AVOCATS
BARREAU
• PARIS

ORDRE DES AVOCATS DE PARIS

COMMISSION OUVERTE

BREVETS ET SECRET DES AFFAIRES

CO-RESPONSABLES : ALEXANDRE JACQUET ET VIRGINIE LEHOUX, AVOCAT.E.S AU BARREAU DE PARIS

[WEBINAR]

26 OCTOBRE 2021

LE SECRET DES AFFAIRES, TROIS ANS APRÈS L'ENTRÉE EN VIGUEUR DE LA LOI 2018-670 DU 30 JUILLET 2018

AVOCATS BARREAU • PARIS

COMMISSION BREVETS ET SECRET DES AFFAIRES

REPI
Réseau Entreprise Propriété Intellectuelle

Le secret des affaires, trois ans après l'entrée en vigueur de la Loi n°2018-670 du 30 juillet 2018

AVOCATS BARREAU • PARIS

COMMISSION BREVETS ET SECRET DES AFFAIRES

REPI
Réseau Entreprise Propriété Intellectuelle

Secret des affaires : mise en perspective

Jean-Pierre CLAVIER

Professeur de droit privé à l'Université de Nantes

Directeur du master droit de la propriété intellectuelle

AVOCATS BARREAU • PARIS

COMMISSION BREVETS ET SECRET DES AFFAIRES

REPI
Réseau Entreprise Propriété Intellectuelle

benech

La protection du secret des affaires dans les entreprises

(Virginie LEHOUX, Avocate)

L’intérêt économique et stratégique de de protéger les secrets des affaires pour les entreprises

Les secrets des affaires sont des a**ctifs essentiels et stratégiques de l'entreprise.**

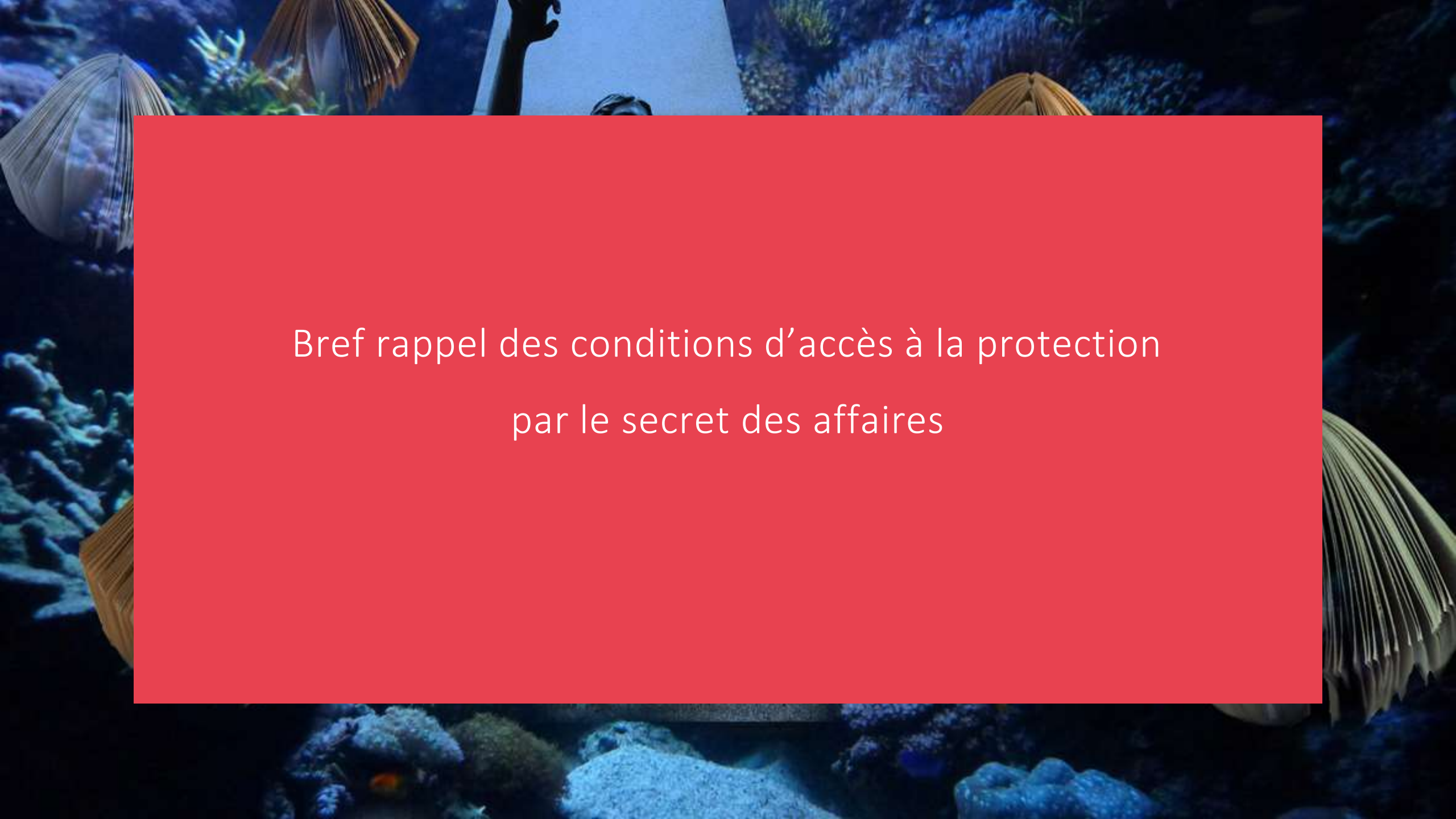
Elles sont mêmes pour certaines entreprises, le cœur de leur business car elles procurent un **avantage commercial, technique et concurrentiel** conséquent (ex : Coca-Cola)

Comme les droits de propriété industrielle, la protection au titre du secret des affaires permet de :

- Sécuriser et valoriser les investissements, notamment en R&D
- Acquérir et conserver des parts de marché
- Gêner les concurrents et les ralentir

