

SECRET DES AFFAIRES

Comment bénéficier
de la protection prévue
par la loi du 30 juillet 2018 ?



GUIDE PRATIQUE À L'USAGE DES TPE / PME / ETI



“

Sans le secret des affaires, c'en serait fini de l'industrie, des services, de l'économie

ROGER-POL DROIT

(Dangereuse transparence, Les Échos, 2011)

Les ingrédients entrant dans la composition de la liqueur Chartreuse et les secrets de sa fabrication constituent le véritable capital des Pères Chartreux.

De même, les recettes ou les détails de toutes les étapes de production du Coca-Cola ou du Nutella ont permis à leur titulaire, parce qu'ils sont conservés secrets, de préserver leur modèle économique.

En collaboration avec Maître Olivier de Maison Rouge, Avocat, et en partenariat avec l'Association française des juristes d'entreprise et la Fédération des industries mécaniques, la Chambre de commerce et d'industrie Paris Ile-de-France propose aux entreprises de bonnes pratiques pour pouvoir bénéficier de la protection du secret des affaires, telle que définie par la loi du 30 juillet 2018.

POURQUOI CE GUIDE PRATIQUE ?

DIDIER KLING

Président de la CCI Paris Ile-de-France

Pour préserver l'innovation et les informations stratégiques des entreprises dans une économie mondialisée et ultra connectée, le législateur européen a adopté, le 8 juin 2016, une directive sur la protection des savoir-faire et des informations commerciales non divulgués (secret des affaires) contre l'obtention, l'utilisation et la divulgation illicites. La [loi n° 2018-670 du 30 juillet 2018](#) vient de transposer en droit français ce texte, offrant aux entreprises un nouvel outil juridique.

Le secret a déjà une place dans l'environnement juridique français : secret défense, secret bancaire, secret familial, secret médical, secret administratif, secret de la correspondance ou secret de l'instruction. Désormais, les secrets des affaires seront reconnus par la loi comme étant des composants essentiels du capital immatériel des entreprises et pourront, à ce titre, bénéficier d'un cadre protecteur spécifique. C'est aujourd'hui une réalité, nos entreprises sont vulnérables : elles sont pillées, notre droit n'étant pas suffisamment efficient.

La loi qui vient d'être adoptée répond à un enjeu de compétitivité internationale, face à des concurrents qui, sur ce terrain de l'intelligence économique, sont bien mieux armés que nous. En ce sens, elle constitue un progrès considérable, gage d'une meilleure sécurité juridique.

Certes, la réglementation du secret des affaires se construit dans un environnement de tension, comme en ont témoigné les débats autour de l'adoption de la directive européenne de 2016, ainsi que ceux suscités par toutes les propositions de loi françaises infructueuses déposées depuis 2011. Il faut toutefois se garder de stigmatiser la protection du secret des affaires, qui n'est pas là pour opacifier les activités des entreprises, mais qui permet le renforcement de leur compétitivité. Le secret suppose l'éthique et on ne peut s'en prévaloir que si l'on est vertueux.

En aucun cas la protection du secret des affaires ne saurait entraver le droit du travail, le droit de la presse ou les libertés fondamentales, et notamment la liberté d'expression des lanceurs d'alerte. C'est bien d'ailleurs à la recherche d'un tel équilibre que le texte s'est construit.

Seules les entreprises ayant mis en place, selon les termes de la loi, des « mesures de protection raisonnables » pour garder leurs informations secrètes pourront efficacement faire valoir leurs droits devant les autorités judiciaires. Les ressources et les moyens consacrés à cette protection étant de leur seul ressort, sans davantage de précision dans le texte législatif, il apparaît nécessaire, pour permettre aux TPE/PME/ETI de mettre en œuvre ce nouveau dispositif, de les orienter vers des outils pertinents et des bonnes pratiques.

Une protection efficace du secret des affaires suppose en effet l'appropriation d'une chaîne de valeur composée de trois étapes-clés :

- L'identification des informations confidentielles
- leur classification
- l'organisation de leur protection

Les entreprises doivent prendre conscience de l'importance de cette dynamique. En cas de procès pour atteinte à un secret des affaires, les magistrats vérifieront si ce cadre protecteur est efficace. Si tel n'est pas le cas, l'action judiciaire ne sera pas couronnée de succès.

En d'autres termes, le texte suppose que les entreprises prennent en main leur protection. Et il serait faux d'y voir uniquement de nouvelles contraintes pour celles-ci. Bien au contraire, c'est pour elles l'opportunité de rendre leurs informations stratégiques éligibles à la protection du secret des affaires.

Il serait également faux de croire que seules les grandes entreprises sont concernées. En tout état de cause, elles ont davantage de moyens pour prendre les mesures nécessaires à la sécurisation de leurs données stratégiques. L'enjeu est donc, ici, d'offrir aux TPE/PME/ETI le même niveau d'information et de protection.

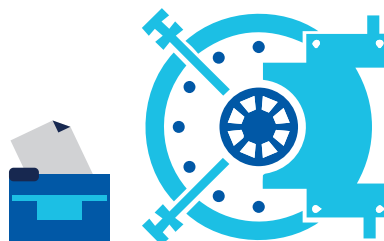
C'est le défi que nous souhaitons relever, en collaboration avec Maître Olivier de Maison Rouge, avec l'appui de l'Association française des juristes d'entreprise (AFJE) et la Fédération des industries mécaniques (FIM), au travers de ce guide qui se veut résolument pragmatique et qui contient un premier outil d'autodiagnostic.



1 POURQUOI PROTEGER UN SECRET DES AFFAIRES ?	6
➤ Pour répondre aux menaces pesant sur les entreprises.....	6
➤ En respectant l'équilibre entre intérêt privé et intérêt public.....	7
2 QU'EST-CE QU'UN SECRET DES AFFAIRES ?	8
➤ De quoi parle-t-on ?.....	8
➤ En quoi le secret des affaires se distingue-t-il de la propriété intellectuelle ?.....	10
3 COMMENT SECURISER LE SECRET DES AFFAIRES DANS L'ENTREPRISE ?	12
➤ Étape 1 : identifier les informations et les ressources de l'entreprise.....	13
➤ Étape 2 : classer les données.....	14
➤ Étape 3 : mettre en place des outils pour sécuriser le secret des affaires.....	14
➤ Étape 4 : nommer un référent dans l'entreprise en charge de la question du secret des affaires.....	18
4 QUE FAIRE EN CAS D'ATTEINTE AU SECRET DES AFFAIRES ?	19
➤ Quand y a-t-il atteinte au secret des affaires ?.....	19
➤ Que faire en cas de contentieux ?.....	20
ANNEXE I	22
Autodiagnostic.....	22
ANNEXE II	24
Tableau comparatif des caractéristiques des droits de propriété intellectuelle et du secret des affaires.....	24
ANNEXE III	25
Glossaire.....	25
REMERCIEMENTS	27



Ce guide sera illustré par l'éclairage d'un entrepreneur, M. Motus, fondateur d'une société dont il ne souhaite pas dévoiler le nom, car elle relève d'un secteur très sensible.



