Le jeu des

8 FAMILLES

d'atteintes à la sécurité économique

et ses 48 fiches thématiques

SÉCURITÉ ÉCONOMIQUE & PROTECTION DES ENTREPRISES

La Gendarmerie nationale et l'INHESJ, acteurs de la politique publique d'intelligence économique

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre

INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

Gendarmerie nationale

Richard LIZUREY
Général d'armée, directeur général de la gendarmerie nationale
(DGGN)

Hélène CAZAUX-CHARLES
Magistrate, directrice de l'Institut national des hautes études de la sécurité et de la justice
(INHESJ)

Agir, sensibiliser et former à la sécurité économique.

L'évènement est quelque peu passé inaperçu pour le grand public, mais pour les praticiens de l'intelligence économique en France, la publication du décret du 20 mars 2019, relatif à la gouvernance de la politique de sécurité économique, marque une étape significative pour ne pas dire disruptive.

En effet, par ce décret, le Gouvernement réaffirme toute la priorité donnée à la préservation de la sécurité et de la souveraineté économiques, et renforce son organisation pour répondre efficacement à l'évolution de la menace. La sécurité économique se voit ainsi dotée d'une véritable politique dont le pilotage reste confié au Commissaire de l'information stratégique et de la sécurité économiques (fonction occupée par l'actuel directeur général des entreprises) ainsi qu'au service qui lui est rattaché (SISSE).

A l'heure où est conféré au dispositif de gouvernance interministérielle de la sécurité économique une nouvelle envergure, la direction générale de la Gendarmerie nationale (DGGN) et l'Institut national des hautes études de la sécurité et de la justice (INHESJ) vous proposent de découvrir « Le jeu des 8 familles d'atteintes à la sécurité économique ». Véritable mode d'emploi ludique et didactique, ce kit de sensibilisation composé d'un jeu de 52 cartes et de 48 fiches thématiques se donne pour ambition de fournir quelques clés de compréhension des atteintes, légales ou non, auxquelles les acteurs économiques sont exposés.

Forte d'un réseau de près de 200 référents « Sécurité économique et protection des entreprises » répartis dans les territoires, la Gendarmerie nationale entend bien poursuivre sa mobilisation pour agir et sensibiliser les acteurs économiques, en partenariat avec le département « Intelligence et sécurité économiques » de l'INHESJ qui forme, depuis plus de 10 ans, ces référents. La vocation de ce département consiste, en effet, à diffuser à l'ensemble des acteurs, quels que soient leur secteur d'activité, la taille de leur structure ou leur nature publique ou privée, cette culture d'intelligence et sécurité économiques.

Avec le jeu des 8 familles d'atteintes à la sécurité économique, la Gendarmerie nationale et l'INHESJ poursuivent ainsi, pour le bénéfice du plus grand nombre, l'écriture d'une histoire commune débutée en 2009 par la fusion de l'IERSE et de l'INHES. Ces actions communes s'inscrivent dans une vision partagée public/privé de la sûreté des entreprises et contribuent ainsi à la structuration d'un véritable État stratège et partenaire des entreprises.

Un jeu donc, mais un jeu sérieux qui aide à comprendre pour agir !

DIRECTION DE LA PUBLICATION
GCA Christian RODRIGUEZ
Hélène CAZAUX-CHARLES
GCA François GIERE
GB Jean-Marc CESARI
GB Laurent BITOUZET
Angélique LAFONT

MAQUETTE PAO
SIRPA Gendarmerie
Infographie INHESJ
Lcl Christophe TORRISI

RÉDACTION
Lcl Christophe TORRISI
Gend Stéphane MORTIER
Laura BANCON
Olivier CLEMENT
Lcl (ER) Thierry ARCHAMBAULT

DÉPÔT LÉGAL
DGGN
4 rue Claude Bernard
92130 Issy-les-Moulineaux

Imprimerie : SDG
11 rue Paul Claudel 87000 Limoges
Avril 2019

ATTEINTES À LA SÉCURITÉ ÉCONOMIQUE: UNE HISTOIRE DE FAMILLE

Christophe Torrisi
Lieutenant-colonel de gendarmerie, adjoint au chef
de département Intelligence et sécurité économiques
(INHESJ)

Pour les acteurs publics de la sécurité économique, qu'ils appartiennent à des services de renseignement spécialisés ou à des services plus généralistes, les familles d'atteintes ne seront peut-être pas une nouveauté. L'idée de les formaliser sous la forme d'un jeu de cartes et de les accompagner de fiches thématiques constitue en revanche un référentiel unique et utile à partager dans le cadre de la démarche partenariale public / privé.

Né d'une initiative de la section sécurité économique et protection des entreprises (SEcoPE) de la Sous-Direction de l'Anticipation Opérationnelle (SDAO) à la DGGN, et fruit d'un travail collaboratif, le jeu des 8 familles d'atteintes à la sécurité économique se donne pour ambition de répondre, par une approche ludique et didactique, à trois défis.

Le premier défi : accompagner les chefs d'entreprise parfois esseulés, souvent désemparés, et qui ne savent pas toujours contre qui ou contre quoi se protéger. Ai-je vraiment pris la mesure de l'intrusion d'une personne, d'une destruction de matériels ou d'un vol de documents sensibles dans mon établissement ? Un salarié me quitte : a-t-il été débauché ? Ce départ est-il répréhensible et avais-je les moyens juridiques de me protéger ? Mon entreprise est dénigrée : vers qui dois-je me retourner ? Comment puis-je remédier à la perte d'une compétence clé ? L'avais-je même anticipée ?

Le deuxième défi : renforcer la prise de conscience. En effet, la difficulté avec les atteintes à la sécurité économique est qu'elles peuvent se parer de légalité, ce qui les rend difficiles à déceler ou à dénoncer.

Le troisième défi : faciliter l'action des policiers et gendarmes confrontés à tous les maux de la société, et qui ne disposent pas toujours, en matière de sécurité économique, des clés de compréhension alors qu'ils se trouvent exposés en première ligne aux victimes d'atteintes en la matière.

Les huit familles qui composent le jeu sont les suivantes :

1. Atteintes physiques sur site
2. Fragilisations/Désorganisations
3. Atteintes aux savoir-faire
4. Intrusions consenties
5. Risques financiers
6. Risques informatiques
7. Fragilités humaines
8. Atteintes à la réputation

Chaque famille compte 6 cartes, lesquelles représentent soit une atteinte, soit un dispositif de protection qui y est lié et décrit de manière aisément compréhensible. Pour chaque famille d'atteinte à la sécurité économique détaillée dans ce jeu, le choix a été fait de mettre en évidence, sans exhaustivité, les principaux risques auxquels sont soumis les acteurs économiques.

Partant du constat qu'identifier les risques, c'est surtout se donner les moyens de mieux les prévenir, il a été décidé d'accompagner chaque carte d'une fiche thématique qui permet de dépasser la simple description de l'atteinte et d'orienter le joueur, l'entrepreneur, le salarié, vers des ressources en ligne insoupçonnées.

La sécurité économique c'est assurément l'affaire de tous. Alors n'attendons plus et jouons ensemble !

LES ATTEINTES PHYSIQUES SUR SITE
Les intrusions

DISSUADER & PROTÉGER

Le renforcement de la surveillance et de la protection des sites industriels ne se révèle pas toujours suffisamment dissuasif et les entreprises doivent en permanence parer à toute éventualité. Qu'elle soit de nature ciblée ou d'opportunité, ***l'intrusion visera souvent l'appropriation de secrets industriels ou le vol d'informations sensibles***. Si la mise en place de dispositifs technologiques permet de réduire les vulnérabilités d'un site, le respect des procédures existantes par chacun des salariés devra être rigoureusement observé.

SÉCURITÉ & SÛRETÉ

Particulièrement préoccupés par le contexte sécuritaire, de nombreux chefs d'entreprises se disent peu ou mal préparés vis-à-vis des actes de malveillance dont ils peuvent être l'objet. Parce que la protection de son organisation ne peut s'envisager qu'au travers d'une sécurité globale, il importe de bien articuler sécurité et sûreté, et d'en définir les contours.

La sécurité au sein d'une entreprise désigne l'ensemble des moyens humains, organisationnels et techniques mis en oeuvre pour prévenir ou faire face à de nombreux risques, qu'ils soient d'ordre technique, physique, chimique ou environnemental (risque incendie, accidents du travail, risques psychosociaux, risques liés aux équipements professionnels, etc.).

La sûreté concerne l'ensemble des moyens humains, organisationnels et techniques réunis pour faire face à des actes spontanés ou réfléchis ayant pour objet de nuire ou de porter atteinte à l'entité concernée (actes de malveillance, intrusions, incivilité, actes terroristes, etc.).

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

VERS L'ÉLABORATION D'UNE NORME « SÛRETÉ & RÉSILIENCE »

Evoluant dans un environnement hyperconcurrentiel et mondialisé, les organisations publiques et privées doivent quotidiennement faire face à des menaces protéiformes qui mobilisent les services de sécurité et de sûreté de ces entités.

L'adoption de normes internationales permet d'intégrer le risque dans la prise de décision et la poursuite d'objectifs de performance. En matière de sécurité et sûreté, certaines références tiennent le haut du pavé, comme par exemple:

- ***La norme ISO 27000*** pour assurer le management de la sécurité de l'information,
- ***La norme ISO 31000*** pour intégrer l'évaluation des risques aux processus de gouvernance,

A l'initiative de la France (AFNOR), une proposition de travail a été présenté à l'organisation internationale de normalisation (ISO) en vue de ***structurer un modèle de management de la sûreté préventive*** plus agile et destiné à homogénéiser les pratiques opérationnelles.

Fin septembre 2018, la proposition française était approuvée par 30 pays sur 34 votants. La conception de la future norme ISO 22342 peut dès lors commencer.

- Si vous recherchez une norme, le site www.Service-Public-Pro.fr peut vous accompagner.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour prévenir toute forme d'intrusion, vous pouvez:

- Identifier, cartographier et hiérarchiser les zones de l'entreprise en fonction des risques et vulnérabilités qu'elles peuvent représenter,
- Le cas échéant, déterminer des droits d'accès par zone,
- Nommer un responsable sécurité si vous en avez la capacité,
- Enregistrer chaque visiteur et imposer un encadrement ainsi qu'un parcours de notoriété,
- Recourir à des dispositifs techniques de surveillance et de détection d'intrusion peut constituer un rempart efficace (clôtures, barrières végétales, volets, serrures, éclairage, chien,…),
- Faire appel à un référent sûreté.
  La gendarmerie vous en présente le dispositif sur son site. De nombreuses ressources sont disponibles sur le site www.referentsurete.fr
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES PHYSIQUES SUR SITE
Les destructions

DES MENACES TOUS AZIMUTS

Les destructions, dégradations et autres détériorations sont autant d'actes de malveillance qui peuvent avoir des **conséquences préjudiciables sur l'activité de l'entreprise** (perte d'exploitation, chômage technique, voire disparition de l'entreprise dans les cas les plus graves). Ces **actes de malveillance** peuvent se manifester **sous diverses formes**, lorsqu'ils sont commis dans le but de nuire à l'entreprise, à ses employés, à ses dirigeants ou encore à ses clients. Dans un contexte de menace terroriste, la tentation est naturellement grande de penser à des agressions d'origine extérieure. Bien que rares, les actions néfastes commises par des salariés en interne ne doivent être ni négligées, ni minimisées.

RESPONSABILISATION ET MANAGEMENT AU SEIN DE L'ORGANISATION

La mise en place de mesures techniques ou organisationnelles peut ne pas suffire à préserver l'intégrité de son établissement, et il importera donc, en amont, d'accompagner chacune de ces mesures par la responsabilisation et l'implication de tous les salariés.

- Pour manager la sécurité économique au sein de votre organisation, vous pouvez vous appuyer sur les outils mis à disposition par le service de l'information stratégique et de la sécurité économiques (SISSE) sur le site www.entreprises.gouv.fr
- Aucun dispositif n'étant infaillible, il importe de bien identifier les menaces et leurs impacts sur votre activité. La ***certification ISO 22301*** a été élaborée pour vous permettre d'anticiper et améliorer la résilience de votre organisation.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

UNE RÉPONSE PÉNALE ADAPTÉE

Les destructions relevant du droit commun

L'article 322-1 du Code pénal, dispose que « La destruction, la dégradation ou la détérioration d'un bien appartenant à autrui est punie de deux ans d'emprisonnement et de 30 000 euros d'amende, sauf s'il n'en est résulté qu'un dommage léger ».

Les destructions visant les intérêts fondamentaux de la nation

L'article 411-9 du Code pénal réprime beaucoup plus sévèrement les destructions lorsque ces faits sont de nature à porter atteinte aux intérêts fondamentaux de la nation. Les peines prévues vont de 15 à 20 ans de détention criminelle et l'amende peut atteindre 300 000 euros.

La faute lourde du salarié

Dans le cadre des relations de travail, la faute lourde constitue la faute la plus sévère qui puisse être relevée à l'encontre d'un salarié, en ce sens qu'elle ***révèle une intention de nuire vis-vis de son employeur ou de l'entreprise*** concernée.