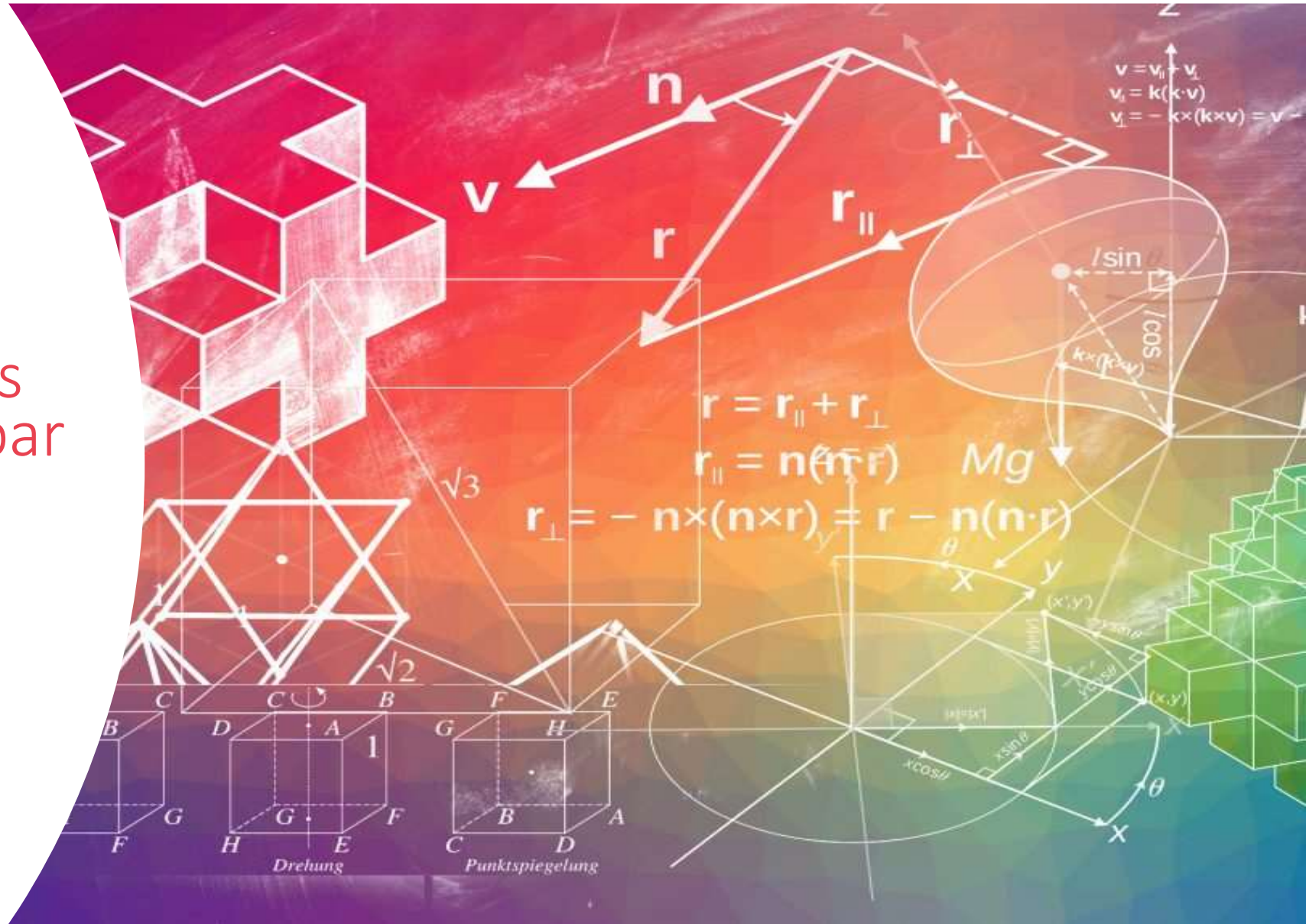
- Il est donc important que les entreprises organisent la protection de leurs secrets des affaires pour répondre aux menaces qui pèsent sur elles (fuites d'informations sensibles, espionnage industriel, cybercriminalité, etc.) dans un contexte de mondialisation et d'usage accru des technologies de l'information.

- La Loi du 30 juillet 2018 contribue à protéger les secrets des affaires.



Bref rappel des conditions d’accès à la protection par le secret des affaires

Rappel des conditions légales de protection par la Loi n° 2018-670



- Article L151-1 du code du commerce :

*Est protégée au titre du secret des affaires « **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.*

Critères de la protection au titre du secret des affaires

1. « Toute information » :

- La **nature** de l'information est **large** : de nature technique (connaissances technologiques, savoir-faire, logiciel, algorithmes, codes sources etc.) et de nature commerciale, économique et financière (données commerciales relatives aux clients, aux fournisseur, aux coûts, d'études, de stratégie de marché, organisationnelles, etc.).
- **Exclusion** : informations courantes, expériences et compétences obtenues par des travailleurs dans l'exercice normal de leur fonction et informations généralement connues de personnes appartenant aux milieux qui s'occupent normalement du genre d'information en question ou qui leur son aisément accessibles (Considérant 14)
- Le support de l'information est indifférent. Mais une identification (i.e. description) est nécessaire.

➢ **2.** Toute information « **secrète** » ou plus exactement :

- une information « ***pas généralement connue*** *ou* ***pas aisément accessible*** *en elle-même ou dans la configuration et l'assemblage exacts de ses éléments* »
- « ***par les personnes familières de ce type d'informations*** *en raison de leur secteur d'activité* »

→ Secret « relatif »

- Cela exclut les informations publiques ou celles qui sont connues dans le domaine professionnel concerné.
- Quid du Territoire ? France ? Europe ? Monde ?