1 POURQUOI PROTÉGER UN SECRET DES AFFAIRES ?

► Pour répondre aux menaces pesant sur les entreprises...

Toutes les entreprises, et notamment les plus innovantes, sont de plus en plus exposées à des actes de prédation, qui trouvent leur origine à l'intérieur ou en dehors de l'Union européenne. Parmi les principales menaces :

- la fuite d'informations sensibles
- l'espionnage industriel
- la cybercriminalité

Les évolutions récentes, telles que la mondialisation, le recours croissant à la sous-traitance, l'allongement des chaînes de distribution et l'usage accru des technologies de l'information et de la communication, contribuent à la hausse des risques liés à ces procédés.

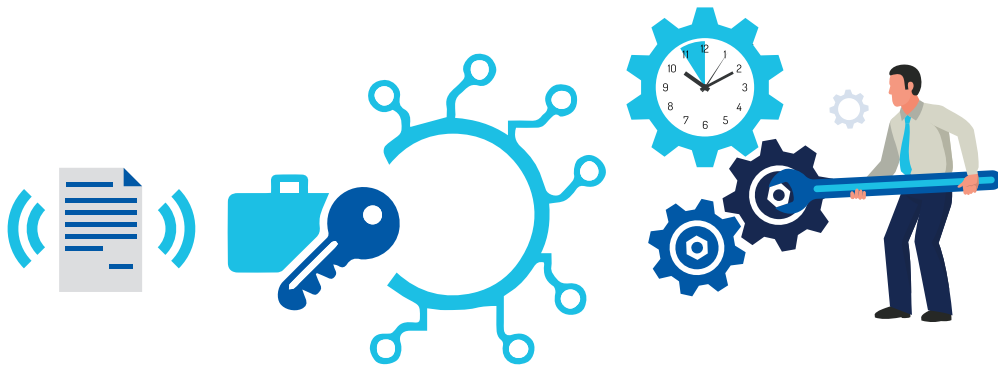
Dans le cadre de la transition numérique, le phénomène a pris une ampleur considérable au point que, dans certains cas, l'information étant détachable de son support, le tiers n'a pas forcément conscience de frauder.

Jusqu'à la loi de 2018, aucun texte spécifique n'était dédié à la protection du secret des affaires.

Aujourd'hui, les entreprises françaises :

- tendent à être à armes égales avec la plupart de leurs concurrents étrangers, notamment américains et chinois, qui ont déjà réglementé le secret des affaires
- peuvent protéger l'innovation en conservant leur avance concurrentielle

La protection du secret des affaires est inhérente à une société plus ouverte. Sa consécration correspond à un véritable changement de culture.



➤ ... en respectant l'équilibre entre intérêt privé et intérêt public

L'enjeu de la loi française est de préserver un équilibre entre les intérêts privés des entreprises pour la défense de leur patrimoine immatériel et l'exercice de libertés fondamentales dont bénéficie chaque citoyen.

Dans cet esprit, le secret des affaires n'est pas protégé lorsque :

- le droit de l'Union européenne ou le droit national en exige la production, notamment à des fins **d'enquête, de contrôle, d'autorisation ou de sanctions des autorités judiciaires ou administratives**
- des **journalistes** d'investigation publient un article de presse le divulguant (liberté d'expression et de communication, en particulier liberté de la presse ; liberté d'information)
- un **lanceur d'alerte** révèle de bonne foi et dans le but de protéger l'intérêt général, une activité illégale, une faute ou un comportement répréhensible
- il s'agit d'empêcher ou de faire cesser toutes menaces ou atteintes à **un intérêt légitime reconnu** par le droit de l'Union européenne ou le droit national (par exemple à la sécurité publique)
- il a été obtenu dans le cadre de l'exercice du **droit à l'information** et à la **consultation des salariés ou de leurs représentants**
- les **salariés** le communiquent à leurs représentants dans le cadre de l'exercice légitime par ces derniers de leur fonction, pour autant que cette divulgation ait été nécessaire à cet exercice

2 QU'EST-CE QU'UN SECRET DES AFFAIRES ?

› De quoi parle-t-on ?

Un secret des affaires suppose l'existence d'une information protégée entre les mains d'un détenteur légitime.

La notion d'information protégée

Le secret des affaires est défini par la [loi du 30 juillet 2018](#) comme toute information qui :

- 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

&

- revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret

&

- 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

Autrement dit, constitue un secret des affaires :

- tout ce qui n'est pas connu du secteur professionnel ou du domaine d'activité concerné
- qui est valorisable compte tenu du fait que cette information est secrète
- et que l'entreprise s'efforce de garder secret en prenant des mesures de protection raisonnables



« Selon une enquête menée en mai 2018 auprès de 412 entreprises par le CROCIS, Centre Régional d'Observation du Commerce, de l'Industrie et des Services de la CCI Paris Ile-de-France, 57% des répondants estiment ne pas détenir d'informations stratégiques. Le champ du secret des affaires est donc sous-estimé par les entreprises ».

“

Le secret des affaires est de savoir quelque chose que personne d'autre ne sait

ARISTOTE ONASSIS

Ce qui peut relever du secret des affaires :

- la R&D
- la stratégie commerciale
- les projets d'acquisition d'entreprise
- le lancement d'un nouveau produit
- les fichiers clients ou fournisseurs
- les données commerciales stratégiques
- les méthodes de prospection commerciale
- les volumes de production
- les taux de marge
- les recettes
- les procédés originaux
- les informations couvertes par des accords de confidentialité ou de non-concurrence
- les formules mathématiques (algorithmes)
- les avis du conseil d'administration ou de la direction
- un organigramme...

et, plus largement, les savoir-faire et informations commerciales non divulgués, lesquels constituent des actifs immatériels et confèrent à leur titulaire un avantage concurrentiel.



« Attention, toute information entrant dans cette catégorie ne bénéficiera de la protection que si elle fait l'objet de mesures de protection raisonnables. Pour aller plus loin, je vous conseille de vous reporter à la partie 3 de ce guide ».



« Prenons l'exemple des études géologiques qui constituent, pour un producteur d'énergie fossile, des informations essentielles, déterminantes. En fonction du coût d'extraction et/ou des autorisations nécessaires, ces informations secrètes peuvent avoir une forte valeur et être destinées à être conservées sur un temps long ».