Le site www.Service-Public.fr (F1137) vous donne quelques conseils sur les distinctions à observer concernant les fautes du salarié.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous souhaitez réduire le risque d'être victime d'une action de destruction:

- Vous devez exploiter tous les ressorts de la prévention situationnelle (dissuader, bloquer, ralentir, détecter, interpeller, etc.).
- Des référents sûreté peuvent vous accompagner. La gendarmerie vous en présente le dispositif sur son site. De nombreuses ressources sont disponibles sur le site www.referentsurete.fr
- Vous devez vous préparer à une gestion de crise dans l'éventualité où les dommages causés auraient un impact direct sur l'activité de votre organisation.
- L'élaboration un plan de continuité d'activité (PCA) peut constituer un préalable nécessaire. La direction générale des entreprises (DGE) a réalisé en juillet 2015 avec CPME un kit PCA à l'usage du chef d'entreprise.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES PHYSIQUES SUR SITE
Les vols de documents sensibles

PROTÉGER SON PATRIMOINE IMMATÉRIEL

Le vol de documents sensibles en entreprise constitue l'un des risques majeurs à considérer avec le plus grand intérêt. Pouvant trouver son origine dans une ***agression extérieure***, cette atteinte à la sécurité économique peut aussi être le fruit de négligences internes, qu'elles soient organisationnelles ou comportementales. Les ***intrusions consenties*** (visites de délégations, stagiaires, conférences, etc.) en constituent une parfaite illustration. Avec l'essor des technologies de l'information et de la communication, le vol de documents sensibles en est que plus aisé, et les ***actes d'espionnage*** sont très souvent insoupçonnés.

IDENTIFIER L'INFORMATION STRATÉGIQUE

Toute entreprise produit et conserve des documents sensibles dont la perte, la diffusion ou l'altération peut se révéler grandement préjudiciable. Toutefois, au risque de paralyser l'activité d'un établissement, ***toutes les informations sensibles ne sont pas à protéger de façon identique***.
Une analyse précise des risques doit être le préalable à toute démarche de protection. Celle-ci permettra de déterminer les moyens les mieux adaptés de protection et d'échange de l'information ainsi que les conditions de son stockage.

- Pour bien identifier l'information stratégique, exploitez les outils mis à disposition par le service de l'information stratégique et de la sécurité économiques (SISSE) sur le site de la direction générale des entreprises (DGE) à l'adresse suivante: www.entreprises.gouv.fr
- Parmi les fiches de « La sécurité économique au quotidien » l'une d'entre-elles s'intitule « Bien identifier l'information stratégique à protéger ».

Ce document a été réalisé par la DGGN et l'INHESJ et à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

PRÉVENIR LA FUITE D'INFORMATION

Faisant suite aux préconisations d'un rapport de 2006 relatif à l'***économie de l'immatériel***, l'Etat créait, par arrêté du 23 avril 2007, un service à compétence nationale dénommé « ***Agence du Patrimoine Immatériel de l'Etat*** (APIE) » destiné notamment à accompagner les administrations dans la valorisation et la protection de leur patrimoine immatériel.

S'inscrivant dans une dynamique relativement similaire, l'***association française de la normalisation*** (AFNOR) a entrepris, dans le cadre d'un groupe de travail, de réaliser un guide en vue de faire prendre conscience aux organisations des impacts économique, financier, d'image, et concurrentiel d'une fuite de tout ou partie de son patrimoine informationnel.

- En date de 2014, ce guide, référencée sous le n° ***BP Z90-001 « Prévention et gestion de la fuite d'informations - Protection du patrimoine informationnel*** », présente et décrit les principaux domaines de la prévention et de la gestion de la fuite d'information (DLP) et indique comment en limiter les risques.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Afin de vous accompagner dans la compréhension de ces atteintes, et vous permettre d'agir sur vos vulnérabilités, la Direction Générale de la Gendarmerie Nationale et l'Institut National des Hautes Études de la Sécurité et de la Justice vous proposent de découvrir le « ***Jeu des 8 familles d'atteintes à la sécurité économique*** ». Ludique et véritable outil de sensibilisation, ce jeu de 52 cartes s'accompagne de 48 fiches thématiques relatives aux atteintes abordées.

Pour prévenir les vols et la fuite de documents sensibles, vous pouvez commencer par:

- Identifier puis protéger les documents sensibles afin qu'ils ne soient accessibles qu'aux personnes ayant besoin d'en connaitre (meilleure traçabilité),
- Instaurer une culture de confidentialité (charte informatique, clauses de confidentialité, etc.) prenant en compte le classement et l'archivage des documents sensibles,
- Entreprendre une numérisation de son fond documentaire en vue d'optimiser les processus métiers et assurer une meilleure protection de ses actifs matériels,
- Avec l'adoption, fin juin 2018, de la loi sur le secret des affaires, ***une information pourra être protégée par le secret des affaires*** sous réserve « d'être connue par un nombre restreint de personnes », « de revêtir une valeur commerciale, effective ou potentielle », et « de faire l'objet de mesures de protection raisonnables pour en conserver le caractère secret ».
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES PHYSIQUES SUR SITE
Le responsable sécurité

PRÉVENTION ET PROTECTION DES RISQUES

La prévention et la protection des risques en entreprise vise à réduire le nombre d'incidents et les coûts qui y sont liés. Il importe alors qu'une personne soit désignée pour veiller à la bonne application des mesures de sécurité prévues.
Depuis le 1er juillet 2012, les employeurs doivent disposer, au sein de leur entreprise, d'un ***responsable en charge de la protection et de la prévention des risques professionnels***. Ces dispositions sont rappelées par les décrets n°2012-135 relatif à l'organisation de la médecine du travail et n°2012-137 relatif à l'organisation et au fonctionnement des services de santé au travail.

LE RÔLE DU RESPONSABLE SÉCURITÉ

L'article L.4644-1 du code du travail dispose que « L'employeur désigne un ou plusieurs salariés compétents pour s'occuper des activités de protection et de prévention des risques professionnels de l'entreprise…». Celui-ci aura à coeur de ***protéger les patrimoines matériel et immatériel de l'entreprise, tout en préservant les conditions de travail***.
Le choix est laissé aux entreprises de confier cette charge à l'un de ses employés ou de recourir à un prestataire extérieur.

Dans sa mission de ***prévention des risques professionnels***, le responsable sécurité doit s'engager à préserver la santé des travailleurs de l'établissement. Son action sera d'évaluer les risques, de diffuser des consignes de sécurité ainsi que de prévenir et informer les nouveaux et anciens salariés des risques professionnels.

Les facteurs de risques professionnels sont définis à l'article L.4161-1 du code du travail.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LE DOCUMENT UNIQUE DE SÉCURITÉ (D.U.S)

Depuis le décret n°2001-1016, le document unique de sécurité revêt un caractère obligatoire pour toutes les entreprises et associations disposant d'un salarié ou plus.

Pour les grandes entreprises, un document unique est établi pour chaque établissement et secteur d'activité. Aucun modèle n'est imposé. Ce document permet de recenser et de hiérarchiser l'ensemble des risques professionnels potentiels, lesquels peuvent engager la responsabilité du dirigeant concerné.

QUELLES OBLIGATIONS ET SANCTIONS ?

Si aucune sanction n'est prévue en cas d'absence de responsable sécurité, l'employeur d'une entreprise d'au moins 50 salariés se doit de présenter (article L4612-16 du code du travail), au moins une fois par an, au comité d'hygiène, de sécurité et des conditions de travail (CHSCT):

- Un rapport annuel écrit faisant le bilan de la situation générale de la santé, de la sécurité et des conditions de travail dans son établissement,
- Un programme annuel de prévention des risques professionnels et d'amélioration des conditions de travail.

En revanche, au regard des dispositions de l'article R4741-3 du code du travail, le fait de ***méconnaître les dispositions relatives aux documents et affichages obligatoires*** est puni de l'amende prévue pour les ***contraventions de la quatrième classe***, étant précisé que « l'amende est appliquée autant de fois qu'il y a de personnes employées dans des conditions susceptibles d'être sanctionnées au titre du présent article ».

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

La présence d'un responsable sécurité reste vivement conseillée:

- En cas de risque professionnel grave, www.Service-Public.fr (R17125) tient à disposition un formulaire à adresser dans les 15 jours à l'inspecteur du travail, en double exemplaire.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES PHYSIQUES SUR SITE
Les vols de matériels ou de matériaux

LE PRIX DE LA RÉDUCTION DES COÛTS

Dans un contexte de mondialisation des échanges, les entreprises cherchent de plus en plus à ***travailler en flux tendus, notamment pour réduire les coûts liés au stockage des marchandises***. Aussi, un simple vol de matériels ou de matériaux peut rapidement occasionner des difficultés de fonctionnement ou des retards de production pour les entités qui en sont victimes. Indépendamment des mesures qui seront prises en interne pour prévenir ces vols d'appropriation, une réflexion devra être réalisée en amont pour sécuriser l'ensemble de la chaîne logistique et identifier, par exemple, tous les acteurs de la chaîne d'approvisionnement.

VOLS SINGULIERS ET CONSÉQUENCES PLURIELLES

Les vols de matériels/matériaux peuvent avoir des répercussions plus ou moins graves sur la poursuite d'activité d'une entreprise. Si la première des ***conséquences*** reste de nature ***financière,*** le ***risque image*** (atteinte à la réputation de l'entreprise et perte de confiance) se révèle plus difficile à déterminer. Il ne doit en aucun cas être minimisé.

Du gardiennage privé vers des solutions techniques de traçabilité

Si le gardiennage privé apporte des réponses concrètes à la prévention des vols de matériels/matériaux, certains entrepreneurs ou coopératives agricoles se trouvent parfois démunis lorsque le vol concerne par exemple des dizaines de tonnes de Colza. Confrontée à un risque similaire, une exploitation ostréicole vendéenne a fait le choix de recourir à un dispositif technologique visant à dissimuler des « huitres en polyéthylène haute densité connectées » dans ses parcs à huitres, avec l'intention ferme de ne pas laisser les voleurs tracer la route !

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

EXPORTER MAIS PAS N'IMPORTE COMMENT !

Le statut d'opérateur économique agréé

Pour les entreprises qui sont plus particulièrement tournées vers l'exportation, l'obtention du statut d'opérateur économique agréé (OEA) participe dans une certaine mesure à la ***sécurisation de la chaîne logistique***. Ce label de confiance contribue à une certaine reconnaissance sur la scène internationale et facilite les échanges avec les services des douanes chargés de les délivrer.

3 types d'autorisation d'opérateur économique agréé peuvent être délivrées par les douanes françaises:

- L'autorisation OEA « Simplifications douanières » (« OEA C »),
- L'autorisation OEA « Sécurité et Sûreté » (« OEA-S »),
- L'autorisation combinée d'OEA « Simplifications douanières + Sécurité et Sûreté » (« OEA-F »).

Pour plus d'information sur ce label, se rendre sur le site web http://douane.gouv.fr/.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour prévenir les vols de matériels ou de matériaux, vous pouvez:

- Prendre connaissance de la fiche intitulée « Sécuriser ses flux de marchandise », mise à disposition par le service de l'information stratégique et de la sécurité économiques (SISSE) sur le site de la direction générale des entreprises (DGE) à l'adresse suivante: www.entreprises.gouv.fr
- Vous assurer de la bonne tenue de vos transactions en signant des « Incoterms ». Des explications précises vous sont fournies sur le site www.douane.gouv.fr
- Faire appel à un référent sûreté. La gendarmerie vous en présente le dispositif sur son site. De nombreuses ressources sont disponibles sur le site www.referentsurete.fr
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES PHYSIQUES SUR SITE
La zone à régime restrictif (ZRR)

PROTÉGER LE POTENTIEL SCIENTIFIQUE ET TECHNIQUE

La ZRR est une zone à accès réglementé qui s'inscrit dans le cadre de la **protection du potentiel scientifique et technique** (PPST) de la Nation. Les biens matériels et immatériels qui s'y trouvent favorisent les activités scientifiques de recherche fondamentale ou appliquée utiles au développement technologique de la nation Toute captation ou détournement pourrait:

- Porter atteinte aux intérêts économiques de la nation,
- Renforcer les arsenaux militaires étrangers ou affaiblir les capacités de défense et de sécurité nationale,
- Contribuer à la prolifération des armes de destruction massive et de leurs vecteurs,
- Être utilisé à des fins terroristes sur le territoire national ou à l'étranger.

COMMENT DEMANDER LA CRÉATION D'UNE ZRR ?

La ZRR est créée par arrêté du ministre de tutelle de l'établissement qui en fait la demande. Chaque responsable doit donc prendre l'attache avec le haut-fonctionnaire de défense et de sécurité (HFDS) de ce ministère en vue de déterminer l'utilité de créer une ZRR. Si la décision de création est effectivement prise, il doit alors:

- Envoyer au ministère de tutelle un dossier de demande formelle,
- Les modalités pratiques diffèrent selon les ministères,
- Il existe six ministères référents (Ecologie, Recherche, Economie, Santé, Défense, Agriculture).

L'arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation précise dans son annexe II la liste des secteurs scientifiques et techniques à protéger. Ceux-ci sont identifiés par un nombre.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

L'ACCÈS À UNE ZRR ET LE DEVOIR D'INFORMATION

Tout accès physique ou virtuel à une ZRR est soumis à ***autorisation du chef de l'établissement après avis du ministre***. Tout document ou répertoire informatique présent au sein de la ZRR ne peut être consulté que par une personne dûment habilitée. Tout recrutement (CDD, CDI, intérimaires), toute activité de recherche, tout prestataire, est soumis à une autorisation d'accès avec avis du ministre de tutelle. Chaque personnel doit être informé du statut de création d'une ZRR, des règles qui la régissent, et des sanctions pénales encourues par un contrevenant.

QUID DE LA SIMPLE VISITE ?

Une visite se caractérise par son aspect temporaire et par l'absence de participation aux activités scientifiques et techniques de la ZRR. Elle est soumise à la seule ***autorisation du chef d'établissement***.

QUELLES OBLIGATIONS POUR LE CHEF D'ÉTABLISSEMENT ?

La réglementation oblige le responsable du site implanté au sein d'une ZRR à informer le haut fonctionnaire de défense et de sécurité de son ministère de tutelle de tous projets de séminaires, congrès, conférences, etc.