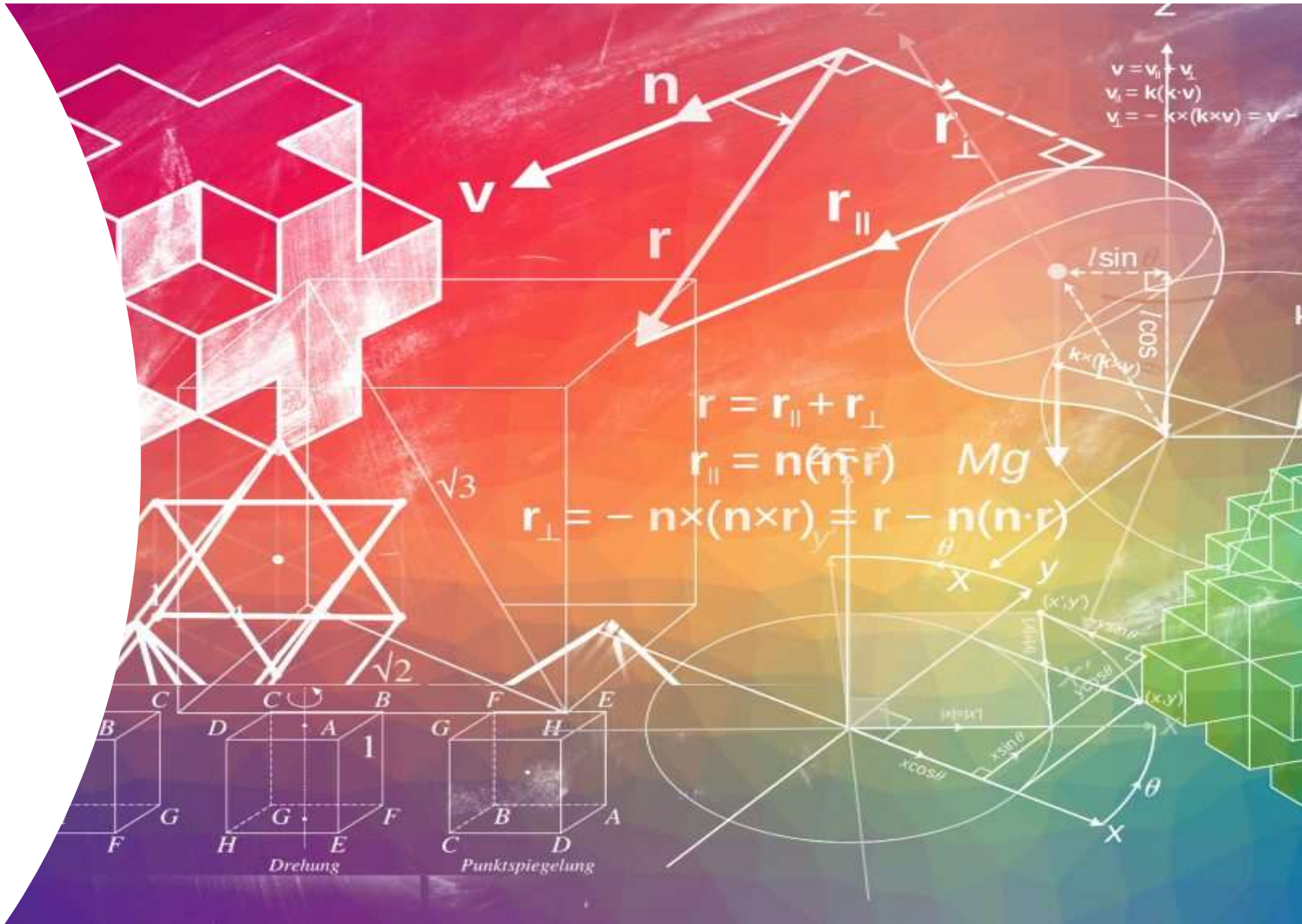
3. Toute information protégée de façon « **raisonnable** » par son détenteur légitime, « **compte tenu des circonstances »**

- Protégés par quels moyens ? Les tribunaux devront fixer le niveau et la valeur de la protection raisonnablement déployée : mesures techniques et/ou contractuelles ?
- Exigence « relative » : Test de proportionnalité (taille de l'entreprise, importance de l'information protégée, secteur industriel concerné, politiques internes de protection, etc.)
- La charge de la preuve incombe au demandeur
- Notion de « détenteur légitime » : celui qui en a le contrôle de façon licite i.e. celui qui a le droit d'autoriser l'accès, l'utilisation et la divulgation du secret des affaires

4. Elle doit avoir une **valeur commerciale** (**effective ou potentielle**) du fait de son caractère secret

- Question de la preuve et de sa charge ?
- Définition négative de la valeur commerciale par le considérant 14 de la Directive : l'obtention, l'utilisation ou la divulgation illicite du secret est susceptible de porter atteinte aux intérêts de la personne qui en a le contrôle de façon licite **en ce qu'elle nuit au potentiel scientifique et technique de cette personne, à ses intérêts économiques ou financiers, à ses positions stratégiques ou à sa capacité concurrentielle.**
- Pour le Pr Galloux, cette valeur n'existe qu'à partir du moment où pour les concurrents, leur connaissance est susceptible de leur faire réaliser des économies et donc justifie qu'ils paient pour l'obtenir.

L’apport de la jurisprudence



- Nous n'avons **pas identifié de décision sur le fond** sanctionnant une atteinte au secret des affaires de sorte qu'il est possible de s'interroger sur le point de savoir si les entreprises ont réellement pris conscience de l'intérêt de la Loi lorsqu'il s'agit de **faire respecter ses secrets des affaires**, par exemple à l'égard d'un ex-salarié indélicat ou d'un concurrent qui s'approprie et utilise un savoir-faire auquel il a illicitement eu accès.

- Il existe des **décisions en référé visant à obtenir des mesures conservatoire ou faire cesser des atteintes** au secret des affaires : ex Chambéry Civ, 1ère 30/11/2020 (RG 20/00550) ; Paris, Pôle 1, ch 2, 08/04/2021 (RG 21/05090) ; Versailles 6ème ch, 17/02/2020 (19/03646)

- Il y a de **nombreuses décisions rendues dans le cadre de mesure d'instruction** :

On observe ainsi que les parties utilisent les dispositions du Code de Commerce pour tenter de **faire obstacle à des mesures d'instructions** (article 145 du Code de Procédure Civile, enquête de l'Autorité de la Concurrence, saisie contrefaçon notamment).

- **Charge de la preuve** :

Paris, Pôle 5, Ch2, 17/12/2020 RG 19/18575 :

C’est à la partie qui entend se prévaloir de la protection au titre du secret des affaires de montrer que les critères de constitutifs de la définition du secret des affaires sont réunis.