Attention, certains secrets sont déjà réglementés et la nouvelle loi s'insère dans cet environnement juridique. Il en va ainsi :

- du secret d'Etat
- du secret de l'instruction
- du secret défense
- du secret professionnel (notamment pour les médecins, commissaires aux comptes, avocats, banquiers...)
- du secret administratif...



« Bien entendu, la protection du secret des affaires ne doit pas permettre de dissimuler des opérations ou pratiques illicites telles que :

- des malversations économiques ou financières
- des plans concertés de destruction de l'outil industriel ou de délocalisation massive
- des délits d'initiés
- des actes de corruption
- des actions de blanchiment d'argent, de fraudes fiscales
- des ententes commerciales prohibées... »

Le détenteur légitime du secret des affaires

Est détenteur légitime d'un secret des affaires celui qui l'a obtenu par l'un des moyens suivants :

- 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. C'est ce qu'on appelle "l'ingénierie inverse" ou "le reverse engineering"

► En quoi le secret des affaires se distingue-t-il de la propriété intellectuelle ?

Le secret des affaires peut recouvrir des hypothèses qui sont hors du champ de la propriété intellectuelle. Mais il peut y avoir aussi un lien, en ce sens que le droit reconnu au détenteur du secret des affaires peut en constituer :

Soit un complément

En pratique, les droits de propriété intellectuelle et le secret des affaires sont naturellement amenés à se rencontrer.

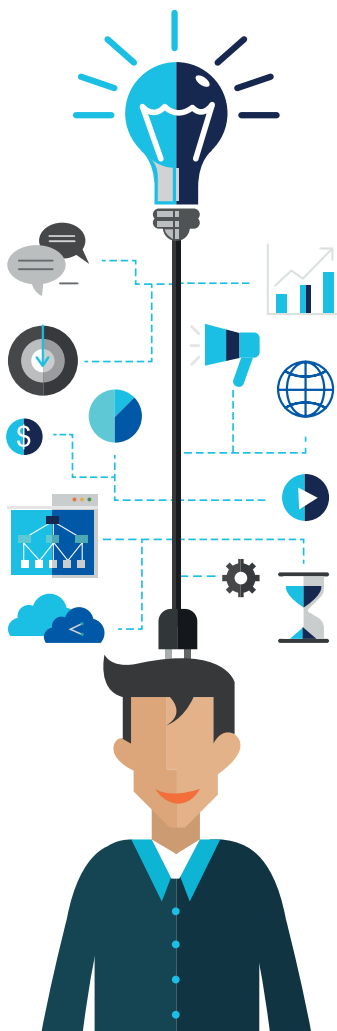
Le secret des affaires est parfois, chronologiquement, la première protection d'une innovation :

- une entreprise ne dévoile pas la maquette de la plaquette de communication sur laquelle elle travaille (futur objet du droit d'auteur)
- un constructeur automobile ne diffuse pas les premiers croquis d'un nouveau modèle de véhicule (futur dessin ou modèle)
- une entreprise ne révèle pas les premiers résultats de ses expériences technologiques (futur brevet d'invention)...
- ... ou les informations relatives au lancement d'un nouveau produit (future marque de commerce)

Le secret est parfois concomitant à la protection d'un brevet. Il peut soit englober des éléments qui ne figurent pas dans ce dernier afin de ne pas les dévoiler à la concurrence, soit des éléments qui ne sont pas brevetables.



« Même les droits de propriété intellectuelle ont besoin du secret des affaires. Si le brevet est la partie émergée de l'iceberg, il ne peut être utilisé pleinement qu'au travers d'un savoir-faire ».



Soit une alternative

Certes, le brevet confère à son titulaire un droit exclusif pour l'exploitation de l'invention et peut être valorisé par la concession de licences d'utilisation, mais le secret peut lui être préféré. C'est même la solution privilégiée par nombre d'entreprises, et notamment les PME, l'avantage principal étant que les conditions de protection du secret sont beaucoup plus souples que celles relatives aux droits de propriété industrielle : absence de procédures administratives, de taxes, de limites territoriales ; durée de protection (voir tableau en annexe II). Mais surtout, breveter impose de publier l'invention, qui va donc être connue de la concurrence.




« Le choix entre brevet et secret est éminemment stratégique. Chaque entreprise doit apprécier les avantages et les inconvénients des deux options, tout en prenant en considération les coûts financiers. Prenons l'exemple d'un grand laboratoire pharmaceutique qui garde secrète une formule de médicament constituant l'un de ses produits phares. Sans être très complexe, la breveter l'aurait inévitablement conduite à terme dans le domaine public et donc permis à ses concurrents de l'utiliser à leur profit ».

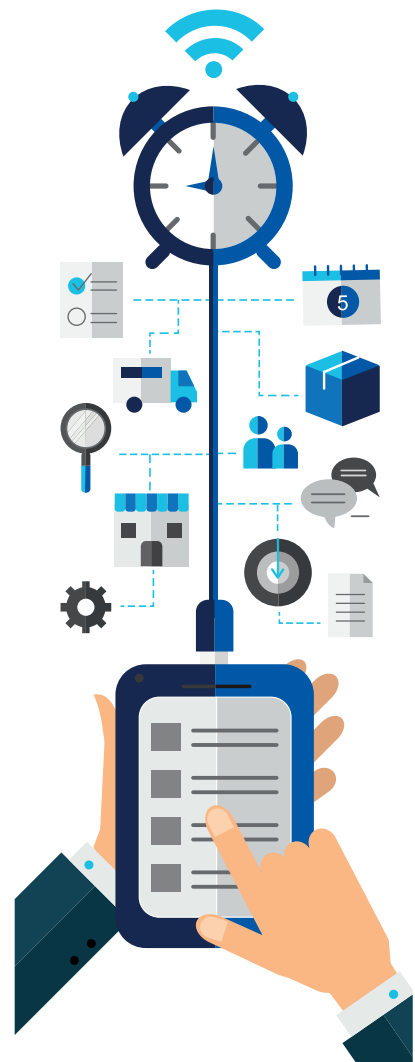
3 COMMENT SÉCURISER LE SECRET DES AFFAIRES DANS L'ENTREPRISE ?

La loi laisse aux entreprises une grande latitude pour définir les « mesures de protection raisonnables » les mieux adaptées à la protection de leurs secrets des affaires.

Il s'agit donc, à travers ce guide, de recenser les outils et les bonnes pratiques qui vont leur permettre de bénéficier de la loi. Elles pourront s'assurer, grâce à un autodiagnostic proposé en annexe, d'avoir pris les moyens nécessaires pour pouvoir revendiquer la protection prévue.