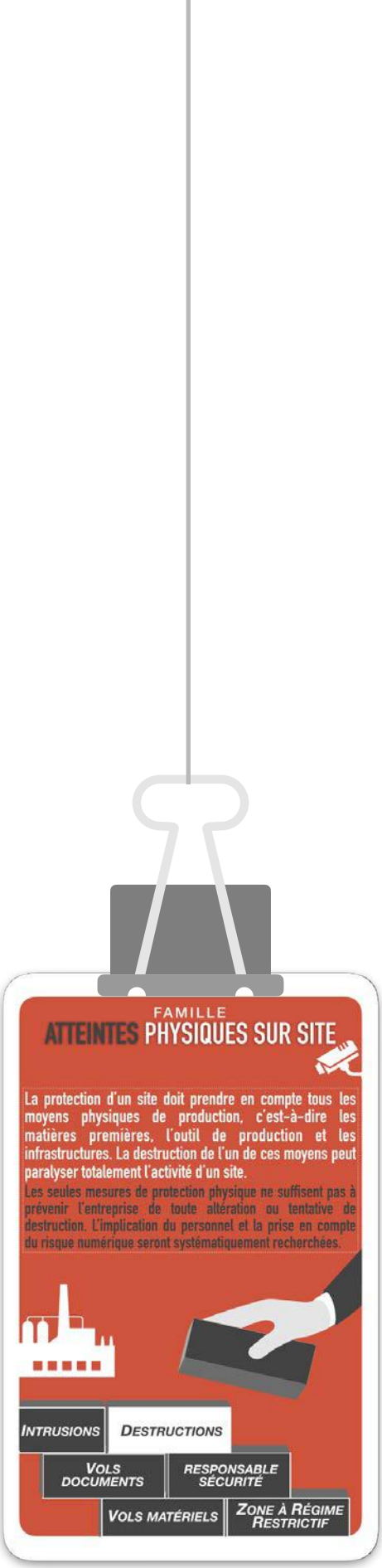
- La coopération avec un partenaire étranger doit faire l'objet d'un avis conforme du HFDS.
- Le règlement intérieur de l'établissement doit être en conformité avec la réglementation de la ZRR.

QUELLES SANCTIONS PÉNALES ?

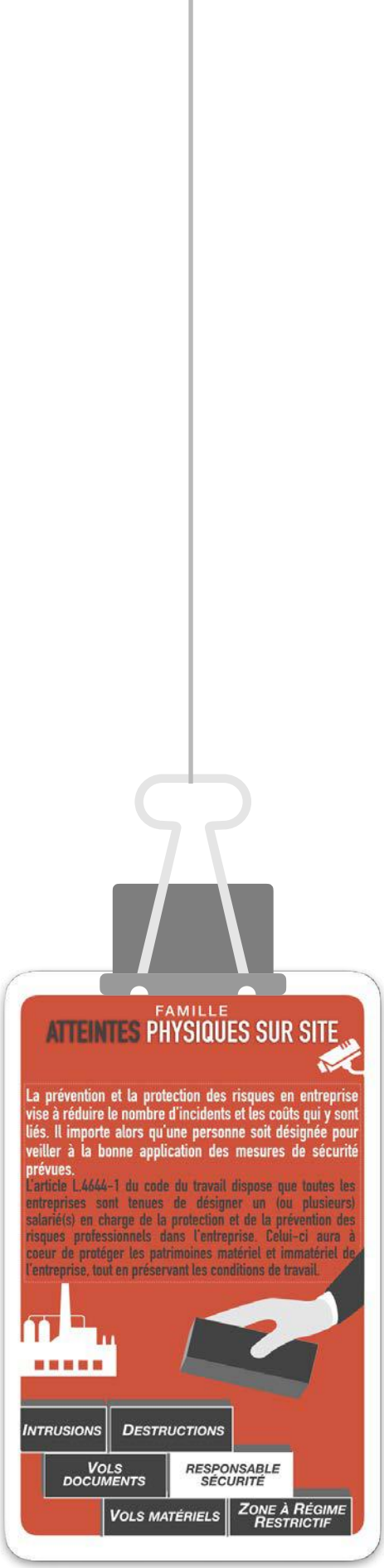
En toutes circonstances, il est crucial de porter une attention particulière aux faits survenus ou infractions commises au sein de la ZRR et d'informer sans délai la brigade de gendarmerie ou le commissariat de police le plus proche.

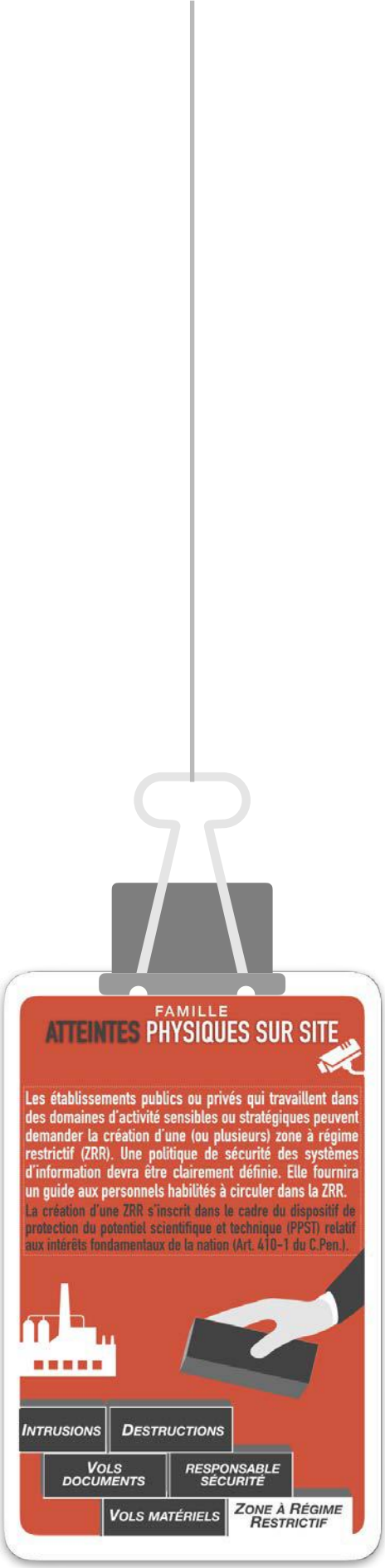
- Pénétrer sans autorisation dans une ZRR est punie d'une peine de ***6 mois d'emprisonnement et de 7.500 € d'amende*** (art.413-7 du code pénal),
- L'atteinte aux intérêts fondamentaux de la nation est punie de ***15 ans de réclusion criminelle et de 225.000 € d'amende*** (art. 411-9 du code pénal).
- Lorsqu'il est commis dans le but de servir les intérêts d'une puissance étrangère, d'une entreprise ou organisation étrangère ou sous contrôle étranger, le même fait est puni de ***20 ans de détention criminelle et de 300 000 euros d'amende*** (art. 411-9 du code pénal).
- Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) assure le pilotage du dispositif PPST et valide tout projet de création de ZRR. Un circulaire du 7 novembre 2012 en précise les modalités de mise en oeuvre.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT



Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT





Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILISATIONS/DÉSORGANISATIONS D'ENTREPRISE
Le parasitisme

TIRER PROFIT DES EFFORTS D'AUTRUI

Le « parasitisme », ou « agissements parasitaires » est une notion qui s'est construite et affirmée progressivement par le biais de la jurisprudence. Un arrêt de la Cour de Cassation de 1999 définit le parasitisme comme étant ***« l'ensemble des comportements par lesquels un agent économique s'immisce dans le sillage d'un autre afin de tirer profit, sans rien dépenser, de ses efforts et de son savoir-faire ».***

L'action de parasitisme profite donc à son auteur, en ce sens qu'elle lui procure un avantage concurrentiel, fruit d'un savoir-faire, d'un travail intellectuel et d'investissements.

D'une manière générale, trois conditions principales et cumulatives doivent être réunies:

- Existence d'une faute;
- Existence d'un dommage préjudiciable;
- Existence d'un lien de causalité entre la faute et le dommage.

QUELLE DIFFÉRENCE ENTRE CONTREFAÇON ET PARASITISME ?

Dans la pratique, il est relativement fréquent de voir un plaignant ester en justice en se fondant sur les actions cumulées de parasitisme et de contrefaçon, dans la mesure où l'on reproche au mis en cause de tirer indûment profit des investissements financiers ou intellectuels d'un autre. La notion de « copie d'oeuvre originale » est généralement apparente. Pour autant, les deux notions sont distinctes et méritent quelques précisions.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

L'action en contrefaçon est régie par les dispositions du Code de la propriété intellectuelle et suppose que le plaignant dispose d'un droit privatif sur une création originale ou un signe distinctif. L'existence d'une faute n'est pas nécessaire. L'exercice d'un droit de propriété suffit à agir.

L'action en justice pour parasitisme relève du droit de la concurrence. Le plaignant doit mettre en évidence des abus liés à des agissements déloyaux et se fondera sur l'article 1240 du Code civil pour faire valoir des dommages et intérêts. La logique est donc différente. Plaignant et mise en cause ne sont pas nécessairement concurrents.

UN EXEMPLE DE PARASITISME

Utilisation d'un personnage publicitaire ressemblant fortement à un personnage de film.
Dans une affaire datant de 2004, la société éditrice d'un film publicitaire avait été confondue pour des agissements parasitaires et condamnée à payer des dommages et intérêts à la société productrice d'un film de cinéma.

Le film publicitaire s'était appuyé, sans autorisation, sur la notoriété du film (notamment l'actrice dans une tenue qui rappelle celle de son personnage) pour créer une filiation entre le produit, objet de la campagne publicitaire, et cette œuvre cinématographique. Si le parasitisme a pu être établi, il n'y a pas eu lieu de démontrer une situation concurrentielle entre les parties prenantes.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous pensez être victime d'agissements parasitaires, vous devez:

- Solliciter rapidement les services d'un avocat qui vous aidera à matérialiser au mieux l'acte de concurrence déloyale dont vous êtes victime, ainsi que la nature de votre préjudice,
- Vous rapprocher du tribunal de grande instance pour un contentieux avec un salarié ou le tribunal de commerce si le contentieux vous oppose à un autre commerçant,
- Garder à l'esprit que le délai de prescription est de 5 ans, ce délai commençant à courir à compter du jour où les faits de concurrence déloyale ont pris fin (article 2224 du code civil).
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILISATIONS/DÉSORGANISATIONS D'ENTREPRISE
La débauche de personnel

UNE NOTION DE RUPTURE ABUSIVE

Le débauchage ou débauche de personnel qualifie l'action d'un salarié qui rompt abusivement le contrat qui le lie à son employeur pour accepter d'être engagé par une entreprise concurrente. Ainsi, au regard des dispositions de l'article L1237-3 du code du travail, «[..]le nouvel employeur est solidairement responsable du dommage causé à l'employeur précédent». Pour cela, il faudra nécessairement démontrer:

- Qu'il est intervenu dans la rupture,
- Qu'il a embauché un travailleur qu'il savait déjà lié par un contrat de travail,
- Qu'il a continué à occuper un travailleur après avoir appris que ce travailleur était encore lié à un autre employeur par un contrat de travail.

UN ACTE DE CONCURRENCE DÉLOYALE À MATÉRIALISER

Par principe, le fait qu'une entreprise débauche le personnel d'un de ses concurrents ne suffit pas pour constituer en soi un acte de concurrence déloyale. Pour qu'une faute soit matérialisée, il importe donc de mettre en évidence, par exemple, la ***désorganisation du fonctionnement de l'entreprise*** dite victime. La matérialisation d'une perturbation ou d'un simple déplacement de clientèle ne suffira donc pas.

Par ailleurs, le débauchage d'employé pourra, dans de très nombreux cas, être considéré comme licite si son contrat de travail ne fait référence à aucune ***clause de non-concurrence***, même si au demeurant, le transfert de l'employé conduit à un déplacement de clientèle. Pour réduire le risque de concurrence déloyale, l'employeur peut aussi faire le choix de s'accorder avec ses contractants sur une ***clause de non-sollicitation***. Ces deux notions sont précisées ci-après.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

EXISTENCE DE CLAUSES RESTRICTIVES

La clause de non-concurrence

Ce type de clause impose à l'employé de ne pas faire concurrence à son employeur une fois qu'il aura quitté l'entreprise. Toutefois, 4 conditions doivent être remplies sous peine de nullité, à savoir:

- La clause doit être justifiée par les intérêts légitimes de l'entreprise,
- La clause doit être limitée dans le temps et l'espace,
- La clause doit comporter une contrepartie financière,
- La clause doit tenir compte des spécificités de l'emploi du salarié et de la possibilité pour ce dernier de retrouver un emploi.

Ces éléments sont rappelés de manière générale par l'article L120-2 du code du travail et de façon plus exhaustive par une jurisprudence de 2002 de la chambre sociale de la Cour de Cassation.

La clause de non-sollicitation de personnel

Par ce type de clause, le contractant d'une entreprise s'engage vis-à-vis de cette dernière à ne pas solliciter ou embaucher les salariés ou collaborateurs de son cocontractant. Reposant sur un régime moins restrictif que celui de la clause de non-concurrence, la clause de non-sollicitation de personnel participe dans une certaine mesure à prévenir les velléités de débauchage du personnel.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous pensez être victime d'un débauchage de personnel, vous devez:

- Solliciter rapidement les services d'un avocat qui vous aidera à matérialiser au mieux l'acte de concurrence déloyale dont vous êtes victime, ainsi que la nature de votre préjudice,
- Vous rapprocher du tribunal de grande instance pour un contentieux avec un salarié ou le tribunal de commerce si le contentieux vous oppose à un autre commerçant,
- Garder à l'esprit que le délai de prescription est de 5 ans, ce délai commençant à courir à compter du jour où les faits de concurrence déloyale ont pris fin (article 2224 du code civil).
- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILISATIONS/DÉSORGANISATIONS D'ENTREPRISE
Le détournement de clientèle

UNE ENTORSE AU DEVOIR DE LOYAUTÉ

L'employé d'une entreprise est en principe tenu par un contrat de travail qu'il se doit d'exécuter de bonne foi (article L1222-1 du code du travail), ce qui traduit un devoir de fidélité vis-à-vis de son employeur.