- **<u>Caractère secret des informations</u>** :

- Les juridictions apprécient si les informations sont secrètes :
  - Informations dans leur configuration aisément accessibles ou non : ex accord d'achat de brevets entre NOKIA et WADE et avenants et contrat de licence JME 27/05/2021 (20/04020)
  - Informations échangées dans le cadre d'appels d'offre : refus de reconnaitre en référé le caractère secret du savoir-faire divulgué de façon non autorisé et qui a fait l'objet de mesure de réparation, puis qui a ensuite été réutilisé dans un second appel d'offre : Chambéry Civ, 1ère ch 3/11/2020 (20/00550)

- **<u>Caractère secret des informations</u>** :

- Paris, Pôle 1, ch 2, 08/04/2021 (21/05090) : Pour des pièces versées au débat concernant des données chiffrées et nominatives (parts de marché, volume des référence commandées, réponse à la DGCCRF, la politique commerciale de la société, des contrats avec des clauses de confidentialité), la Cour relève :
  - le caractère sensible et **par nature** confidentiel de l'information,
  - l'existence de clause de confidentialité.
- Ord Pdt TGI Paris, 22/11/2019 (19/10783) : document technique à usage interne comportant la mention « Confidentiel.

- **<u>Mesures raisonnables par le détenteur légitime</u>:**

- Nous n'avons pas identifié de décision qui viendrait définir la notion de « détenteur légitime »
- Examen de l'existence de clause de confidentialité : ex : Paris Pôle 1 ch 2, 8 avril 2021 (21/05090)
- Pdt TGI Paris Ord 25/10/2019 (09/07498) : Brochures qui avaient été prises librement sur un présentoir à l'entrée du siège social d'une société et qui ont été saisies par un huissier dans le cadre d'une saisie-contrefaçon : aucune mesure de protection raisonnable pour les conserver secrètes.

- **<u>Mesures raisonnables par le détenteur légitime</u>:**

- Existence de mesures de protection : Ex TJ Paris 4 juin 2021 (20/01390) : « *force est de constater que la liste des clients identifiés nominativement (avec pour certains d'entre eux la mention de l'identité d'une personne physique) et par pays destinataire des boites de maquillage en litige ne se trouve pas sous cette forme aisément accessibles, dispose en elle-même d'une forte valeur commerciale potentielle et* ***fait en l'occurrence l'objet de mesures élevés de protection***. »

  En l'espèce, les sociétés FAPAGAU ET COMPAGNIE et L'OREAL faisaient état du fait que les documents revêtent la mention « C3 – très confidentiel », que l'accès à ce type de document est très restreint et qu'ils sont conservés au sein d'un système d'information conservant l'identité et le moment auquel ces documents ont été édités ainsi qu'en attestent la date et l'heure après la mention « C3 – très confidentiel »

- **<u>Mesures raisonnables par le détenteur légitime</u>:**

- JME 25/07/2019 (19/06252) : à propos de l'extrait d'un plan qui était accroché au mur du local dans lequel l'huissier a été reçu pour la réalisation des opérations de saisie-contrefaçon : « *La société PYOPOWERS MEDICAL TECHNOLOGIES Franc n'allègue d'ailleurs pas l'existence de « mesures de protection raisonnables, compte tenu des circonstances, pour conserver le caractère secret de ce plan, ne serait-ce par exemple que* ***sa protection minimale dans une armoire fermée à clefs***. »

- **<u>Appréciation de la valeur commerciale</u> :**

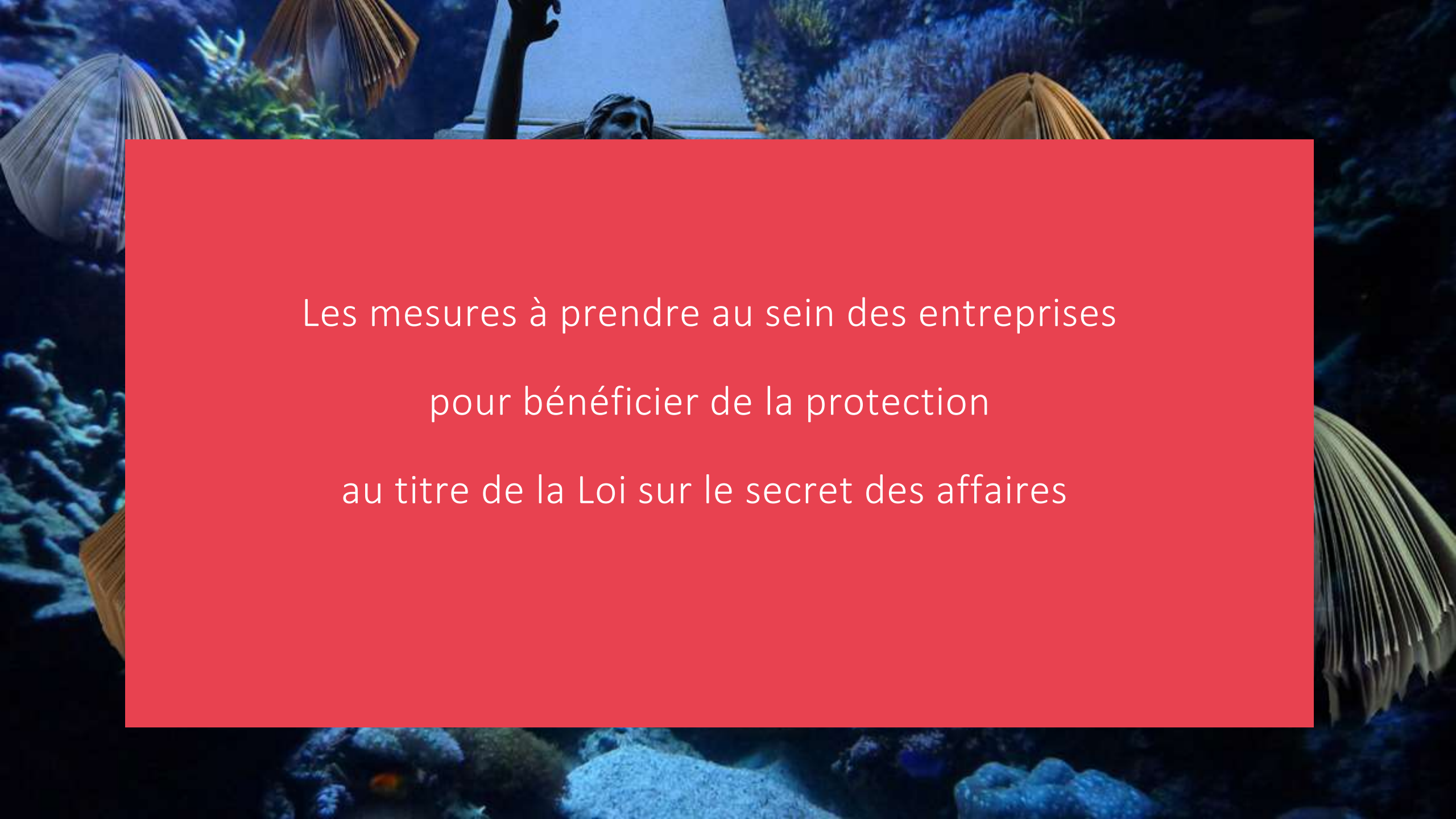
➢ **Elle se déduit du caractère secret** :