« Très vite, je me suis rendu compte qu'il est vital pour un entrepreneur qui exerce dans un secteur de pointe de savoir utiliser les outils existants pour sécuriser ses informations confidentielles. Reste à trouver un modèle d'organisation adapté aux particularités de chaque entreprise et des données à protéger ».



Un référentiel est proposé ici à titre de modèle, mais il n'est nullement contraignant. L'objectif est d'inciter les entreprises à déployer une politique de sécurité des informations, en respectant quatre étapes clés :

- L'identification des informations et des ressources de l'entreprise
- la classification des données
- la mise en place d'outils destinés à sécuriser le secret des affaires
- et la désignation d'un référent pour gérer le secret des affaires



➤ ETAPE 1

Identifier les informations et les ressources de l'entreprise

- Inventorier les informations sensibles de l'entreprise (orientations stratégiques, études et veille concurrentielle, fichiers clients et prospects, listes des fournisseurs, contrats, données comptables, dossiers du personnel, organigrammes, plans, procédés de fabrication, codes sources, algorithmes...)
- Identifier les personnes impliquées (dirigeants, administrateurs, responsables métiers, responsables sécurité, responsables juridiques, responsables ressources humaines, responsables intelligence économique, experts-comptables, documentalistes, salariés...)
- Recenser les systèmes et supports d'information de l'entreprise (ordinateurs fixes et portables, accès à internet, messagerie électronique, logiciels, clés USB, Wi-fi, téléphones fixes et portables, photocopieurs, armoires et locaux d'archivage...)
- Analyser le schéma de l'entreprise et son métier (notamment localiser les différents sites de l'entreprise, en identifiant les filiales et les lieux de production)
- Recenser les savoir-faire, la R&D, les connaissances techniques de l'entreprise
- Évaluer les potentiels concurrentiels et l'innovation performante, à travers une cartographie et une étude de l'environnement économique
- Cartographier les risques en examinant les vulnérabilités (par métier et à quel moment)



« Cette démarche est importante, car les entreprises se trouvent souvent dépourvues, face à cet enjeu essentiel qu'est la gestion de leur patrimoine informationnel, c'est-à-dire l'ensemble des informations dont elles disposent (par exemple les données clients et fournisseurs, les logiciels, le savoir-faire...) ».



« Il faut se concentrer sur ce qui vaut la peine d'être tenu secret ; toute information n'a pas vocation à être protégée. Le patrimoine informationnel n'existe que s'il est décrit, par exemple dans une base de données, un plan, un document descriptif, un cahier des charges ou encore dans un contrat (de licence, de sous-traitance, de coopération). En quelque sorte, le secret des affaires, est celui que je crée, mais aussi celui que je co-crée avec un partenaire ou celui qu'un tiers va me confier. Tracer l'information est donc essentiel : c'est repérer d'où elle vient et à quel moment elle a été créée. Or, trop nombreuses sont les entreprises qui minimisent l'importance de leurs informations par rapport aux risques de pillages encourus.

Attention, le secret des affaires est loin d'être l'apanage du seul responsable juridique. Chaque secteur de l'entreprise est susceptible de receler un secret des affaires ».

› ETAPE 2

Classer les données

- Il peut être utile de mentionner explicitement qu'une information est confidentielle. L'entreprise pourra affiner cette classification en hiérarchisant les informations. Elle leur attribuera, par exemple, un code reflétant le niveau de classification selon différents critères, à déterminer : public, sensible, critique, stratégique (par exemple C0, C1, C2, C3)
- Cela permet en outre de délimiter le rang des personnes ayant accès à ces informations

› ETAPE 3

Mettre en place des outils pour sécuriser le secret des affaires

L'entreprise a le libre choix des moyens à mettre en œuvre pour définir sa politique de sécurité des informations. Les guidelines qui suivent pourront l'orienter utilement.

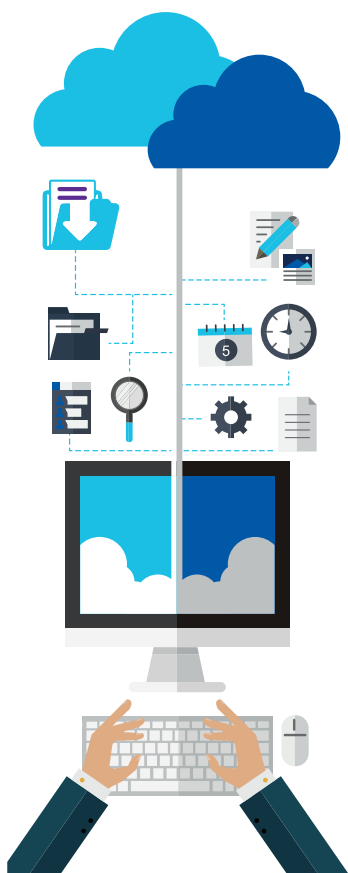
Mesures physiques ou techniques pour formaliser et dater les informations confidentielles

Prévoir un moyen de traçabilité et de conservation des preuves dans l'éventualité d'une action judiciaire (c'est-à-dire prouver qu'à une date certaine, l'entreprise détenait bien les informations) :

- Enveloppe Soleau, du nom de son inventeur Eugène Soleau. Concrètement, celle-ci se compose de deux compartiments dans lesquels le déposant glisse les copies identiques du descriptif des informations. L'un des compartiments, cacheté et daté, est archivé par l'Institut national de la propriété industrielle (INPI) pour une durée de cinq ans, renouvelable une fois. L'autre, également cacheté et daté, est renvoyé au déposant, qui doit le conserver sans l'ouvrir. Cette enveloppe peut être commandée en ligne auprès de l'INPI (<https://www.inpi.fr/fr/protéger-vos-creations/l'enveloppe-soleau/enveloppe-soleau>) ; le service de dépôt en ligne e-Soleau permet également de bénéficier d'un archivage sécurisé et certifié AFNOR (<https://www.inpi.fr/fr/services-et-prestations/e-soleau>)
- Dépôt privé auprès d'un officier ministériel (huissier ou notaire)
- Dépôt en ligne auprès d'un prestataire spécialisé



« Pour hiérarchiser, il convient de déterminer ce qui fait la valeur de l'entreprise sur le marché, c'est-à-dire son avantage compétitif. Mais cela suppose la réalisation d'un audit, bien entendu sécurisé par une clause ou un accord de confidentialité. Certes l'opération représente un coût, mais l'entreprise en tirera des avantages certains. »



- Envoi d'une lettre recommandée à soi-même
- Cahiers de laboratoire
- Horodatage électronique
- Archivage numérique
- Blockchain privée (système pour lequel les permissions d'accès, de lecture et de vérification du registre de la blockchain sont contrôlées de manière plus stricte que dans la blockchain publique, tout en conservant la plupart des avantages de la technologie comme la garantie d'authenticité, ou la décentralisation...)