Ainsi, lorsque qu'un acte contraire à l'intérêt de l'entreprise est régulièrement constaté, il peut révéler une faute.

Le détournement de clientèle en constitue un exemple concret qui se caractérise par le fait d'un ***employé qui détourne un client de son employeur à son profit ou celui d'une société concurrente dans laquelle il a des intérêts***.

Le détournement de clientèle devra mettre en évidence la volonté de nuire de son auteur, et la violation de son obligation de fidélité. Cet acte de concurrence déloyale l'expose au paiement de dommages et intérêts (Article 1240 du code civil).

DÉPLACEMENT ET DÉTOURNEMENT DE CLIENTÈLE

En l'absence de clauses restrictives dans son contrat, un employé reste libre d'aller travailler chez un concurrent de son ancien employeur. Ce dernier ne disposant pas d'un droit privatif sur ses clients, la jurisprudence admet que le départ du salarié puisse entraîner un ***déplacement de clientèle non fautif***, en ce sens qu'***aucun procédé déloyal*** n'a pu être matérialisé.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

DIVERS MODES OPÉRATOIRES

Détournement par démarchage

La sollicitation de clientèle par un ancien employé reste licite tant qu'aucun acte déloyal n'est commis dans le processus, tel que le dénigrement de son ancien employeur.

Détournement de fichiers

Un détournement de clientèle peut survenir par un détournement de fichiers de la part d'un ancien employé. Tout détournement n'est pas forcément illicite, sauf à considérer la mise en oeuvre d'un procédé déloyal. Le cas échéant, le salarié fautif pourra être mis en cause pour abus de confiance (article 314-1 du code pénal) et concurrence déloyale.

Détournement de commande

Un détournement de clientèle peut également survenir sous la forme d'un détournement de commande. En effet, ce cas de figure se déroule lorsqu'un fournisseur se rapproche directement du client sans passer par l'intermédiaire qu'il est censé solliciter.

Détournement par confusion

Ce type de détournement vise à capter la clientèle en créant la confusion dans l'esprit du client en utilisant notamment les signes distinctifs de l'entreprise (logos et autres emblèmes).

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous pensez être victime d'un détournement de clientèle, vous devez:

- Solliciter rapidement les services d'un avocat qui vous aidera à matérialiser au mieux l'acte de concurrence déloyale dont vous êtes victime, ainsi que la nature de votre préjudice,
- Vous rapprocher du tribunal de grande instance pour un contentieux avec un salarié ou le tribunal de commerce si le contentieux vous oppose à un autre commerçant,
- Garder à l'esprit que le délai de prescription est de 5 ans, ce délai commençant à courir à compter du jour où les faits de concurrence déloyale ont pris fin (article 2224 du code civil).
- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILISATIONS/DÉSORGANISATIONS D'ENTREPRISE
La confusion

CRÉER LE DOUTE DANS L'ESPRIT DU CLIENT

Dans un contexte d'***hyper compétition*** entre les entreprises, voire de « ***coopétition*** » (terme bien connu en intelligence économique pour qualifier des alliances « gagnantes-gagnantes » entre concurrents), il n'est pas rare d'observer des manoeuvres pour le moins frauduleuses, lesquelles ne sont pas toujours réprimées par le droit pénal.

La confusion constitue ainsi une ***pratique anticoncurrentielle*** qui expose son auteur à une action en concurrence déloyale et au paiement de dommages et intérêts au profit de l'entité qui en est victime.

La confusion peut par exemple naître de l'***imitation d'un nom commercial, d'une marque ou d'une publicité***. Cette imitation aura pour objectif de créer un certain ***doute dans l'esprit du public***, en vue de détourner, dans une certaine mesure, la clientèle d'un concurrent.

DES FAITS CONSTITUTIFS DE CONCURRENCE DÉLOYALE

Fondée sur les dispositions de l'article 1240 du code civil, l'action en concurrence déloyale impose de manière générale, et comme en matière de parasitisme ou de dénigrement, que trois conditions principales et cumulatives soient réunies:

- Existence d'une faute;
- Existence d'un dommage préjudiciable;
- Existence d'un lien de causalité entre la faute et le dommage.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

CONFUSION ET CONTREFAÇON: DES NOTIONS DISTINCTES

L'action en contrefaçon est régie par les dispositions de l'article L716-1 du code de la propriété intellectuelle et suppose que le plaignant dispose d'un droit privatif sur une création originale ou un signe distinctif.

- L'existence d'une faute n'est pas nécessaire.
- L'exercice d'un droit de propriété suffit à agir et rappelons à ce titre que l'article L713-3 du code de la propriété intellectuelle évoque le risque de confusion.

L'action en concurrence déloyale pour confusion se révèle sensiblement distincte, en ce sens qu'il s'agit de prouver le comportement fautif de son concurrent et de mettre en évidence le préjudice subi, notamment la perte de clientèle.

- Précisons que le détournement de clientèle n'est pas répréhensible en soi, car il découle du principe de la libre concurrence.
- En revanche, tous les moyens ne peuvent être employés et le principe d'une concurrence loyale devra être recherché. La confusion dans l'esprit du public peut être relevée même en l'absence d'intention de nuire.
- Le cumul de ces deux notions demeure envisageable, sous réserve que la faute constitutive de concurrence déloyale soit distincte de la participation aux faits de contrefaçon.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous pensez être victime d'un acte de confusion, vous devez:

- Solliciter rapidement les services d'un avocat qui vous aidera à matérialiser au mieux l'acte de concurrence déloyale dont vous êtes victime, ainsi que la nature de votre préjudice,
- Vous rapprocher du tribunal de grande instance pour un contentieux avec un salarié ou le tribunal de commerce si le contentieux vous oppose à un autre commerçant,
- Garder à l'esprit que le délai de prescription est de 5 ans, ce délai commençant à courir à compter du jour où les faits de concurrence déloyale ont pris fin (article 2224 du code civil).
- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILISATIONS/DÉSORGANISATIONS D'ENTREPRISE
Le dénigrement

JETER PUBLIQUEMENT LE DISCRÉDIT

Selon une jurisprudence bien établie, le dénigrement peut se définir comme étant le fait de « ***jeter publiquement le discrédit sur une personne, un produit ou un service identifié*** ».

Avec l'essor des médias sociaux, ces comportements se révèlent malheureusement de plus en plus fréquents. Bien que susceptibles de donner lieu à des poursuites judiciaires, les faits ne sont pas toujours faciles à déceler, notamment pour des petites structures ne disposant pas d'un service de veille.

PUBLICITÉ ET DÉVALORISATION DE L'IMAGE PUBLIQUE

Fondée sur les dispositions de l'article 1240 du code civil, l'action en concurrence déloyale impose de manière générale, et comme en matière de parasitisme ou de confusion, que trois conditions principales et cumulatives soient réunies:

- Existence d'une faute;
- Existence d'un dommage préjudiciable;
- Existence d'un lien de causalité entre la faute et le dommage.

Toutefois, s'agissant de dénigrement, le plaignant ***devra démontrer*** que cet acte a fait l'objet d'une ***certaine publicité*** et les propos employés sont ***de nature à dévaloriser son image*** auprès de la clientèle. Il importe, par ailleurs, que ***les propos du dénigrement visent une entreprise identifiable, sa marque ou ses produits***.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

DIFFAMATION ET PUBLICITÉ COMPARATIVE: DES NOTIONS DISTINCTES

La diffamation

La diffamation est l'allégation ou l'imputation d'un fait qui porte ***atteinte à l'honneur ou à la considération*** d'une personne. Le fait allégué doit être vérifiable, car à défaut il relèvera de l'injure.

Le dénigrement se distingue de la diffamation, car il émane d'un acteur économique qui cherche à bénéficier d'un avantage concurrentiel sur son concurrent. Par ailleurs, les faits de diffamation publique se prescrivent par 3 mois, alors que ce délai est porté à 5 ans pour le dénigrement.

La publicité comparative

Le dénigrement doit également être distingué de la publicité comparative, laquelle « ***met en comparaison des biens ou des services*** en utilisant soit la citation ou la représentation de la marque, de la raison ou dénomination sociale, du nom commercial ou de l'enseigne d'une entreprise concurrente, titulaire des droits de propriété intellectuelle ». Impliquant un ou plusieurs concurrent, elle demeure ***licite, sous réserve*** que des conditions cumulatives soit respectées:

- Publicité non trompeuse,
- Porter sur des biens ou services de même nature et répondant aux mêmes besoins,
- Comparaisons vérifiables, pertinentes et objectives.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous pensez être victime d'un dénigrement, vous devez:

- Solliciter rapidement les services d'un avocat qui vous aidera à matérialiser au mieux l'acte de concurrence déloyale dont vous êtes victime, ainsi que la nature de votre préjudice,
- Vous rapprocher du tribunal de grande instance pour un contentieux avec un salarié ou le tribunal de commerce si le contentieux vous oppose à un autre commerçant,
- Garder à l'esprit que le délai de prescription est de 5 ans, ce délai commençant à courir à compter du jour où les faits de concurrence déloyale ont pris fin (article 2224 du code civil).
- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILISATIONS/DÉSORGANISATIONS D'ENTREPRISE
La divulgation de savoir-faire

LE SECRET NE VAUT QUE S'IL EST PRÉSERVÉ

Le droit français ne donne pas de définition précise de la notion de savoir-faire mais il est communément admis que cette terminologie comprend l'***ensemble des informations techniques ou commerciales, non brevetées, qui procurent un avantage concurrentiel*** à une entreprise. Le savoir-faire ne permet pas à lui seul de se prévaloir d'un droit de propriété exclusif et opposable à tous.

La divulgation de savoir-faire constitue néanmoins un acte de concurrence déloyale qui expose son auteur à des dommages et intérêts sur le fondement des dispositions de l'article 1240 du code civil.

UNE PROTECTION EUROPÉENNE DES SAVOIR-FAIRE

Le 8 juin 2016, le parlement européen votait définitivement la « ***directive européenne sur la protection des savoir-faire et des informations commerciales non divulguées*** » mieux connue sous le vocable de « directive européenne sur le secret des affaires ».

La loi n°2018-670 du 30 juillet 2018, qui en constitue la transposition française, énonce que ***toute information peut-être protégée au titre du secret des affaires*** sous réserve:

- Qu'elle ne soit pas connue du grand public ou du secteur d'activité concerné,
- Qu'elle revête une valeur commerciale, effective ou potentielle, du fait de son caractère secret,
- Qu'elle fasse l'objet de la part de son détenteur légitime de mesures de protection raisonnables [..] pour en conserver le caractère secret.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

DIVULGATION LICITE OU ILLICITE

Les cas de divulgation licite

Les articles L151-7 à L151-9 du code du commerce énoncent les cas pour lesquels, la loi autorise la divulgation d'un savoir-faire, comme par exemple:

- Demandes émanant des autorités juridictionnelles ou administratives, et relatives à l'exercice des pouvoirs d'enquête, de contrôle, d'autorisation ou de sanction,
- Respect de la liberté de la presse, et de la liberté d'information telle que proclamée dans la Charte des droits fondamentaux de l'Union européenne,
- Révélation d'une activité illégale, d'une faute ou d'un comportement répréhensible, dans le but de protéger l'intérêt général et de bonne foi,
- Divulgation intervenue dans le cadre de l'exercice du droit à l'information et à la consultation des salariés ou de leurs représentants,

Les cas de divulgation illicite

Les articles L151-4 à L151-6 du code du commerce rappellent que d'une manière générale, l'obtention d'un secret des affaires est illicite lorsqu'elle est ***réalisée sans le consentement de son détenteur légitime*** et qu'elle résulte notamment:

- D'un accès non autorisé à tout document, substance, objet et autres fichiers,
- De tout autre comportement considéré comme contraire aux usages en matière commerciale.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous pensez être victime d'une divulgation de savoir-faire, vous devez:

- Solliciter rapidement les services d'un avocat qui vous aidera à matérialiser au mieux l'acte de concurrence déloyale dont vous êtes victime, ainsi que la nature de votre préjudice,
- Vous rapprocher du tribunal de grande instance pour un contentieux avec un salarié ou le tribunal de commerce si le contentieux vous oppose à un autre commerçant,
- Garder à l'esprit que les actions relatives à une atteinte au secret des affaires sont prescrites par cinq ans à compter des faits qui en sont la cause (article L152-2 du code du commerce).
- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.

Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES AUX SAVOIR-FAIRE
La perte de compétence clé

L'HUMAIN SINON RIEN !

L'humain représente sans nul doute la ressource la plus importante de l'entreprise. Sans lui, sans ses idées, sans ses connaissances, sans ses savoir-faire, aucune activité n'est possible ! ***Lorsque certaines compétences, rares ou fondamentales dans l'activité de l'entreprise, se trouvent concentrées entre les mains d'une seule personne*** ou de quelques uns, leur départ peut avoir des conséquences graves pour l'entreprise, voire remettre en cause tout un pan de son activité. Il convient donc de se prémunir de la perte d'une compétence clé. On estime que près de 15 % les PME transmises suite au décès de son dirigeant font faillite.

IDENTIFIER ET CONSERVER LES COMPÉTENCES CLÉS

Les savoir-faire particuliers doivent faire l'objet d'une identification précise dans l'entreprise:

- Quel est le savoir technique ?
- Où se trouvent les expertises ?
- Y-a-il des responsabilités uniques ?

Ensuite, il conviendra d'adapter la politique des ressources humaines de l'entreprise pour:

- Anticiper les départs liés au « *turn over* » *naturel*,
- Fidéliser les personnes détenant les compétences clés pour l'entreprise (salaire, intéressement, reconnaissance, etc.).
- Veiller à ce que les différentes fonctions et missions de l'entreprise ne soient pas trop cloisonnées.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

UN EXEMPLE DE PERTE DE COMPÉTENCE CLÉ

Quand la démission remet en cause l'existence d'une start-up !