- Ord JME TJ Paris 27/05/2021 : « *aussi bien d'une part, l'accord d'achat de brevets du 22 juillet 2017 entre les sociétés NOKIA et WADE, ses annexes et avenants, et les actes de confirmation, que, d'autre part, le contrat de licence* (…) *entre les sociétés NOKIA et HUAWEI, ne sont pas, dans leur configuration, aisément accessibles.* ***Ils revêtent un valeur commerciale effective compte tenu de leur caractère secret*** *et font indiscutablement l'objet de mesures de protection raisonnables par leurs détenteurs légitimes compte tenu des circonstances*. »

➢ **Importance de la date :**

- Ex Paris, Pôle 1, ch 2, 08/04/2021 (21/05090) : données financière dans une assignation : Pour la Cour, « *informations manifestement non publiques, non aisément accessibles et datent de moins de 5 années de sorte qu'elles sont suffisamment récentes pour demeurer sensibles et stratégiques d'un point de vue commercial et concurrentiel*. »
- Ex : Paris Pôle 5, ch 2 17/12/2020 (19/18575): à propos de messages électroniques échangés entre août 2002 et mars 2007 dans le cadre de négociation d'un contrat qui a expiré depuis 2014 : « *La valeur commerciale de ces échanges, vieux de plus de quatorze ans, n'est pas montrée par la société Airnov* ».

- *Orleans, 01/04/2021 (18/13471)* : « *Le constat porte sur une période de temps limité (…) et remonte donc à plus de cinq ans et les données saisies, si elles peuvent avoir un intérêt direct pour permettre d'apprécier l'existence ou a contraire l'absence de faits de concurrence déloyale et de parasitisme en 2015,* ***n'ont plus la même acuité au regard du secret des affaires compte tenu des années écoulée****s. »*



Les mesures à prendre au sein des entreprises

pour bénéficier de la protection

au titre de la Loi sur le secret des affaires

Difficultés pratiques

- Les grands groupes avaient déjà mis en place des procédures pour protéger leurs secrets des affaires avant l'entrée en vigueur de la Loi.

- La difficulté porte sur la capacité des entreprises de plus petites tailles à identifier les informations valorisables, au sein de tout leur système d'information.

- Elles doivent également avoir la volonté de formaliser et décliner les procédures adaptées aux enjeux.

Une **protection efficace** du secret des affaires suppose la mise en place d'une **procédure spécifique** au sein des entreprises composée de **trois** étapes-clés :

- l'identification des informations confidentielles éligibles au secret des affaires ;
- leur classification confidentielle ;
- l'organisation et le choix de leur protection, par la mise en place d'outils destinés à sécuriser les secrets d'affaires

Etape 1 : identifier les informations et les ressources de l'entreprise

- Inventorier les **informations sensibles** de l'entreprise et celles qui ont de la **valeur** :

Informations techniques :

- Résultats de la R&D,
- Procédés de fabrication
- Plans de fabrication
- Comptes rendus d’essais
- Codes sources
- Algorithmes
- Savoir-faire
- Projets de développement en cours
- Analyse des pistes de développement des concurrents
- Dossiers techniques retraçant l’ensemble des opérations de fabrication des pièces et les coûts associés, etc.

Informations commerciales et financières :

- Données commerciales stratégiques : Volumes de production, taux de marge, bénéfices, politiques de prix , etc
- Stratégie commerciale
- Gammes de produits
- Analyse de la stratégie commerciale des concurrents
- Etudes et veille concurrentielle
- Propositions commerciales
- Projets d'acquisition d'entreprise
- fichiers clients ou fournisseurs ou prospects;
- Méthodes de prospection commerciale ;
- Contrats, etc,

Organisation interne

- Procédures réglementaires
- Procédures « qualité »
- Plan de gestion des risques/analyse de risques
- Rapport d’audit interne
- Modèles de contrats
- Décision / Avis du conseil d’administration ou de la direction
- Organigramme
- Dossiers du personnel, etc,

- **Identifier les personnes ayant besoin d'y avoir accès :**

➢ **En interne**: les salariés travaillant sur le projet

- Direction / Commerciaux / Administratif : De quelles informations ont-ils besoin ?
- Techniciens
  - ➢ Attention aux stagiaire , experts indépendants

➢ **A l'extérieur de l'entreprise** :

- Partenaires commerciaux: laboratoire pour des essais, sous-traitant, distributeur, clients
- Institutionnels (dans le cadre de subventions par ex)
- Universitaires ou bureau d'études indépendant
- Colloques, conférences

- Recenser les **systèmes d'information** de l'entreprise (ordinateurs fixes et portables, serveurs, hébergement, accès à internet, messagerie électronique, logiciels, clés USB, Wi-fi, téléphones fixes et portables, photocopieurs, armoires et locaux d'archivage…) ;

- **Cartographier l'entreprise et ses partenaires** (notamment localiser les différents sites de l'entreprise, en identifiant les filiales et les lieux de production, prestataires) ;

- Evaluer les **risques** et vulnérabilités.

Etape 2 : Classifier les données confidentielles.

La Loi suggère de mentionner explicitement qu'une information est confidentielle.

Mais l'entreprise pourrait affiner cette classification en hiérarchisant les informations. Elle pourrait ainsi leur attribuer un code reflétant le niveau de classification selon différents critères : public, sensible, critique, stratégique (par exemple Strate 0, Strate 1, Strate 2, Strate 3).