« Les enveloppes Soleau doivent être gérées rigoureusement. Il est conseillé de les référencer afin de les lier à des dossiers.

De même, il est important de remplir correctement les cahiers de laboratoire, par exemple en veillant à ne pas laisser d'espace vide entre deux informations.

L'enquête du CROCIS précitée révèle que, parmi les entreprises qui sécurisent leurs informations, les voies privilégiées sont : l'obtention d'un titre de propriété industrielle (27 %), le marquage de documents (24 %) et le dépôt d'enveloppe Soleau (18 %). »

Sécuriser les systèmes d'information et d'intranet



« On peut crypter et a minima fermer les bureaux, cacher les écrans... Une entreprise, qui a de plus en plus d'informations à protéger, peut travailler avec un cloud interne, à condition de ne pas y incorporer une information hypersensible ».

Créer des leures identifiés et identifiables dans le support de l'information pour faciliter la preuve de la fraude



« L'idée astucieuse consiste à intégrer sciemment une erreur sans conséquence sur le produit attestant que même l'erreur a été reprise par celui qui a enfreint les droits du détenteur du secret des affaires ».

Mesures spécifiques aux salariés de l'entreprise

- Mettre en place une **gestion rigoureuse des accès aux systèmes informatiques** (habiliter les collaborateurs à accéder à des données définies en fonction de leur mission et de leur statut, prévoir une politique stricte en matière de mot de passe)
- Insérer dans les contrats de travail des **clauses de confidentialité**, et éventuellement une clause de non-concurrence
- Rédiger et diffuser une **charte éthique générale** et une **charte informatique**
- Rappeler la politique en matière de secret des affaires dans : un **accord collectif**, le **règlement intérieur**, une **note de service**, un **règlement de sécurité des informations**, un **livret de sécurité remis à chaque salarié entrant dans l'entreprise...**
- **Sensibiliser régulièrement les salariés** (réunions, formations...)

Mesures spécifiques aux partenaires de l'entreprise

Il est recommandé de sélectionner et de travailler avec des partenaires (sous-traitants, prestataires informatiques, cabinets d'études de marché, d'audit, d'assurance, transporteurs,...) dans un cadre contractuel.

Prévoir notamment :

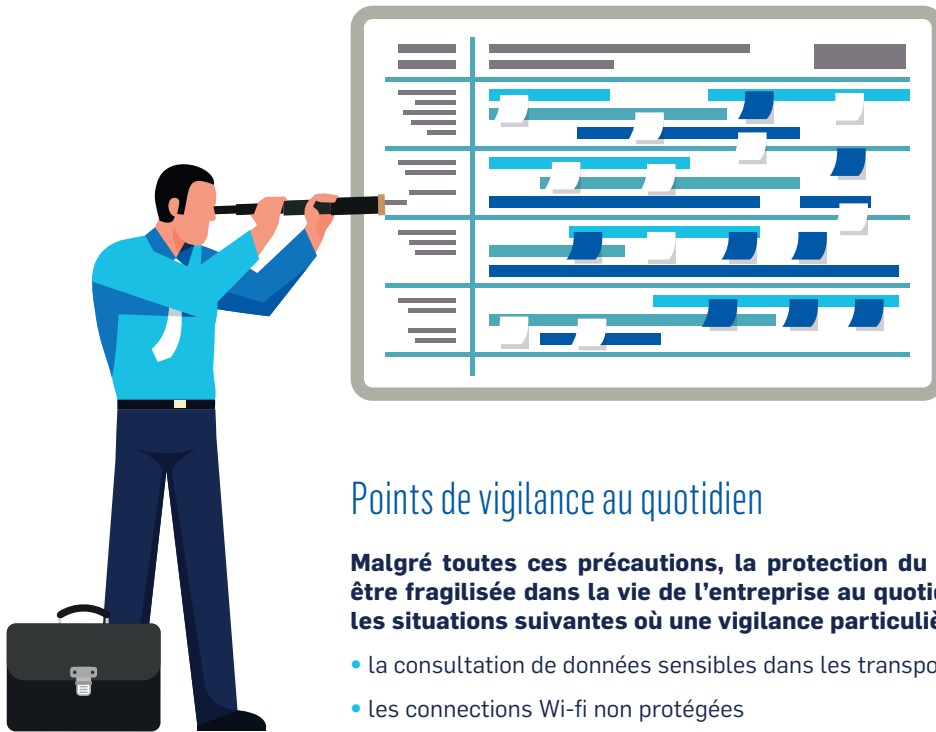
- Des **accords de confidentialité** (pour interdire la divulgation et l'usage non-autorisé d'informations confidentielles qui ont été communiquées à l'occasion d'une négociation ou d'un contrat)
- Du moins, des **clauses de confidentialité dans les contrats**
- Des **clauses de non-concurrence**
- Une **clause générale** dans le contrat de licence **imposant au licencié la mise en œuvre de moyens matériels de protection du secret** (une restriction d'accès, des salles sécurisées, la sensibilisation de son personnel, une procédure à appliquer en cas de départ d'un employé, la sécurité informatique...)
- Des **clauses d'audit, naturellement dans le respect de l'organisation interne du partenaire**



« Premièrement, il faut borner l'obligation de confidentialité, quant à son objet et sa temporalité : quelle information fait l'objet du contrat ? Jusqu'à quelle date ? Renouvelable ou non ?

Deuxièmement, il est important de déterminer, dans le préambule du contrat, la raison pour laquelle des informations confidentielles vont être divulguées.

Troisièmement, cette politique de sécurité doit être suivie dans le temps, en dépit des changements de personne, d'équipements ou d'organisation ».



Points de vigilance au quotidien

Malgré toutes ces précautions, la protection du secret des affaires peut être fragilisée dans la vie de l'entreprise au quotidien, et notamment dans les situations suivantes où une vigilance particulière est recommandée :

- la consultation de données sensibles dans les transports en commun
- Les connexions Wi-fi non protégées
- les réunions dans des espaces non-protégés
- les salons professionnels
- les visites d'entreprises
- les réponses à des marchés, y compris des marchés publics
- les stagiaires, intérimaires et autre personnel non permanent
- le personnel extérieur à l'entreprise



L'ÉCLAIRAGE
DE M. MOTUS

« Sur les marchés publics, il faut être tout particulièrement attentif au cahier des charges du donneur d'ordre, lequel peut dévoiler aux concurrents les spécificités technologiques constituant le savoir-faire d'un candidat.