Une start-up spécialisée dans les services en ligne, suite à la démission de son directeur, a vu son chiffre d'affaires réduire de plus de 50 % en six mois. Cette démission a mis en péril le projet d'entrée en bourse de la start-up. Le directeur détenait à la fois une responsabilité unique et un savoir-faire précis.

Sur un plan juridique

La gestion d'une compétence clé implique de formaliser les risques liés à celle-ci dans les contrats de travail, en y incluant, le cas échéant, des clauses de confidentialité ou des clauses de non-concurrence.

Il est également possible pour l'entreprise de souscrire une ***assurance homme-clé*** pour certaines compétences rares. Celle-ci couvre généralement la perte d'exploitation, le remboursement de certains prêts bancaires et les frais de réorganisation.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour vous prémunir de la perte d'une compétence clé, vous pouvez:

- Encadrer contractuellement l'activité de cette personne pour limiter les vulnérabilités,
- Préparer la redistribution des tâches et projets menés par l'éventuel partant vers d'autres salariés,
- En matière de gestion des ressources humaines, disposer d'un panel de candidats potentiels, susceptibles de compenser, ne serait-ce que partiellement, son départ.
- Dans de rares cas, la perte d'une compétence clé peut vous empêcher de poursuivre votre activité. La cessation temporaire d'activité peut constituer une solution provisoire. Le site www.Service-Public-Pro.fr (F32703) vous accompagne dans cette démarche.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES AUX SAVOIR-FAIRE
La captation de brevet

LE BREVET: UN MONOPOLE D'EXPLOITATION

Le brevet est une solution technique à un problème technique qui doit, pour être délivré par l'Etat:

- faire apparaitre une ***nouveauté,***
- impliquer une ***activité inventive,***
- être ***susceptible d'application industrielle***.

Le brevet permet surtout de rentabiliser des investissements de recherche parfois lourds. Il crée enfin les conditions d'un ***avantage compétitif stratégique*** pour l'entreprise, en ce sens qu'il lui procure un monopole d'exploitation.

L'espace professionnel du site www.Service-public-Pro.fr met à la disposition de tous une fiche pratique (F23626) sur le dépôt de brevet et liste de manière particulièrement exhaustive les ***formulaires et services en ligne utiles***.

En France, l'institut national de la propriété industrielle (INPI) est l'organisme public en charge des questions de propriété industrielle.

LA CAPTATION DE BREVET: UN RISQUE MAJEUR POUR L'ENTREPRISE

Le brevet déposé à l'INPI fait partie des actifs de l'entreprise. S'il fournit un ***droit de propriété*** à son titulaire, il lui permet également d'***interdire toute exploitation*** (utilisation, fabrication, importation...) ***de son invention*** effectuée sans son autorisation et ce ***pendant*** une durée maximale de ***20 ans***. Ainsi, afin de contourner ces blocages, certaines entreprises concurrentes n'hésitent pas à utiliser des moyens détournés pour s'approprier ces droits de propriété industrielle. Le rachat d'entreprise et certains contrats n'en constituent que quelques exemples.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Captation de brevet: le rachat d'entreprise.

L'INPI rappelle sur son site www.inpi.fr qu'à la fermeture de l'entreprise, différents événements affectant la vie du brevet peuvent se produire (cession du brevet, liquidation judiciaire de l'entreprise…). Certains investisseurs étrangers ont rapidement compris que le rachat d'entreprise pouvait leur fournir le moyen de rattraper un retard technologique dans le domaine concerné.

Captation de brevet: vigilance dans la signature des contrats !

Soucieux d'obtenir ou de maintenir un avantage concurrentiel, la plupart des chefs d'entreprise ont désormais acquis le réflexe du dépôt d'une demande de brevet lorsque la situation le justifie. Mais peu ou mal conseillé, le titulaire d'un droit de propriété industrielle peut très vite se faire déposséder en manquant de vigilance sur l'acceptation de ***clauses de propriété industrielle*** présentes dans des contrats de recherche ou de co-développement ou l'acceptation d'un ***accord de confidentialité*** prévoyant l'utilisation ***« à sa guise et sans contrepartie »*** d'un brevet.

Captation de brevet: les transferts de technologie.

L'accès ou le maintien dans un marché concurrentiel impose de consentir des transferts de technologie (***vendre par contrat, à un acquéreur, les droits d'utilisation d'une technique, d'un procédé ou d'un produit dont on est propriétaire***). Dans un rapport au parlement de 2018 sur les exportations d'armement, il est rappelé que ces concessions sont devenues nécessaires pour l'industrie de défense, et que la France ne fait que s'adapter à la demande.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour diminuer votre exposition au risque de captation de brevet, vous devez:

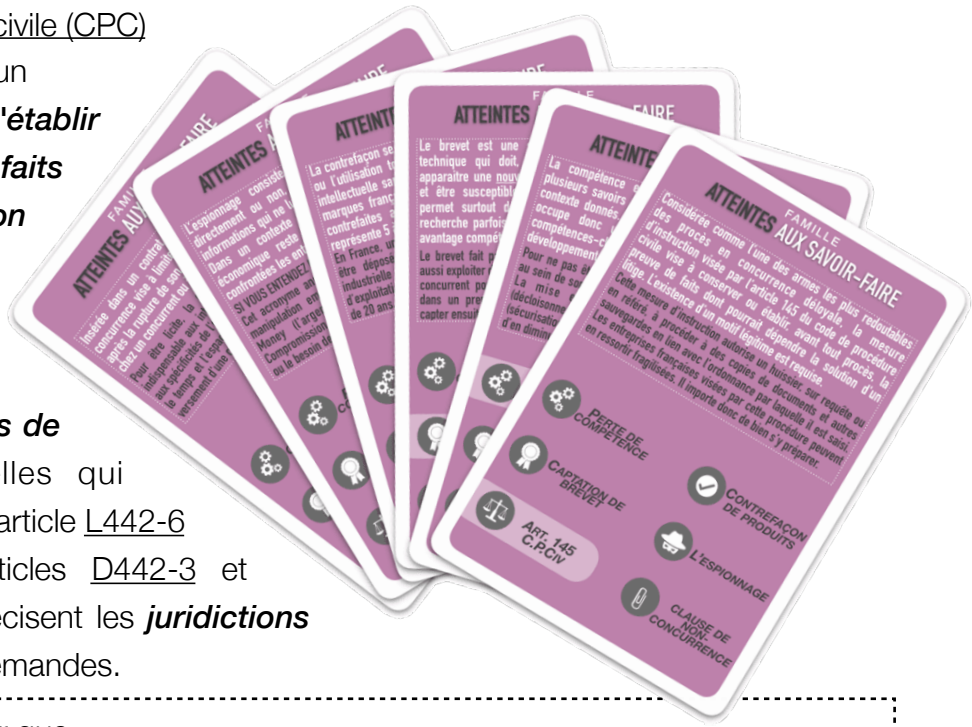
- Solliciter les conseils juridiques d'un avocat spécialisé avant toute signature de contrat,
- Suivre les conseils du SISSE pour protéger son savoir et ses idées sur www.entreprises.gouv.fr,
- Mettre en place une veille pour détecter et se prémunir des contrefaçons,
- L'article L615-1 du code de la propriété intellectuelle dispose que « Toute atteinte portée aux droits du propriétaire du brevet, tels qu'ils sont définis aux articles L. 613-3 à L. 613-6, constitue une contrefaçon ».
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES AUX SAVOIR-FAIRE
L'article 145 du code de procédure civile

PROUVER LES FAITS DE CONCURRENCE DÉLOYALE

L'article 145 du code de procédure civile (CPC) peut être mis en oeuvre « S'il existe un ***motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige*** […]».



Les litiges concernés font référence à des ***pratiques anticoncurrentielles ou restrictives de concurrence***, c'est à dire celles qui méconnaissent les dispositions de l'article L442-6 du code du commerce. Les articles D442-3 et R420-3 du code du commerce précisent les ***juridictions compétentes pour instruire*** ces demandes.

Par ailleurs, il est important de retenir que:

- Cette procédure est une ***mesure d'instruction dite « in futurum »,*** c'est-à-dire qu'elle doit être engagée avant toute procédure au fond portant sur les faits incriminés,
- La mesure repose sur l'existence d'une situation crédible pouvant engendrer un litige,
- La mesure sollicitée ne doit pas porter atteinte à la vie privée ou au secret des affaires de manière non justifiée,
- La sollicitation d'une telle mesure a pour effet de se prémunir du ***risque de disparition ou de destruction d'éléments de preuve***,
- Les mesures d'instruction […] peuvent être ordonnées à la ***demande de tout intéressé***,
- Les mesures d'instructions […] sont ordonnées ***sur requête ou en référé***,
- La Cour d'Appel de Paris est compétente pour connaître des décisions rendues.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

UNE VÉRITABLE ARME PROCÉDURALE

En matière de concurrence déloyale, la matérialisation des preuves constitue l'une des plus grandes difficultés rencontrées par chacun des adversaires. En agissant sur le fondement de l'article 145 du CPC, le demandeur est en mesure d'obtenir du juge la ***désignation d'un huissier de justice*** chargé de ***se déplacer dans les locaux ou le domicile de la personne visée*** afin de saisir tout document permettant d'***établir les faits allégués.***

Une procédure civile qui se distingue de la perquisition en droit pénal

Dans le cadre de la saisie du juge, le requérant doit s'efforcer de déterminer la nature des documents qu'il souhaite voir saisir par ***l'huissier de justice***, afin que ce dernier ***ne soit pas livré à lui-même*** dans la recherche de preuves. A défaut, le défendeur pourrait faire valoir que les conditions de recevabilité de la procédure ne sont pas réunies et faire suspendre le séquestre par la voie d'un référé-rétractation (Art 496 al 2 CPC).

Une procédure traumatisante pour celui qui la subit

Indépendamment de la saisie éventuelle d'éléments de preuve (numérique ou papier), l'intérêt majeur de cette procédure réside dans sa ***célérité et l'effet de surprise*** engagé. En effet, parce que non contradictoire, le défendeur ne sera informé de la mesure que lorsque l'huissier de justice se présentera à lui, accompagné du ou des experts dûment mandatés.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

S'il parait difficile d'anticiper une telle procédure, il convient de s'y préparer au mieux:

- En déterminant des procédures d'alerte en interne, destinées à désigner un responsable chargé d'encadrer le constat d'huissier en lien avec l'avocat de l'entreprise,
- En s'assurant de la légitimité de l'action engagée tant sur le fond que sur la forme,
- En suivant les conseils prodigués par le service de contre-ingérence économique de la DGSI dans le « Flash n°27 » en date d'octobre 2016, disponible sur le site www.entreprise.gouv.fr
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES AUX SAVOIR-FAIRE
La contrefaçon de produits

UN FLÉAU À L'ÉCHELLE MONDIALE

Selon les estimations, la contrefaçon représenterait 5 à 10 % du commerce mondial. Pour l'organisation de coopération et de développement économique (OCDE), le volume des échanges physiques de contrefaçon de produits de consommation dépasserait le produit intérieur brut (PIB) de 150 pays, pour une valeur globale de 250 milliards de dollars par an. La contrefaçon se définit comme la ***reproduction, l'imitation ou l'utilisation totale ou partielle d'un droit de propriété intellectuelle sans l'autorisation de son propriétaire***.

L'organisme public en charge de ces questions est l'INPI.

LA VIOLATION D'UN DROIT DE PROPRIÉTÉ INTELLECTUELLE

Si la contrefaçon constitue par essence une pratique anti-concurrentielle, elle se matérialise par des atteintes à la sécurité économique qui enfreignent des droits de propriété industrielle, littéraire ou artistique. D'une manière générale, on distingue quatre grands droits qui ont la particularité de conférer une protection territoriale (par pays) dont la durée peut être perpétuelle ou limitée:

- ***Droits des brevets d'invention*** (protection pour une durée qui ne peut excéder 20 ans),
- ***Droits d'auteurs et droits voisins*** (DADV) (protection pour une durée qui ne peut excéder 70 ans à compter de la mort de l'auteur),
- ***Droits des dessins et modèles*** (protection pour une durée qui ne peut excéder 25 ans)
- ***Droits des marques de fabrique*** (protection perpétuelle à compter de la demande d'enregistrement. En pratique, il s'agit d'un droit renouvelable tous les 10 ans, indéfiniment).

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

PLURALITÉ ET COMPLEXITÉ DES SANCTIONS

L'INPI rappelle dans une brochure dédiée à la contrefaçon, que cette thématique n'épargne aucun secteur économique, et qu'elle encourage par ailleurs les activités illicites et menace la santé et la sécurité des consommateurs. Un panel de sanctions a progressivement été mis en place par le législateur. Les domaines du droit pénal, du droit civil ou du droit fiscal sont notamment concernés.

Les sanctions pénales

Les contrefaçons constituent un délit pénal réprimé par les art. L335-2 (DADV), L343-1 (Bases de données), L521-4 (Dessins et modèles) et L615-14 (Brevets) du code de la propriété intellectuelle (CPI). Depuis la loi 2017-242 du 28/02/2017, le délai de prescription est porté à 6 ans.

Les sanctions civiles

L'action en contrefaçon peut être engagée en matière civile, devant le TGI compétent, par le titulaire des droits, en vue d'obtenir la réparation de son préjudice sur le fondement de l'article 1240 du code civil. L'action civile en contrefaçon se prescrit par 5 ans à compter des faits qui en sont la cause (article L521-3 du CPI).