Cela permet en outre de délimiter le rang des personnes ayant accès à ces informations.

➔ La classification des informations par strates en fonction de l'importance de l'information

3) Strate 1 : information sensible

Information largement accessible au personnel dont la fuite n'entraîne qu'une gêne sans conséquence durable (ex : méthode de management, grille tarifaire…)

2) Strate 2 : information critique

Information nécessaire pour le bon fonctionnement de la société et dont la fuite pourrait avoir des conséquences graves mais réparables (ex: fuite du savoir faire d'Areva pour le démantèlement des centrales nucléaires).

1) Strate 3 : information stratégique :

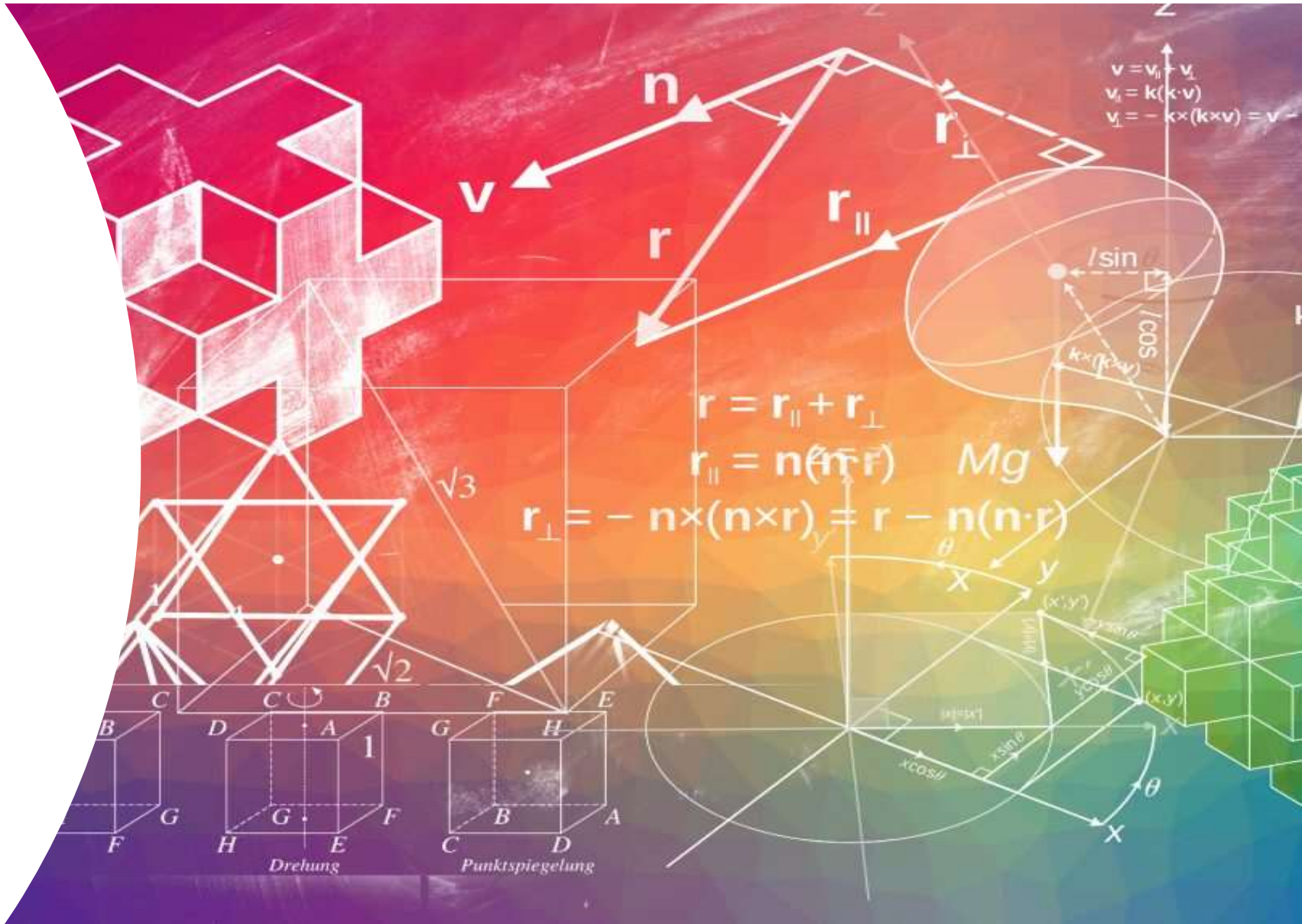
Accessible uniquement par les personnes autorisées.

Dont la divulgation a un impact irréparable et visible pour les résultats, voire la survie de la société (ex : le secret de fabrication de Coca Cola).

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.

Des moyens contractuels



Pour les salariés :