Il faut aussi se méfier des prototypes entreposés dans des ateliers auxquels une entreprise de nettoyage (extérieure) a accès.

Enfin, des précautions doivent être prises vis-à-vis des actionnaires. En ce sens, il est conseillé de leur faire signer un accord de confidentialité pour protéger la recherche et développement.

Pour les entreprises sondées par le CROCIS (enquête précitée), les situations à risque sont les suivantes : départ d'un salarié pour la concurrence (53 %), utilisation des systèmes informatiques ou échanges électroniques (43 %) et échange d'informations avec des partenaires (40 %) ».

➤ ÉTAPE 4

Nommer un référent dans l'entreprise en charge de la gestion du secret des affaires

Force est de constater que la [loi du 30 juillet 2018](#) sur la protection du secret des affaires intervient après deux textes récents aux conséquences importantes pour les PME et les ETI : d'une part, la loi du 9 décembre 2016 relative à la lutte contre la corruption et à la modernisation de la vie économique et d'autre part, le règlement européen du 27 avril 2016 relatif à la protection des données personnelles (dit RGPD), applicable depuis le 25 mai 2018.

Dans ce contexte, le Data Protection Officer (DPO ou délégué à la protection des données) pourrait également être, pour les entreprises visées par ces textes, le référent de premier niveau dans le traitement des alertes prévu par la loi de 2016, ainsi que la personne en charge de la gestion d'une politique de sécurité des informations sensibles qui répondent à la définition du secret des affaires. Deux ou trois activités, selon la taille de l'entreprise, pour une même fonction.

➤ Autodiagnostic des mesures mises en place

Un autodiagnostic est proposé en Annexe I. Il permet à chaque entreprise de se situer et d'évaluer le chemin à parcourir pour progresser. Sa finalité est de déclencher une démarche d'amélioration continue.



« Le DPO en tant que responsable de la gouvernance des données semble le mieux placé pour dire qu'une information n'a pas été classée au bon niveau au moment du choix par l'entreprise du critère de hiérarchisation (public, sensible, critique, stratégique) ».



« Avec les différents éléments désormais en votre possession, une première phase consistera à vous livrer à ce bref exercice, qui va vous permettre d'identifier vos forces et vos faiblesses en la matière ».



4 QUE FAIRE EN CAS D'ATTEINTE AU SECRET DES AFFAIRES ?

➤ Quand y a-t-il atteinte au secret des affaires ?



« On distingue l'obtention, l'utilisation et la divulgation du secret des affaires. Mais, en pratique, ces actions peuvent soit se manifester individuellement, soit se succéder, avec une obtention directe auprès du détenteur légitime ou indirecte auprès d'une personne interposée.

- Exemple d'une obtention directe : dans le domaine de la recherche médicale, un cadre devenu responsable d'établissement démissionne quelques mois plus tard. En dépit des consignes strictes pour protéger les données de santé manipulées, ce salarié a préalablement téléchargé sur un support externe un volume conséquent de données personnelles à caractère scientifique.

- Autre exemple, mais pour une obtention indirecte cette fois : une entreprise du secteur numérique, dont le commercial vient de démissionner pour rejoindre une entreprise concurrente, constate une intrusion dans son serveur par le directeur des systèmes d'information de sa rivale, lequel s'est connecté à distance à partir du compte stagiaire de l'entreprise (identifiant et mot de passe). Cette connexion a permis d'exporter pendant une heure les données commerciales de l'entreprise (fichiers clients, données techniques).

- Dernier exemple, d'une obtention suivie d'une utilisation et d'une divulgation : un salarié en charge des systèmes d'information d'une industrie mécanique qui, arrivé en fin de contrat de travail, veut « se venger » de son employeur. Avant son départ, il modifie les codes d'accès à la programmation automatisée des logiciels de production, et télécharge préalablement un nombre conséquent de données techniques et commerciales de l'entreprise, sur un support externe qu'il a emporté avec lui. Par la suite, l'entreprise a vu un concurrent se présenter sur le même marché, lequel ne possédait pas auparavant ce savoir-faire. Elle n'a pu que constater la disparition de ses parts de marché en un temps restreint (dans l'intervalle de 18 mois) ».

L'obtention illicite du secret des affaires

• L'obtention d'un secret des affaires est illicite lorsqu'elle intervient sans le consentement de son détenteur légitime et qu'elle résulte :

- d'un accès non autorisé à tout document, objet, matériau, substance ou fichier numérique, ou d'appropriation ou de copie de ces éléments, qui contient ledit secret ou dont il peut être déduit
- de tout autre comportement considéré, compte tenu des circonstances, comme déloyal et contraire aux usages en matière commerciale

L'utilisation ou la divulgation illicite du secret des affaires

- **L'utilisation ou la divulgation d'un secret des affaires est illicite, lorsqu'elle est réalisée sans le consentement de son détenteur légitime, par une personne :**
 - qui a obtenu le secret de façon illicite
 - ou qui a agi en violation d'une obligation de ne pas divulguer le secret ou de limiter son utilisation
- **De même, s'agissant de tout produit résultant d'une atteinte significative au secret des affaires, la production, l'offre ou la mise sur le marché, l'importation, l'exportation ou le stockage sont considérés comme une utilisation illicite, lorsque la personne qui exerce ces activités savait, ou aurait dû savoir au regard des circonstances, que ce secret était utilisé de façon illicite**

L'obtention, l'utilisation ou la divulgation illicite du secret des affaires

L'atteinte peut aussi survenir dans le cadre d'une exploitation en chaîne d'un secret des affaires, lorsque ce secret a été obtenu directement ou indirectement d'une personne qui l'utilisait ou le divulguait elle-même de façon illicite.

► Que faire en cas de contentieux ?

Si, en dépit des précautions prises par l'entreprise, il est porté atteinte à un secret des affaires, des recours judiciaires lui sont ouverts.



« Le procès constitue l'instant crucial à double titre :
• d'une part, le juge va estimer si l'entreprise a mis en œuvre les mesures de protection raisonnables pour sécuriser ses informations stratégiques, rendant ainsi celles-ci éligibles à la protection du secret des affaires
• d'autre part, de son côté, le juge doit prendre les mesures nécessaires afin que le secret ne soit pas dévoilé davantage ».