Les sanctions douanières

La contrefaçon constitue également un délit douanier, les sanctions fiscales douanières se cumulant avec les sanctions pénales. Ces infractions résultent notamment de la combinaison des articles L. 716-9 et L. 716- 10 du CPI, 38, 414, 417 et 428 du code des douanes.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous pensez être victime d'actes de contrefaçon, vous devez:

- Solliciter les conseils juridiques (annuaire) d'un avocat spécialisé qui saura vous orienter sur la nature du contentieux à engager et vous inciter à collecter un maximum de preuves,
- Consulter les nombreuses brochures explicatives de l'INPI sur son site www.inpi.fr.
- Pour déposer plainte au pénal, vous rapprocher du service territorialement compétent,
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES AUX SAVOIR-FAIRE
L'espionnage industriel

LA QUÊTE D'INFORMATIONS STRATÉGIQUES

Défini aux articles 411-1 et suivants du code pénal, l'espionnage réprime de la manière la plus sévère ***« Le fait de livrer à une puissance étrangère, à une organisation étrangère ou sous contrôle étranger [..] des documents, matériels, équipements, etc. »***.

De nombreuses affaires à portée internationale ont mis en évidence l'existence de faits d'***espionnage industriel*** sans que la notion d'espionnage ne soit systématiquement retenue par les tribunaux judiciaires. La protection européenne du secret des affaires apporte une réponse nouvelle. Toutefois, ***la captation malveillante demeure, dans la plupart des cas, liée à des faiblesses humaines ou organisationnelles***. Quelle que soit la technique utilisée, c'est bien l'information stratégique de l'entreprise qui est visée.

METTRE EN OEUVRE L'ART DE LA TROMPERIE ET DE LA PERSUASION

L'art de la tromperie et de la persuasion ne fait qu'exploiter les faiblesses individuelles de chacun avec des conséquences parfois très dommageables pour l'entreprise, quand elles ne se révèlent pas irréversibles !

Avec « MICE », on ne va peut être pas vous manquer !

Cet acronyme anglo-saxon reprend les quatre leviers de la manipulation que sont l'argent (***Money***), l'adhésion à une cause (***Ideology***), le chantage (***Compromission***) et le besoin de reconnaissance (***Ego***).

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

PRÉSERVER LES INTÉRÊTS FONDAMENTAUX DE LA NATION

Définir les intérêts fondamentaux de la nation et sanctionner les atteintes

La divulgation d'informations portant atteinte aux intérêts fondamentaux de la nation est réprimée par 15 ans de détention criminelle et 225 000 euros d'amende (Article 411-6 du code pénal):

- Les intérêts fondamentaux comprennent le patrimoine culturel et le potentiel économique et scientifique de la France (Article 410-1 du code pénal),
- La protection du secret de la défense nationale est visé par l'article 413-9 du code pénal.

La protection du secret des affaires

Le 8 juin 2016, le parlement européen votait définitivement la « directive européenne sur la protection des savoir-faire et des informations commerciales non divulguées » mieux connue sous le vocable de « directive européenne sur le secret des affaires ».

La loi n°2018-670 du 30 juillet 2018, qui en constitue la transposition française, énonce que ***toute information peut-être protégée au titre du secret des affaires*** sous réserve:

- Qu'elle ne soit pas connue du grand public ou du secteur d'activité concerné,
- Qu'elle revête une valeur commerciale, effective ou potentielle, du fait de son caractère secret,
- Qu'elle fasse l'objet de la part de son détenteur légitime de mesures de protection raisonnables [..] pour en conserver le caractère secret.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

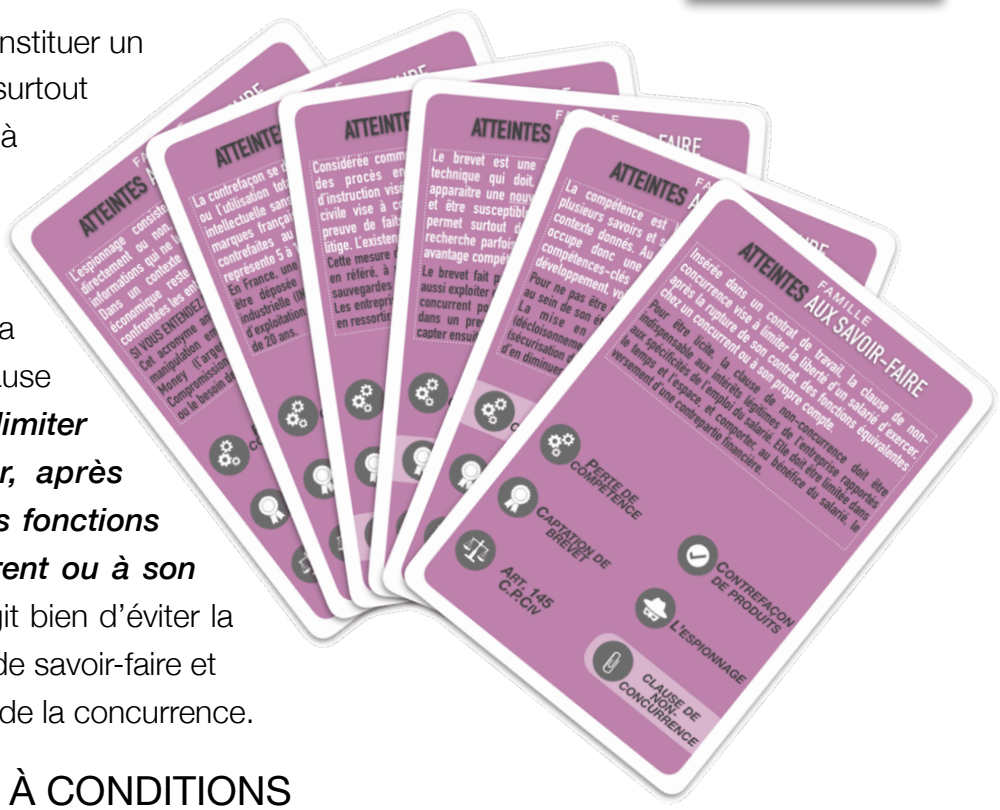
Pour diminuer l'exposition au risque d'espionnage industriel, vous devez:

- Mettre en place des ***protocoles de sécurité*** en interne et les faire respecter par les visiteurs et les salariés (ports de badge, parcours de notoriété, suivi des personnels temporaires, discrétion dans les déplacements, filtres de confidentialité sur les écrans de terminaux numériques, etc.)
- Suivre les conseils énoncés dans les ***fiches thématiques n°3*** et ***n°37*** du jeu des 8 familles.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES AUX SAVOIR-FAIRE
La clause de non-concurrence

LIMITER LA LIBERTÉ D'UN SALARIÉ



Le départ d'un employé peut constituer un risque majeur pour l'entreprise, surtout si celle-ci ne s'est pas préparée à cette éventualité. Des dispositions légales permettent d'insérer, dans le contrat de travail ou la convention collective, une clause de non-concurrence qui vise à ***limiter la liberté d'un salarié d'exercer, après la rupture de son contrat, des fonctions équivalentes chez un concurrent ou à son propre compte***. Au final, il s'agit bien d'éviter la double peine: celle d'une perte de savoir-faire et d'un renforcement concomitant de la concurrence.

UNE CLAUSE SOUMISE À CONDITIONS

Si ce type de clause impose à l'employé de ne pas faire concurrence à son employeur une fois qu'il aura quitté l'entreprise, quatre conditions doivent être toutefois remplies sous peine de nullité, à savoir:

- La clause doit être justifiée par les intérêts légitimes de l'entreprise,
- La clause doit être limitée dans le temps et l'espace,
- La clause doit comporter une contrepartie financière,
- La clause doit tenir compte des spécificités de l'emploi du salarié et de la possibilité pour ce dernier de retrouver un emploi.

Ces éléments sont rappelés de manière générale par l'article L120-2 du code du travail et de façon plus exhaustive par une jurisprudence de 2002 de la chambre sociale de la Cour de Cassation.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

INTÉRÊTS RÉCIPROQUES DU SALARIÉ ET DE L'EMPLOYEUR

Tout en offrant au salarié la liberté de quitter son entreprise, la clause de non concurrence garantit à l'employeur qu'un certain devoir de loyauté lui sera accordé sous conditions.

La clause de non-concurrence peut prendre effet:

- à la date effective du terme du contrat si un préavis est prévu,
- au départ du salarié en l'absence de tout préavis.

L'employeur peut-il renoncer à l'application de la clause de non-concurrence ?

- Oui, si le contrat ou une convention collective le prévoit.
- À défaut, l'employeur devra rechercher un accord avec le salarié.

Le non respect d'une clause de non-concurrence est-il sanctionnable ?

En cas de ***non respect de la clause par le salarié***, ce dernier pourra être amené à restituer la contrepartie financière qu'il a perçue. Si la situation le justifie, il pourra être sanctionné par un juge au versement de dommages-intérêts.

Si ***l'employeur fait défaut à son obligation de versement de l'indemnité*** compensatrice, le salarié n'est plus tenu de respecter la clause de non-concurrence. Comme pour le salarié, l'employeur pourra être sanctionné par un juge au versement de dommages-intérêts, si la situation le justifie.

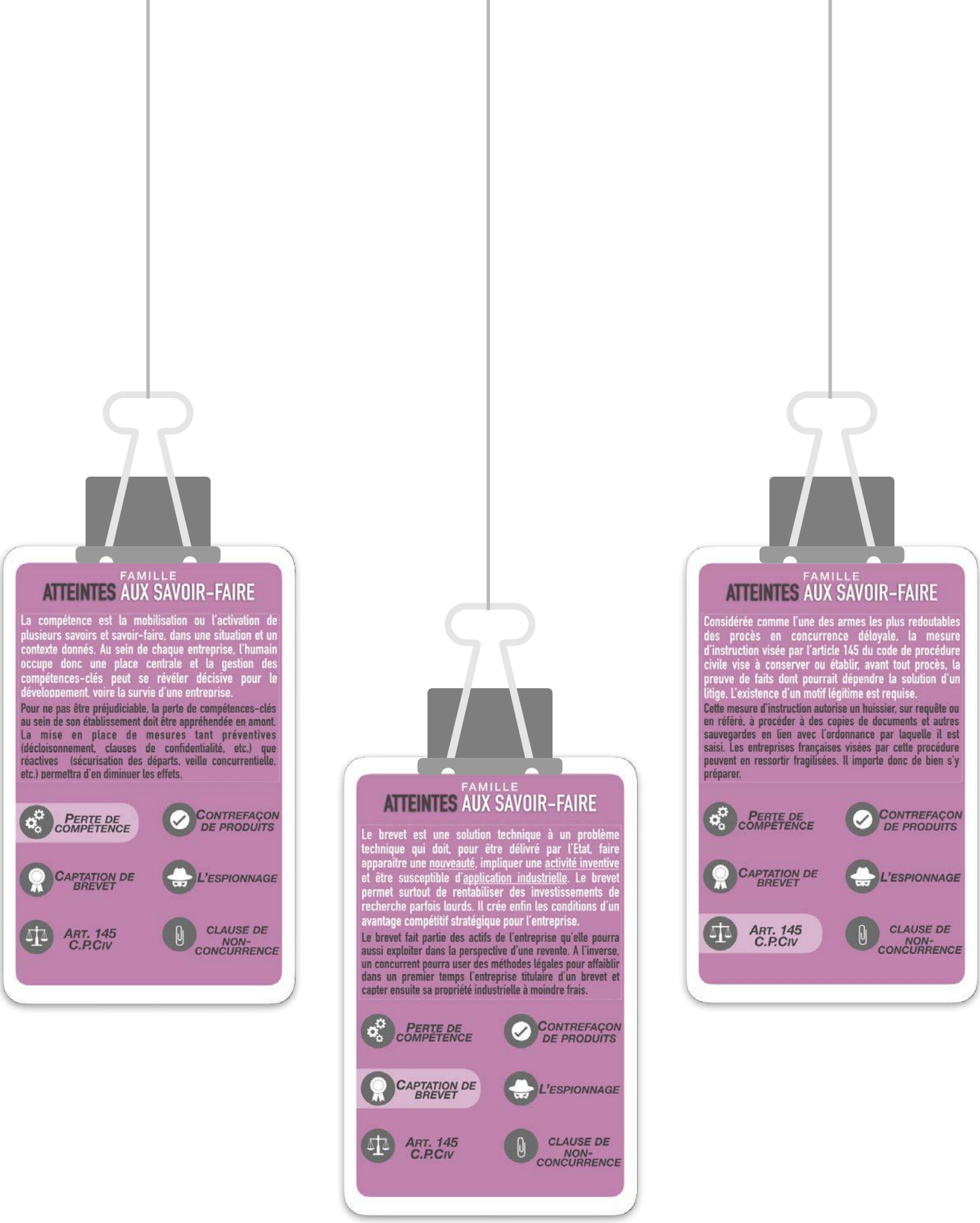
RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

La clause de non-concurrence ne constitue que l'un des moyens utiles à la préservation de savoir-faire:

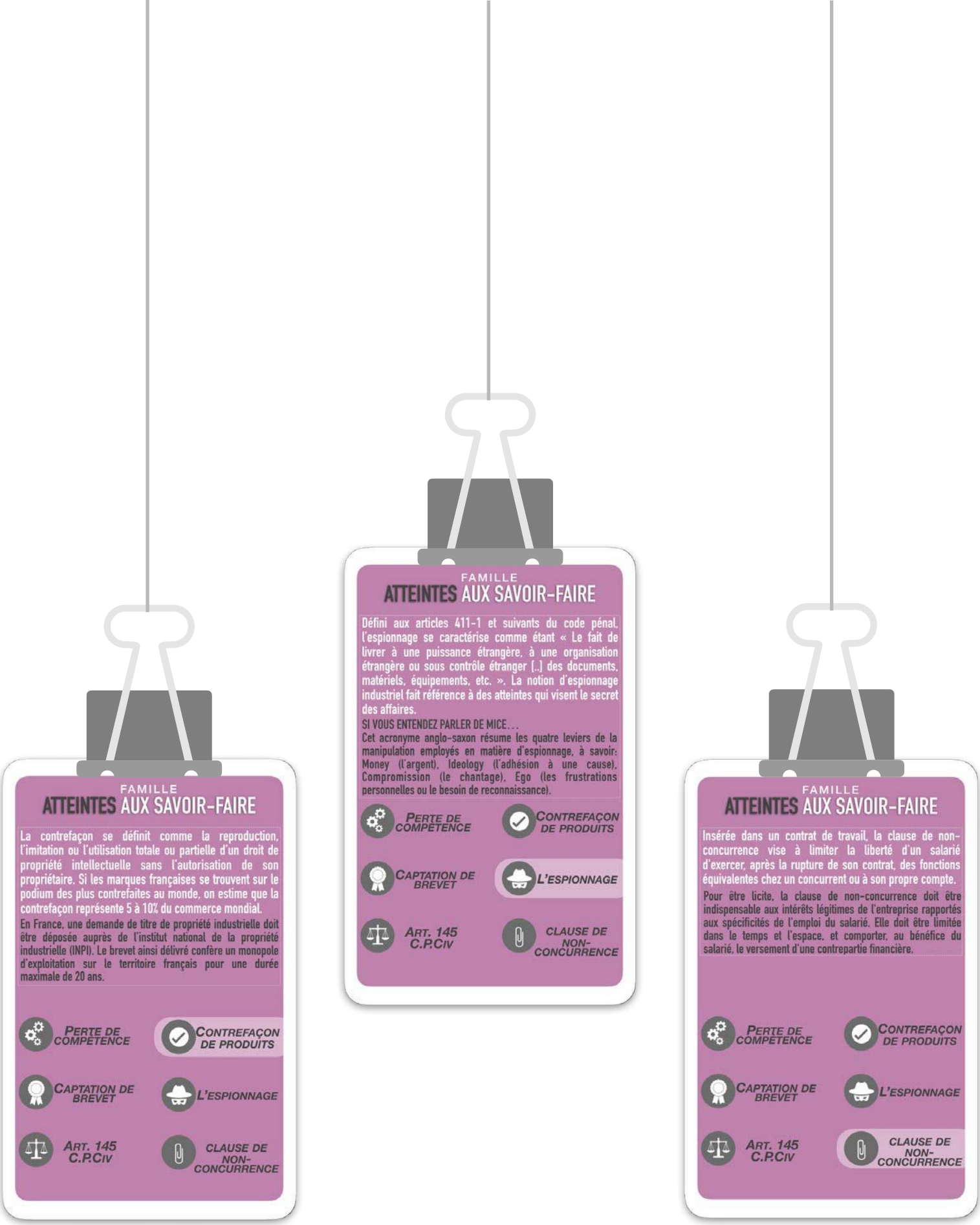
- Toutes les entreprises n'ont pas forcément les moyens de verser l'indemnité compensatrice,
- Le site www.Service-Public.fr (F1910) rappelle, plus en détail, les modalités de cette clause.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT



Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.

Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT



Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.

Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES INTRUSIONS CONSENTIES
Les conférences, salons et séminaires

DES LIEUX D'ÉCHANGES…ET DE PRÉDATION !

Les conférences, salons et autres séminaires sont très souvent considérés, à tort ou à raison, comme des ***évènements à haute valeur ajoutée***, en ce sens qu'ils ***participent au rayonnement de l'entreprise***, que ce soit en terme d'image, ou de valorisation des produits fabriqués et projets développés. Pour autant, bien qu'attractifs et indispensables à certaines activités, les conférences, salons et séminaires, constituent d'excellents ***vecteurs de captation d'informations stratégiques*** pour des personnes malintentionnées. Il apparait donc essentiel de mesurer les risques avant de se lancer.

PRENDRE CONSCIENCE DES RISQUES

La recherche de ressources financières s'avère cruciale pour le développement d'un projet d'entreprise. Soulever des fonds, conquérir de nouveaux marchés et satisfaire ses clients constituent autant de démarches indispensables à la survie d'une entreprise. Mais dans un marché hyper concurrentiel où les manoeuvres les plus offensives sont parfois observées, prendre le temps de la réflexion rime toujours avec sage décision.

- Conférence ou séminaire, êtes-vous certain de ne pas trop en dévoiler ? Êtes-vous sûr d'identifier toutes les personnes de votre auditoire ?
- Vous évoquez un projet novateur, les informations dévoilées ont-elles un caractère stratégique ? Si oui, ces informations ont-elles fait l'objet d'une démarche de protection ?
- Se poser les bonnes questions, c'est déjà commencer à se protéger !
- Le SISSE met à disposition, sur son site, deux guides destinés à la ***mobilité internationale des scientifiques*** à travers certains principes directeurs et un vade-mecum.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour aborder les conférences, salons et séminaires en toute sécurité, vous pouvez:

Avant l'évènement:

- Organiser en amont l'évènement en sélectionnant les informations susceptibles d'être diffusées, de façon à ne pas compromettre l'entreprise, ses projets et autre savoir-faire.
- Limiter au strict minimum l'emport de documents et matériels, et, sensibiliser conférenciers ou commerciaux au phénomène d'élicitation (méthode visant à soutirer de l'information),
- En cas de besoin, n'utiliser qu'un ordinateur dédié à l'évènement de façon à limiter les risques liés au vols ciblés ou d'opportunité,
- Récupérer les coordonnées des contacts utiles en lien direct avec l'organisation de l'évènement, de façon à remonter rapidement tout incident,
- Demeurer discret dans vos échanges, à l'occasion de l'utilisation des moyens de transport,

Pendant l'évènement:

- Respecter les règles d'hygiène informatique, notamment les conseils de prudence édictés dans le passeport de conseils aux voyageurs de l'ANSSI,
- Rester vigilant et discret sur la nature des rencontres et des échanges,
- Penser à prendre des notes relatives aux questions posées ou évènements survenus,
- Ne jamais perdre de vue que d'éventuels prédateurs peuvent mettre en oeuvre, à votre préjudice, des moyens techniques,

Après l'évènement:

- Rester vigilant jusqu'à votre départ vis-à-vis de la sécurité de vos matériaux et matériels informatiques et dresser un bilan d'activité prenant en compte toutes vos observations.

- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES INTRUSIONS CONSENTIES
Les visites de délégations étrangères

PRÉVENIR LE RISQUE DE PRÉDATION ÉCONOMIQUE

Dans son rapport relatif à l'activité pour l'année 2017, la délégation parlementaire au renseignement rappelle combien les entreprises sont aujourd'hui confrontées à un risque croissant de prédation qui, au delà du risque individuel, peut menacer la pérennité du patrimoine économique national. L'accueil d'une délégation étrangère est souvent porteur d'opportunités nouvelles pour l'établissement concerné. Toutefois, dans un contexte hyperconcurrentiel où ***chaque information peut présenter un intérêt stratégique***, toute menace n'est donc pas à écarter. Y penser en amont, c'est prendre les mesures adaptées pour se protéger !

L'ACCUEIL DE TOURISTES…INDUSTRIELS

Le manque d'ouverture, de bienveillance, d'amabilité, voire une attitude arrogante quand elle n'est pas méprisante, tel peut-être le souvenir laissé par des français à des étrangers.

Le tourisme industriel est une réalité qui trouve sa principale manifestation dans les visites d'entreprises. Parce que ce tourisme participe à soutenir l'économie et constitue en outre un ***vecteur d'influence et de promotion des savoir-faire*** à l'échelle internationale, les pouvoirs publics y accordent un intérêt grandissant:

- La direction générale des entreprises (DGE) fournit sur son site des données statistiques,
- L'association de la visite d'entreprise (AVE) a lancé en décembre 2012, avec le soutien financier de l'Etat (DGE), le premier portail de la visite d'entreprise. Cette association a pour objet la valorisation et la promotion de la filière visite d'entreprise (ou tourisme de savoir-faire).
- La visite d'entreprise dispose même de son guide du Routard !

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

DES PRÉDATEURS A L'IMAGINATION FERTILE

A l'occasion de leur visite, les membres d'une délégation étrangère pourraient être tenté de s'approprier quelques secrets industriels:

- Prétexter la panne d'un ordinateur portable et solliciter la mise à disposition d'un ordinateur peut avoir de sérieuses incidences si l'on a pas pensé en amont à s'assurer que, l'ordinateur objet du prêt, ne contient pas de données stratégiques (un interlocuteur malintentionné pourrait par exemple utiliser un support amovible particulièrement intrusif).
- Il n'est pas rare non plus qu'un membre d'une délégation s'égare lors d'une visite et qu'il soit retrouvé en dehors du parcours de notoriété (sous réserve que celui-ci ait été défini).
- L'expérience montre que certains visiteurs n'hésiteront pas non plus à tremper l'un de leurs vêtements dans des solutions liquides accessibles pour en prélever un échantillon.

LE CAS PARTICULIER DU MONDE DE LA RECHERCHE SCIENTIFIQUE

Les échanges internationaux en matière de recherche scientifique sont aussi nécessaires qu'ils peuvent se révéler bénéfiques. Mais seule une approche stratégique de ces échanges favorisera la protection des informations sensibles et une diffusion adaptée des connaissances.

- Le SISSE met à disposition, sur son site, deux guides destinés à la ***mobilité internationale des scientifiques*** à travers certains principes directeurs et un vade-mecum.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour vous préparer à la visite de délégations étrangères, vous pouvez:

- Aborder aussi bien la protection des savoir-faire que la sécurité des visiteurs et des salariés,
- Suivre les conseils de la DGSI prodigués dans le flash ingérence n°40 de février 2018 consacré à la visite des délégations étrangères et disponible sur www.entreprises.gouv.fr ,
- Consulter www.Services-Public.fr (F21921) pour renseigner votre délégation sur les visas à obtenir.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES INTRUSIONS CONSENTIES
L'entrisme

INFLUER SUR LES ORIENTATIONS STRATÉGIQUES D'UNE ORGANISATION RIVALE

L'entrisme est une technique d'influence dont la pratique ***consiste à introduire, de manière concertée, des membres d'une organisation militante*** (syndicat, parti politique, association, etc.) ***dans une organisation rivale, en vue d'en modifier les orientations***. Les méthodes employées pour faire de l'entrisme se révèlent par leur nature très diverses, donc difficiles à parer. L'entrisme peut être mis en oeuvre par une direction au sein d'une même organisation, dans le but d'infléchir le pouvoir d'opposition (opposition des syndicats par exemple). Mais généralement, on distingue deux types d'entrisme:

- L'***entrisme officiel*** qui consiste à agir ouvertement (« à bannières déployées »),
- L'***entrisme clandestin*** qui, à l'inverse, se fonde sur la discrétion, et use de méthodes plus insidieuses.

UNE TECHNIQUE HISTORIQUEMENT MILITANTE

D'un point de vue historique, l'entrisme est une ***stratégie politique révolutionnaire mise en oeuvre par les trotskistes*** au début du XXème siècle, dans une période où leur influence sur les masses ouvrières tendait à s'infléchir. L'entrisme des trotskistes à l'intérieur du parti communiste français (PCF), au début des années 1950, en constitue un exemple concret. De manière plus contemporaine, les exemples d'entrisme en politique sont fréquents, notamment en France lors des périodes d'élections locales, et par le seul « jeu des alliances ».

L'exemple du Brexit

Au cours du second semestre 2018, le parti conservateur britannique, auquel appartient la Première ministre, a dû faire face à des milliers d'adhésions. Certains spécialistes ***soupçonnent des partisans du « Brexit dur » de vouloir infiltrer*** le parti pour influencer sa ligne politique.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LA QUESTION DE L'ENTRISME RELIGIEUX EN ENTREPRISE

Depuis 2015, des organisations patronales et professionnelles s'inquiètent des ***tentatives d'infiltration ou de noyautage menées par des fondamentalistes religieux au sein de certaines sections syndicales*** de grandes entreprises françaises.

À la faveur de quelques jurisprudences européennes, le droit français a su en partie s'adapter. Pour rappel:

- Les entreprises privées ne sont pas soumises au principe constitutionnel de laïcité (Art 1). Toutefois, liberté de croyance (ou de religion) ne veut pas dire liberté d'exercer cette croyance.
- Les entreprises privées peuvent introduire un ***principe de neutralité dans leur règlement intérieur*** (article L1321-2-1 du Code du Travail), sous réserve de respecter les dispositions légales des articles L1121-1 et L1321-3 du Code du Travail. Le règlement intérieur ne peut être introduit qu'après avoir été soumis à l'avis du comité social et économique (article L1321-4).
- Le Ministère du Travail met à disposition depuis 2017 un guide pratique sur le sujet.

L'ENTRISME AU SERVICE DE LA GUERRE ÉCONOMIQUE

Les rapports de force qui s'observent aujourd'hui sur la scène internationale dépassent la seule notion d'hyper concurrence entre les entreprises. L'occasion pour certains spécialistes d'évoquer ***un contexte de guerre économique***.