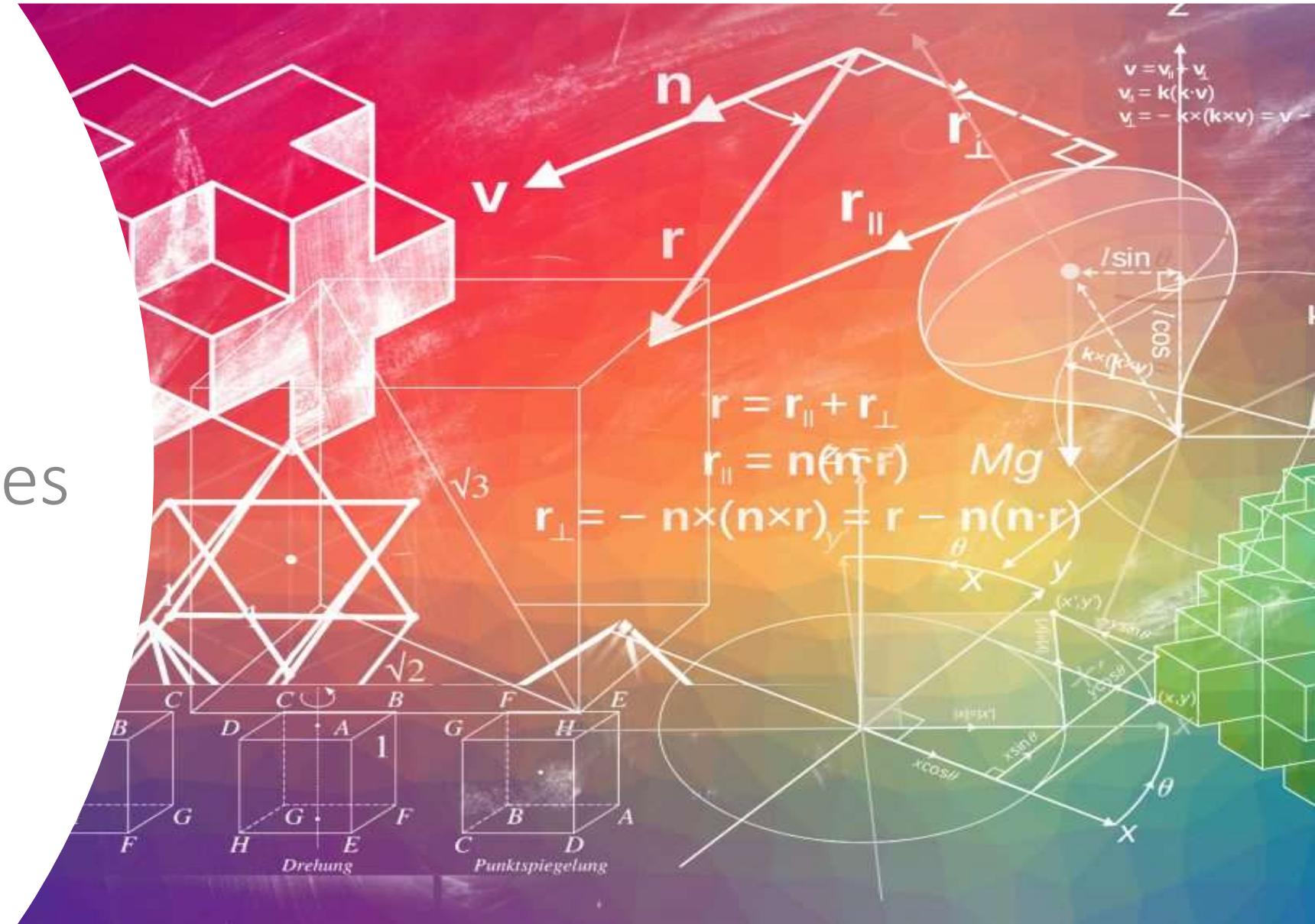
- Obligation de loyauté implicite
- Insérer dans les contrats de travail des clauses de confidentialité, de restitution des documents sensibles et éventuellement une clause de non-concurrence ;
- Rédiger et diffuser une charte éthique générale et une charte informatique ;
- Rappeler la politique en matière 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… ;

Pour les partenaires

Prévoir un contrat qui comprendra :

- une clause de confidentialité (identification des informations, des personnes habilitées à recevoir l'information) : non divulgation/utilisation
- Des clauses de non-concurrence et de non-débauchage
- Une clause générale imposant au partenaire 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.

Des moyens techniques/pratiques



Les moyens organisationnels pour se prémunir

- Sécurisation et rangement des informations
- Les moyens de préserver le secret : les supports
- Se pré-constituer des preuves
- La destruction des documents
- Implication et sensibilisation du personnel

- **Sécuriser les systèmes d'information et intranet :**
  - Mesures techniques : mot de passe sur les fichiers, solution de chiffrement des mails / disques durs / contrôle de l'usage des périphériques sur les postes (attention aux clefs USB)
  - Antivirus à jour – effectuer les mises à jour régulièrement
  - Appliquer les patchs correctifs de sécurité
  - Privilégier si possible le travail en circuit fermé (des ordinateurs hors réseau pour la protection d'informations spécifiques)
  - Politique de restriction de l'accès à l'information : autorisation / habilitation / hiérarchisation de l'accès, mot de passe à échéance déterminée.
  - Attention en cas d'accès à distance aux postes de travail depuis le domicile ou un autre lieu
  - Externalisation de la gestion informatique envisageable (notamment pour avoir une sauvegarde externe en cas de cyber attaque)

- Où ranger ?
  - Informations numériques : enregistrement à échéance automatique prédéterminée sur disque dur externe et/ou Cd Rom, externalisation des sauvegarde, ordinateur hors réseau, blockchain
  - Informations matérielles : coffres forts (classique/électronique), armoires fermées à clefs !
  - Dans des endroits clos et sécurisés.

- Comment ranger ?
  - Politique organisée de rangements et d'accès à l'information selon la classification opérée
  - Maintenance informatique : dépistage de tracking
  - L'information confidentielle : pas au dessus de la pile !

Les moyens de préserver le secret : les supports

- **Rédiger des comptes rendus des réunions de travail** (indices utiles pour déterminer la paternité d'une information)
- **Cahiers de laboratoire**
- ***Sauvegardes internalisées et externalisées***
- ***Coffres***
- **Apposer la mention « confidentielle » sur tous les documents sensibles** (offres, documentation technique, plans…)

Se pré-constituer des éléments de preuves

- **Eventuels dépôts auprès d'un officier public ministériel conférant une date certaine**
- **Dépôts INPI :** enveloppe Soleau
- **Dépôts APP :** pour les logiciels
- **Effectuer des copies et sauvegardes** (conserver les originaux)
- **Horodatage électronique**
- **Blockchain**
- **Dans le cadre d'une collaboration :** Identifier précisément les connaissances/informations propres afin de déterminer quelles seront les informations communes (importance des annexes)

La destruction des documents

A la fin d'une collaboration, l'une des problématiques est la conservation des éléments échangées avec l'autre partie.

Il faut donc organiser soit :

- Le retour des éléments,
- La destruction des éléments,
- un mixte des deux

Idéalement, ces deux points doivent être prévus dans les contrats :

« *A la fin de la collaboration, pour toutes les raisons prévues dans le cadre du présent contrat, les Destinataires des informations confidentielles s'engagent à détruire l'ensemble des informations confidentielles transmises pour les besoins du projet, à défaut de quoi il engagera sa responsabilité contractuelle ».*

En pratique :

- Utiliser une broyeuse
- Devant Huissier

Implication et sensibilisation du personnel

- **Sensibiliser le personnel (ingénieurs, techniciens, équipes commerciales…) notamment lorsqu'ils ont accès à ces informations**

  - Dès l'embauche par le contrat de travail (obligation de loyauté + confidentialité)
  - Participation à des formations (connaître les termes, les enjeux et les moyens d 'action)
  - Charte interne d'usage et de bonnes pratiques; note interne sur les procédures à suivre en cas de contagion des ordinateurs

- **Responsabilisation du personnel : connaissance de ce qui est confidentiel et de la valeur des informations**

  - L'information doit être vue à la fois comme un patrimoine vivant et économique dont les salariés sont codétenteurs et coresponsables.