La protection du secret des affaires devant les juridictions civiles ou commerciales

La procédure judiciaire peut être aménagée au moyen de mécanismes permettant d'assurer la préservation du secret des affaires. Il est prévu notamment que le juge puisse :

- Prendre seul connaissance de la pièce contenant un secret des affaires, limiter sa communication ou sa production à certains éléments, en ordonner la communication ou la production sous forme de résumé ou en restreindre l'accès à certaines personnes



« Il faut savoir que, fréquemment, un secret est invoqué au cours d'une procédure qui n'est pas intentée spécifiquement pour le défendre. Il peut s'agir, par exemple, d'une affaire de contrefaçon, de licenciement, d'atteinte à la concurrence ou au droit de la distribution... Certaines actions peuvent même être instrumentalisées pour accéder au secret des affaires d'un concurrent. Afin de pallier ce risque, la loi met en place un dispositif de protection très efficace en étendant la protection du secret des affaires à toutes les procédures judiciaires au cours desquelles un tel secret pourrait être produit ».

- Décider que les débats auront lieu et que la décision sera prononcée hors la présence du public
- Adapter la motivation de sa décision et les modalités de sa publication aux nécessités de la protection du secret des affaires

Par ailleurs, des obligations de confidentialité peuvent peser sur les personnes ayant accès au dossier.



« Un process similaire est prévu devant les juridictions administratives (par exemple pour les contentieux en matière de marchés publics). Il convient également de noter que l'Autorité de la concurrence a déjà mis en place un mécanisme de ce type, qui a fait ses preuves ».

Quelle réponse des juridictions à une atteinte au secret des affaires ?

Pour prévenir une atteinte imminente ou faire cesser une atteinte illicite à un secret des affaires, le juge peut ordonner des mesures d'urgence, à titre provisoire ou conservatoire.



« Dans certains secteurs, très exposés, il est essentiel qu'une entreprise puisse faire interdire, même provisoirement, la production ou la mise sur le marché de produits résultant de l'atteinte à son secret des affaires, ordonner la destruction totale ou partielle d'un objet ou d'un fichier numérique contenant ce secret, ou encore rappeler des circuits commerciaux les produits résultant de son atteinte... Les mesures provisoires permettent de régler momentanément une situation en attendant la décision définitive du juge. Les mesures conservatoires ont pour objectif la sauvegarde d'un droit ou d'une chose ».



« Aux côtés de la voie civile, il peut être envisagé de faire sanctionner par le droit pénal les atteintes au secret des affaires, au titre des vols de données, des vols de savoir-faire ou vols de secret de fabrication, des intrusions dans le système informatique, voire du débauchage de salariés ».

De surcroît :

- Le juge peut allouer des **dommages et intérêts** en réparation du préjudice effectivement subi
- Il peut ordonner toutes mesures de **publicité de sa décision**

Annexe I

AUTODIAGNOSTIC

► Savez-vous identifier les éléments sensibles de votre entreprise ?

- ◇ Orientations stratégiques
- ◇ Avis juridiques / recommandations juridiques
- ◇ Etudes et veille concurrentielle
- ◇ Fichiers clients et prospects
- ◇ Listes des fournisseurs
- ◇ Contrats
- ◇ Données comptables et financières
- ◇ Données commerciales
- ◇ Méthodes de protection commerciale
- ◇ Dossiers du personnel
- ◇ Organigrammes
- ◇ Plans
- ◇ Procédés de fabrication
- ◇ Codes source
- ◇ Algorithmes

► Comment la protection du secret des affaires est-elle prise en compte dans votre entreprise ?

- ◇ Vous avez mis en place des mesures de protection (cahiers de laboratoire, envoi d'une lettre recommandée à vous-même, dépôt chez un notaire ou huissier, dépôt auprès d'une société d'auteurs ou d'un organisme spécialisé, enveloppe Soleau, marquage des documents...)
- ◇ Avant de lancer un projet important vous traitez les aspects relatifs à la sécurité des informations
- ◇ Vos inventions sont protégées
- ◇ Il existe des consignes claires pour classer, archiver et détruire les informations sensibles
- ◇ Votre système d'information est sécurisé
- ◇ Vous insérez des clauses de confidentialité dans les contrats conclus avec vos partenaires

➤ Afin de formaliser le secret des affaires, quelles sont les 2 mesures qui vous semblent les plus efficaces ?

- ◇ Obtention d'un titre de propriété industrielle (brevets, dessins et modèles, marques)
- ◇ Cahiers de laboratoire
- ◇ Envoi d'une lettre recommandée à vous-même
- ◇ Dépôt chez un notaire ou huissier
- ◇ Dépôt auprès d'une société d'auteurs ou d'un organisme spécialisé
- ◇ Enveloppe Soleau
- ◇ Marquage des documents
- ◇ Horodatage électronique

➤ Votre entreprise vous semble-t-elle aujourd'hui à l'abri d'une atteinte au secret des affaires dans les hypothèses suivantes ?

- ◇ Colloque
- ◇ Salon professionnel
- ◇ Réponse à un appel d'offres
- ◇ Diffusion d'informations à des actionnaires
- ◇ Départ d'un salarié pour la concurrence
- ◇ Négociation commerciale
- ◇ Echanges d'informations avec des partenaires (fournisseurs, cotraitants...)
- ◇ Utilisation des systèmes informatiques et échanges électroniques
- ◇ Déplacement
- ◇ Divulgarion d'informations au cours d'un procès
- ◇ Diffusion d'informations à l'extérieur de l'entreprise

➤ Quels sont selon vous les 2 éléments d'un dispositif performant pour protéger de secret des affaires ?

- ◇ (In)formation régulière des collaborateurs
- ◇ Mise en place de règles internes spécifiques (règlement intérieur, charte...)
- ◇ Mesures de sécurité techniques ou physiques
- ◇ Clause de confidentialité ou de non-concurrence dans les contrats de travail
- ◇ Marquage des documents
- ◇ Accord ou clause de confidentialité avec les partenaires
- ◇ Clause de non-concurrence avec les partenaires
- ◇ Traçabilité des échanges

Résultats sur 35

Moins de 20 : votre entreprise est confrontée à un risque bien réel de divulgation du secret des affaires

De 20 à 30 : la protection de votre secret des affaires peut être accrue par la mise en place de solutions simples

Plus de 30 : vous avez le souci de protéger le patrimoine immatériel de votre entreprise

Annexe II

Tableau comparatif des caractéristiques des droits de propriété intellectuelle et du secret des affaires

