent un intérêt certain dans la mesure où les tiers n'y ont pas accès, assurant ainsi une meilleure confidentialité aux parties.*

2. La révélation du secret de fabrique par le salarié

Le cas spécifique du secret de fabrique[33] 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[34].

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 euros d'amende.

À NOTER

- Seule la révélation 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.

Le manquement d'un salarié peut être sanctionné dans le cadre d'une action en responsabilité civile pour violation du secret des affaires.

32. 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.

33. Article L621-1 du Code de la propriété intellectuelle et article L1227-1 du Code du travail.

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

3. 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 lancé une alerte dans le respect des conditions fixées par la loi (art. L. 1132-3-3 du Code du travail modifié). Cette protection est également prévue à l'article **151-8, 2°** du Code de commerce en vertu duquel la protection du secret des affaires ne s'étend pas aux cas où son obtention, son utilisation ou sa divulgation ont pour but de protéger l'intérêt général dans la mesure où elle permet de révéler – de bonne foi – une activité illégale, une faute ou un comportement répréhensible.

4. La responsabilité contractuelle/délictuelle/concurrence déloyale

Lorsque les conditions ne sont pas remplies pour intenter une action sur le fondement de la violation du secret des affaires (voir point 1), la victime peut envisager d'agir sur le terrain de la responsabilité civile de droit commun.

Le Code civil[35] 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 le chapitre VI, l'article 1112-2 du Code civil, applicable depuis le 1er octobre 2016, dispose 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 leur responsabilité civile. Il est recommandé de prévoir un accord de confidentialité, qui confortera l'engagement.

Dans le cas où 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. Il sera possible de demander l'application de la pénalité mentionnée dans l'accord ou à défaut demander la réparation du préjudice.

L'action en concurrence déloyale permet de sanctionner certains comportements contraires au devoir de loyauté. Cette action est possible lorsque 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).

Pour pouvoir mettre en œuvre la responsabilité civile, trois conditions doivent être remplies : une faute, un préjudice et un lien de causalité entre les deux.

35. 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.

5. L'abus de confiance

La divulgation d'une information sensible peut être, sous certaines conditions, sanctionnée sur le fondement de l'abus de confiance (art. 314-1 et suivants du Code pénal). Ce délit 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 60000 euros 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 euros d'amende* ».

Le champ d'application 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 d'exercer une action pour 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).

36. Voir par exemple, TGI Clermont-Ferrand, ch. corr. 21 juin 2010 ; TGI Versailles, ch. corr. 18 décembre 2007. Voir aussi : Cour de cassation, chambre criminelle, 22 mars 2017, n° 15-85929 : « les employés d'une société commerciale, dépositaires des informations sur les clients de celle-ci, peuvent être poursuivis pour abus de confiance s'ils utilisent ces informations à leur profit personnel ou pour une structure qu'ils ont créée pour détourner cette clientèle ».
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).
38. Voir également le chapitre VII
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 » **www.economie.gouv.fr/daj/recours-contentieux**.

Références et bibliographie

Articles et ouvrages

- Eric Chevrier (dir.), livre blanc « Secret des affaires », Dalloz, 2018, 39 p.
- 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.
- Jean Lapouterle (dir.), « La protection des secrets d'affaires : perspectives nationales et européennes », LexisNexis, 2017, 170 p.
- 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.
- Renaud Salomon, premier vice-président adjoint au TGI de Paris, « Le secret des affaires », Dossier, La Semaine juridique entreprise et affaires n° 35, 1er septembre 2016, page 1454.

Sites Internet et divers

Agence pour la protection des programmes (APP)
www.app.asso.fr

Commission d'accès aux documents administratifs (Cada)
www.cada.fr

« Guide de la sécurité des données personnelles », (Cnil)
www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf

« RGPD : passer à l'action », (Cnil)
www.cnil.fr/fr/rgpd-passer-a-laction

Direction des Affaires juridiques (DJA) du ministère de l'Economie
www.economie.gouv.fr/daj/recours-contentieux

Institut national de la propriété intellectuelle (Inpi), Enveloppe Soleau
www.inpi.fr/fr/proteger-vos-creations/lenveloppe-soleau/enveloppe-soleau

Lepage, A. et al., « Le droit de savoir », rapport 2010 de la Cour de cassation
www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2010_3866/

« Guide pratique sur la protection des données personnelles » (MEDEF)
www.medef.com/fr/content/guide-pratique-sur-la-protection-des-donnees-personnelles

« Valorisation, transfert de technologie et innovation issue de la recherche publique », Réseau C.U.R.I.E., Cahiers de laboratoire
www.curie.asso.fr/IMG/pdf/rapport_2018.pdf

Société des ingénieurs et scientifiques de France (IESF)
www.iesf.fr/

Société civile des auteurs multimédia (Scam)
www.scam.fr/

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
Fédération des industries mécaniques - (FIM)

Faustine Burnichon, chargée d'études juridiques
Union des transports publics et ferroviaires - (UTP)

Tiphaine Fritz, juriste, direction des Affaires juridiques
Fédération nationale des travaux publics - (FNTP)

Rafael Mejia, chargé de mission, direction Droit de l'entreprise du MEDEF
Rapporteur du groupe de travail

Françoise Vergriète-Matringes, présidente de la commission Commande publique
Alliance française des industries du numérique (Afnum)

Dépôt légal : 3e édition, mars 2019 - Tous droits réservés - N° ISBN : 978-2-86658-192-3 (version numérique).

MEDEF
55, avenue Bosquet
75007 Paris
Tél. : 01.53.59.19.19
www.medef.com