- **Précautions à prendre lors de contacts extérieurs** (éviter toute divulgation accidentelle, ne pas communiquer plus que nécessaire)

- **Possibilité de restreindre l'accès et la diffusion des documents « secrets » en interne**

- **Salles de confiance : discussion/zone blanche/zones sans portables** (éviter écoutes téléphoniques, captation des données…)

- **Cheminement intellectuel :**
  1. Avoir conscience de l'importance de l'information
  2. Pour ensuite, mettre en œuvre les moyens matériels et juridiques pour en assurer la protection.

Dernière préconisation : nommer un référent dans l'entreprise en charge de la question du secret des affaires.

Le DPO (Data Protection Officer) ou Délégué à la protection des données (DPD) institué par la Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles [qui transpose le règlement européen du 27 avril 2016 relatif à la protection des données personnelles (dit RGPD)] pourrait également être la personne en charge de la gestion d'une politique de sécurité des informations sensibles qui répondent à la définition du secret des affaires.

LA PRESERVATION DU SECRET DES AFFAIRES DANS LE CADRE DES PROCEDURES CIVILES ET PENALES

Jean-Frédéric GAULTIER

ETAT DE LA JURISPRUDENCE

Décisions rendues sur le fondement des **articles L. 153-1 et suivants du code de commerce** :

- **Tribunaux de commerce : 8**
- **Tribunaux judiciaires : 10**
- **Cours d'appel : 38**

Recherche effectuée sur Doctrine à partir des mots-clefs « L151 » et « L153 »

ETAT DE LA JURISPRUDENCE

Ces décisions statuent principalement sur des demandes de :

- **levée de séquestre provisoire**
- **désignation d'un expert** en vue de l'examen des pièces
- détermination des **modalités de communication des pièces**

Selon cette recherche, aucune décision n'a été rendue au fond sur le fondement des articles L.151-1 et suivants du code de commerce

GESTION DE LA CONFIDENTIALITE DEVANT LE TRIBUNAL JUDICIAIRE

Placement sous séquestre provisoire (article R153-1 du code de commerce):

- Une faculté pour le juge, lorsqu'il est saisi sur le fondement de l'article 145 du code de procédure civile ou d'une requête aux fins de saisie-contrefaçon, ainsi qu'au cours d'une mesure d'instruction ordonnée sur ce fondement

- Une certaine latitude est laissée à l'huissier

- La mesure de séquestre provisoire est levée et les pièces sont transmises au requérant si, dans un **délai d'un mois à compter de la signification de la décision**, le juge n'a pas été saisi d'une demande de modification ou de rétractation de son ordonnance

GESTION DE LA CONFIDENTIALITE DEVANT LE TRIBUNAL JUDICIAIRE

Modalités de communication des pièces (articles L153-1 et R. 153-2 et suivants du code de commerce):

- la partie ou le tiers invoquant le secret des affaires devra remettre au juge, dans un délai fixé par le juge, (i) la **version confidentielle** intégrale de la pièce, (ii) une **version non-confidentielle** ou un résumé de celle-ci et (iii) un **mémoire** précisant les motifs qui confèrent aux pièces un caractère secret (article R. 153-3)

- Le juge statue sans audience (article R. 153-4)

- le juge peut **refuser la communication** de la pièce, o**rdonner sa communication dans sa version intégrale** le cas échéant en limitant l'accès à celle-ci, ou ben **ordonner la communication d'une version non-confidentielle** ou du résumé de la pièce, en fonction de ce qu'il estimera « nécessaire à la solution du litige » (articles R. 153-5 à 153-7).

GESTION DE LA CONFIDENTIALITE DEVANT LE TRIBUNAL JUDICIAIRE

Confidentialité du jugement (article R153-10 du code de commerce):

- à la demande d'une partie, **un extrait de la décision ne comportant que son dispositif**, revêtu de la formule exécutoire, pourra lui être remis pour les besoins de son exécution forcée, et

- **une version non confidentielle** de la décision, dans laquelle sont occultées les informations couvertes par le secret des affaires, **peut être remise aux tiers** et mise à la disposition du public sous forme électronique

Cour d'appel de Paris, Pôle 5, 16 avril 2019, No. 15/17037 : considérant que les motifs retenus pour juger de la procédure n'ont pas conduit la cour à faire état du contenu de pièces qui seraient de nature à porter atteinte au secret des affaires, la Cour retient « *qu'il n'y a pas lieu d'adapter la motivation du présent arrêt ou les modalités de sa publication* ».

GESTION DE LA CONFIDENTIALITE DEVANT LE TRIBUNAL JUDICIAIRE

Modalités de communication des pièces (décisions rendues en matière de brevets d'invention):

Au cours de la mise en état:

- Que les conseils (avocats et CPI, français et étrangers) et/ou certains représentants des parties
  - Cf. L153-2 du code de commerce
- Signature ou non d'un engagement de confidentialité
- Communication ou consultation des pièces
- Expertise de tri

Lors de l'audience de plaidoiries:

- Chambre du conseil ou audience publique

GESTION DE LA CONFIDENTIALITE DANS LES PROCEDURES PENALES

Enquête préliminaire et instructions

- **Article 11 CPP**: « *Sauf dans le cas où la loi en dispose autrement et sans préjudice des droits de la défense, la procédure au cours de l'enquête et de l'instruction est secrète. (…)* »

- Expertise pénale

Le procès

- **Article 400 CPP:**

  «Les audiences sont publiques.

  Néanmoins, le tribunal peut, en constatant dans son jugement que la publicité est dangereuse pour l'ordre, la sérénité des débats, la dignité de la personne ou les intérêts d'un tiers, ordonner, par jugement rendu en audience publique, que les débats auront lieu à huis clos. (…) »