	Secret des affaires	Brevet	Droit d'auteur	Dessin Modèle	Marque
Conditions de protection	Non accessibilité	Nouveauté Activité inventive Application industrielle	Création de forme Originalité	Nouveauté Caractère propre	Signe distinctif Signe disponible Signe licite
Exclusivité des droits	NON	OUI	OUI	OUI	OUI
Durée de protection	Tant que le secret n'est pas dévoilé	20 ans	70 ans à compter du décès de l'auteur	5 ans renouvelables 5 fois	10 ans renouvelables indéfiniment
Formalités obligatoires	Aucune	Dépôt auprès de l'INPI (publication)	Aucune	Dépôt auprès de l'INPI (publication)	Dépôt auprès de l'INPI (publication)
Coût	Pas de coûts spécifiques, mais mise en place, dans l'entreprise, d'une organisation adaptée	Payant	Gratuit	Payant	Payant
Étendue territoriale	Illimitée	Limitée	Quasi-illimitée (au sein des pays parties à la Convention de Berne)	Limitée	Limitée
Publicité	Aucune	Obligatoire (sauf inventions intéressant la Défense nationale)	Facultative (protection dès la création, même non divulguée)	Obligatoire	Obligatoire
Perte de la protection	D'office si perte du caractère confidentiel	Possible (via une action en justice) + Fin de la protection légale	Possible (via une action en justice) + Fin de la protection légale	Possible (via une action en justice) + Fin de la protection légale	Possible (via une action en justice) + Fin de la protection légale

Annexe III

Glossaire

› Blockchain

La blockchain est une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle (*définition de Blockchain France*). Il existe des blockchains publiques, ouvertes à tous, et des blockchains privées, dont l'accès et l'utilisation sont limités à un certain nombre d'acteurs.

› Cahier de laboratoire

Il s'agit d'un cahier dans lequel sont consignés au jour le jour les travaux des chercheurs, ingénieurs, techniciens, thésards, stagiaires... Chaque cahier possède un numéro unique. Y figurent le nom de l'utilisateur, le nom du propriétaire et un espace en bas de chaque page (numérotée) pour dater et signer.

› Clause de non concurrence

La clause de non-concurrence interdit au salarié, après la rupture de son contrat, d'exercer une activité qui porterait préjudice à son ancien employeur. Elle doit impérativement figurer dans le contrat de travail du salarié.

› Clause ou contrat de confidentialité

L'accord de confidentialité, également appelé accord de secret ou de non-divulgence (le sigle anglo-saxon NDA pour Non Disclosure Agreement est également utilisé) a pour objet d'interdire aux partenaires de révéler les informations confidentielles échangées au cours de leur négociation. Il peut également prendre la forme d'une clause de confidentialité.

› Cybercriminalité

La cybercriminalité est le terme employé pour désigner l'ensemble des infractions pénales qui sont commises via les réseaux informatiques, notamment sur le réseau Internet.

› Enveloppe Soleau

Du nom de son créateur, il s'agit d'une enveloppe à double compartiment, chacun d'eux recevant un exemplaire d'une création, d'une innovation ou d'une information (dessin, photographie, description...). L'Institut national de la propriété industrielle (INPI) délivre et enregistre cette enveloppe. Puis il renvoie un compartiment au déposant et conserve l'autre pendant une durée de cinq ans, renouvelable une fois. L'enveloppe Soleau n'assure aucune protection, ni ne fait naître de monopole d'exploitation. C'est essentiellement un outil de datation, particulièrement efficace pour faire valoir ses droits.

› Espionnage industriel

Sur le plan économique, l'espionnage peut se définir comme étant : soit l'acquisition et/ou l'interception illicite de secrets des affaires ou de savoir-faire d'une entreprise rivale ; soit, même si cela est moins couramment répandu, la déstabilisation d'un concurrent par la divulgation publique de son avantage commercial et/ou industriel. Si la finalité de la manœuvre entreprise consiste toujours à faire perdre à sa victime cette avancée économique majeure lui ayant antérieurement permis d'en tirer profit au détriment des autres acteurs du secteur, il n'en demeure pas moins qu'en droit, il n'existe à ce jour aucune définition juridique de l'espionnage de nature industrielle ou commerciale.

› Ingénierie inverse

L'ingénierie inverse ou rétro-ingénierie est l'activité qui consiste à étudier un objet pour en déterminer le fonctionnement interne ou la méthode de fabrication.

› Lanceur d'alerte

Selon la 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, un lanceur d'alerte est une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance.

› Propriété industrielle

La propriété industrielle a pour objet la protection et la valorisation des inventions, des innovations et des créations industrielles ou commerciales. Elle comprend notamment les brevets, les marques, les dessins et modèles industriels, ainsi que les indications géographiques.

› Propriété intellectuelle

La propriété intellectuelle se compose de deux branches : d'une part, les droits de « propriété industrielle », d'autre part, les droits de « propriété littéraire et artistique » (à savoir, le droit d'auteur pour les créateurs et les droits voisins du droit d'auteur pour les artistes-interprètes, les entreprises de communication audiovisuelle et les producteurs de vidéogrammes ou de phonogrammes). Cet ensemble rassemble des droits intellectuels qui confèrent à leur titulaire un monopole limité dans le temps et une action pour les défendre en cas d'atteintes : l'action en contrefaçon.

› Savoir-faire

Le savoir-faire (ou know-how) désigne généralement un ensemble de pratiques, de comportements, de connaissances, de techniques propres à un secteur d'activité ou à une personne.

› Secret de fabrication

Le secret de fabrication est une expression ne disposant pas de définition légale mais qui désigne un moyen de fabrication ayant un caractère industriel et secret.

› Secret professionnel

Il s'agit de l'interdiction faite aux personnes qui ont connaissance de faits confidentiels dans l'exercice ou à l'occasion de leur fonction, de les divulguer aux tiers, hors les cas où la loi impose ou autorise la révélation du secret.

Remerciements

La CCI Paris Ile-de-France représente et informe les entreprises. Dans le cadre de ces missions, elle encourage et soutient les projets destinés à accompagner celles-ci, afin de leur permettre de se mettre en conformité avec un nouvel environnement juridique, dans le souci essentiel de préserver leur compétitivité.

Elle tient à remercier les auteurs de ce guide :

Olivier de Maison Rouge, *Avocat, Lex-squared*

Anne Outin-Adam, *Directeur des politiques juridiques et économiques, CCI Paris Ile-de-France*

Françoise Arnaud-Faraut, *Secrétaire générale de la Commission droit de l'entreprise et fiscalité, CCI Paris Ile-de-France*

Catherine Druez-Marie, *Expert en propriété intellectuelle, CCI Paris Ile-de-France*

Et tout ceux qui ont contribué à sa réalisation :

Stéphanie Fougou, *Présidente de l'Association française des juristes d'entreprise (AFJE)*

Philippe de Robert Hautequere, *Président de la commission management de l'AFJE*

Yves Blouin, *Responsable juridique à la Fédération des industries mécaniques (FIM)*



27 avenue de Friedland
75382 Paris cedex 08

www.cci-paris-idf.fr



www.cci-paris-idf.fr/etudes et sur Twitter (@CCIParisIDF_Vox)