Par exemple, les leaders mondiaux en matière d'équipementiers Télécoms sont aujourd'hui chinois, ce qui inquiète notamment les Etats-Unis et l'Europe. Au delà d'une stratégie d'investissement très volontariste, c'est surtout l'***entrisme opéré par les entreprises chinoises dans les groupes du secteur de la normalisation des architectures réseaux*** qui leur permet d'orienter le développement des standards mondiaux. Une note rédigée 2017 par la DG Trésor et l'Ambassade de France en Chine décrypte ce phénomène.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour aller plus loin:

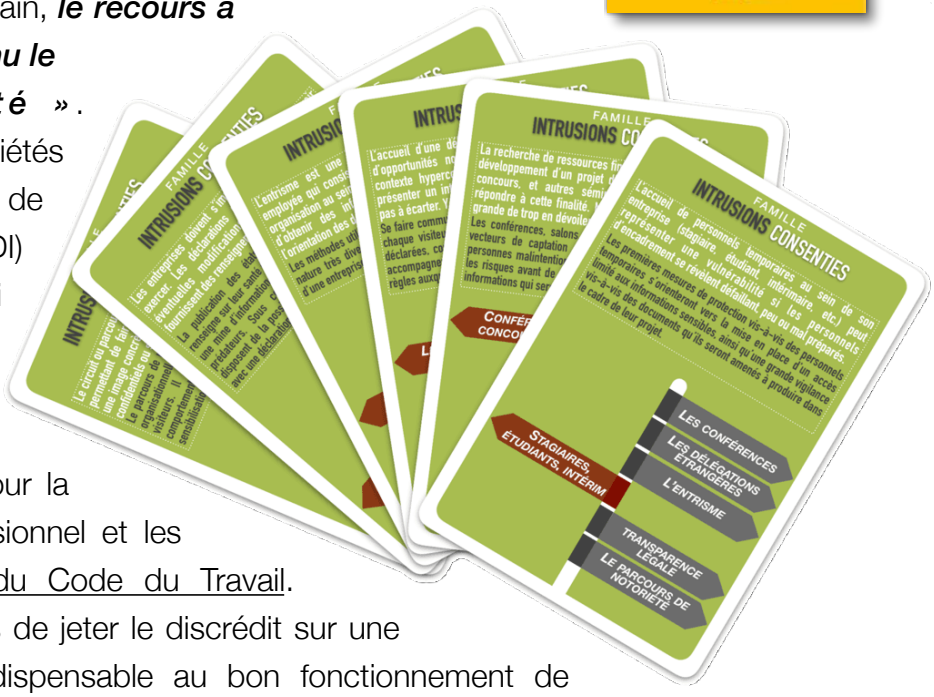
- Le règlement intérieur constitue l'un des moyens de protection dont dispose l'employeur pour se prémunir d'une certaine forme d'entrisme en entreprise. Le site www.Service-Public-Pro.fr (F1905) vous en rappelle les contours. Cette protection reste très partielle.
- Le sujet de l'entrisme ou de l'infiltration de mouvements à caractère sectaire en entreprise et dans les administrations demeure encore largement insoupçonné. Des experts de la MIVILUDES se tiennent à votre disposition. Leur site: www.derives-sectes.gouv.fr
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES INTRUSIONS CONSENTIES
Les stagiaires, intérimaires..

QUAND LE PROVISOIRE DEVIENT DÉFINITIF !

Dans un contexte économique incertain, ***le recours à du personnel temporaire est devenu le symbole de la « flexisécurité »***. L'annonce faite par plusieurs sociétés d'intérim d'intensifier la signature de contrats à durée indéterminée (CDI) avec leurs intérimaires s'inscrit ainsi dans le prolongement de nouvelles dispositions législatives et réglementaires, prévues par la loi n° 2018-771 du 5 septembre 2018 pour la liberté de choisir son avenir professionnel et les articles L 1251-58-1 et suivants du Code du Travail.



Toutefois, s'il ne s'agit en aucun cas de jeter le discrédit sur une population de salariés devenue indispensable au bon fonctionnement de l'économie française, ***il convient de ne pas négliger les vulnérabilités qui peuvent en découler***, auxquelles s'ajoutent celles générées par l'emploi de stagiaires.

UN ENCADREMENT HUMAIN ET JURIDIQUE NÉCESSAIRE

Les vulnérabilités engendrées par le recours à du personnel temporaire tiennent moins à la qualité intrinsèque des personnes qu'au fait qu'ils ne se trouvent liés à l'établissement que de manière ponctuelle. ***Potentiels auteurs d'actes de malveillance, ces personnels peuvent aussi en constituer la cible. La prévention de fuites d'informations stratégiques*** constitue dès lors un enjeu essentiel. L'adoption de simples mesures organisationnelles ou techniques permet de limiter l'occurence de ce risque, et peut consister à:

- Désigner une personne de l'établissement pour encadrer le personnel temporaire,
- Référencer et identifier (par badge) le personnel temporaire,
- Limiter et sécuriser l'accès aux ressources stratégiques de l'établissement,
- Sensibiliser les personnels concernés sur la confidentialité des échanges,
- Ne pas omettre de faire signer une clause de confidentialité (voir Fiche 42).

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

DROITS ET DEVOIRS DU STAGIAIRE EN MILIEU PROFESSIONNEL

Les stages en milieu professionnel offrent aux étudiants l'opportunité de découvrir une certaine réalité du travail. Si l'entreprise y trouve un intérêt réciproque (recrutement par exemple), les abus constatés par le passé ont amené le législateur à se saisir du sujet pour mieux l'encadrer.

La loi 2014-788 du 10 juillet 2014 tendant au développement, à l'encadrement des stages et à l'amélioration du statut des stagiaires, rappelle les trois objectifs poursuivis par le Gouvernement:

- Favoriser le développement des stages de qualité,
- Eviter les stages se substituant à des emplois et protéger les droits,
- Améliorer le statut des stagiaires.

Le stagiaire: un salarié pas comme les autres

- Une convention de stage est obligatoirement formalisée (Art L 124-1 du Code de l'Education) . Elle détermine, entre autres, la durée, les compétences à acquérir, les activités confiées au stagiaire et le montant de la gratification versée (Art D 124-4 du Code de l'Education).
- Bien que dépourvu de contrat de travail, le stagiaire doit tout de même figurer dans le registre unique du personnel comme le prévoit l'article L 1221-13 du Code du Travail.

Des restrictions d'emploi qui s'imposent au chef d'entreprise

- L'employeur ne peut placer le stagiaire dans un poste de travail considéré comme permanent (Art L 124-7 du Code de l'Education) et ne peut donc remplacer un salarié.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour aller plus loin:

- Le service de l'information stratégique et de la sécurité économiques met à disposition sur le site www.entreprises.gouv.fr/ une fiche consacrée à l'accueil du personnel temporaire,
- Le site www.Service-Public.fr (F16734) récapitule en détail toutes les garanties et dispositions légales et réglementaires dont bénéficie le futur stagiaire,
- Dans son espace destiné aux professionnels le site www.Service-Public-Pro.fr (F20559) recense l'ensemble des obligations qui s'imposent à l'employeur pour l'emploi d'un stagiaire,
- Le Ministère de l'enseignement supérieur fournit un guide pratique des stages étudiants.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES INTRUSIONS CONSENTIES
La mise à nu par transparence légale

S'IMMATRICULER POUR QUE ÇA ROULE…

Les entreprises doivent s'immatriculer avant de pouvoir exercer. ***Les déclarations d'activité, actes, statuts, les éventuelles modifications, cessation ou radiation, fournissent des renseignements précieux*** sur leur activité. Si la transparence totale n'est ni envisageable, ni souhaitable, une certaine transparence n'en demeure pas moins nécessaire et imposée par les textes législatifs et réglementaires. La transparence n'est cependant pas sans risques et peut conduire dans certains cas à la fragilisation des entreprises ainsi mises à nu.

UNE CARTE D'IDENTITÉ QUE L'ON PEUT PROTÉGER

La publication des états financiers ou comptes annuels renseignent sur la santé économique d'une entreprise. Ceux-ci constituent donc une mine d'informations à exploiter, surtout pour d'éventuels prédateurs. Lors de la clôture de chaque exercice annuel, une société commerciale doit obligatoirement déposer ses comptes sociaux au registre du commerce et des sociétés (RCS), afin d'en ***garantir la transparence***. À réception par le greffe, les comptes annuels font l'objet d'une publication au bulletin officiel des annonces civiles et commerciales (BODACC).

- Sous-réserve de remplir certaines conditions, les PME peuvent ***demander la confidentialité de leur compte de résultat*** directement sur le site www.infogreffe.
- Le guide des formalités fournit aux entrepreneurs et aux décideurs un panorama fiable, précis et à jour des démarches et formulaires juridiques relatifs aux formalités des entreprises.
- Le site www.Service-Public-Pro.fr fournit également toutes les précisions quant aux sociétés concernées par ces formalités, les documents comptables à déposer, les options de confidentialité possibles et de nombreux autres rappels législatifs et réglementaires.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

UNE OBLIGATION LÉGALE À RESPECTER.

Les entreprises, mais aussi les personnes physiques disposant d'une activité commerciale, artisanale ou autre, doivent nécessairement s'immatriculer pour exercer leur activité. Une fois cette démarche engagée, l'entreprise concernée se voit attribuer plusieurs numéros d'enregistrement.

- ***RCS***: le numéro d'inscription au registre du commerce et des sociétés est composé de la mention RCS, du lieu d'immatriculation, d'une lettre (A pour commerçant, B pour société), et du numéro SIREN de l'entreprise.
- ***SIREN***: ce numéro est attribué par l'INSEE (9 chiffres). Suite à l'immatriculation d'une entreprise, le centre de formalité des entreprises transmet le dossier à l'INSEE, qui fixera le numéro SIREN à l'entreprise. Il s'agit d'un simple numéro d'ordre, sans aucune signification particulière. Il n'est attribué qu'une seule fois et n'est supprimé qu'au moment de la disparition de l'entité juridique.
- ***NIC***: le numéro interne de classement est placé à la fin du SIREN. Il est composé de 5 chiffres.
- ***SIRET***: le numéro du Système Informatique pour le Répertoire des Entreprises sur le Territoire est composé de 14 chiffres. Il associe le numéro SIREN (9 chiffres) à celui du NIC (5 chiffres) et permet de caractériser chaque établissement de l'entreprise, ou l'auto-entrepreneur.
- ***APE***: l'activité principale exercée est une codification à vocation principalement statistique. Ce code permet d'identifier la branche d'activité principale de l'entreprise ou du travailleur indépendant. Attribué par l'INSEE lors de l'immatriculation, il est composé de 4 chiffres + 1 lettre. Les activités exercées dans l'entreprise restent déterminées par celles inscrites sur l'extrait du RCS.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour comprendre la mise à nu par transparence légale, il peut être utile de découvrir l'ensemble des ressources disponibles sur les entreprises. Vous pouvez ainsi:

- Exploiter les ressources du Centre de Documentation Economie-Finances (CEDEF).
- Exploiter les ressources de la Direction de l'Information Légale et Administrative (DILA).
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES INTRUSIONS CONSENTIES
Le parcours de notoriété

UN ACCOMPAGNEMENT BIENVEILLANT…

Le parcours de notoriété est un ***itinéraire préétabli*** permettant de faire visiter un établissement, d'en ***donner une image concrète et valorisante*** tout en ***évitant les locaux confidentiels*** ou sensibles, sauf à considérer que la configuration des lieux le permet déjà. Le parcours de notoriété ne constitue que l'une des mesures à mettre en place lors de l'accueil de visiteurs au sein de l'entreprise. Le chef d'établissement, soucieux de préserver ses avantages concurrentiels, s'efforcera de mettre en place une démarche de sécurité économique visant la protection de son patrimoine immatériel et la sécurité des personnes.

UN PARCOURS QUI S'INSCRIT DANS UNE STRATÉGIE D'OUVERTURE

Pas d'improvisation !

L'ouverture des portes de l'entreprise ne doit pas s'inscrire dans le cadre d'une initiative isolée, mais au contraire se bâtir autour d'une dynamique de projet qui vise à faire connaitre les savoirs et savoir-faire de l'établissement tout en prenant en compte l'exposition aux risques de prédation.

Ainsi, la matérialisation d'un parcours de notoriété devra nécessairement s'accompagner:

- ***De mesures organisationnelles*** qui permettront de gérer au mieux les visiteurs, de la préparation de leur venue à la fin de leur visite, en passant par une communication adaptée et leur identification tout au long du parcours,
- ***De mesures d'ordre techniques*** qui viseront à prévenir les vols de documents ou de matériels sensibles et se prémunir des dégradations visant l'outil de production, tout en assurant la sécurité des visiteurs dans des conditions similaires à celle des salariés,
- ***De mesures comportementales*** visant à impliquer et sensibiliser les salariés sur les risques de fuites d'informations sensibles et le signalement de tout comportement jugé comme intrusif.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ÉTAPES DU TOUR

La mise en application des mesures évoquées supra reste propre à chaque établissement. Toutefois, il importe de ne pas négliger quelques étapes clés.

Répertorier les zones sensibles

L'espionnage industriel n'est pas une légende et le visiteur aguerri n'aura aucun mal à déceler ou déduire des éléments stratégiques de l'entreprise, sous réserve qu'on lui en donne effectivement l'occasion. Répertorier les zones sensibles de l'établissement constitue un préalable nécessaire avant de déterminer l'itinéraire d'un parcours de notoriété qui prendra soin de les éviter.

Ne restez pas sans voix ! (discours de visite)

La communication envers les visiteurs revêt une importance toute particulière. Si elle permet de construire un discours autour de la visite, elle fixe surtout un cadre sécuritaire à respecter, de l'interdiction des prises de vues photographiques au suivi de l'itinéraire préétabli.

L'encadrement juridique des visiteurs

Il importe de ne pas négliger les aspects juridiques liés à la sécurité des visiteurs, mais également l'encadrement juridique des contrôles d'accès qui sont opérés.

- Le responsable sécurité prévu à l'article L.4644-1 du code du travail prendra en compte la présence des visiteurs dans sa mission de prévention des risques professionnels. Le chef d'établissement ne devra pas non plus négliger les aspects assurantiels de sa responsabilité.
- La gestion des contrôles d'accès, notamment des visiteurs, peut nécessiter la mise en oeuvre d'un traitement automatisé d'informations nominatives. Si la Norme simplifiée NS-042, élaborée à cet effet par la CNIL, perd sa valeur juridique depuis l'entrée en vigueur du RGPD, elle permet au responsable de traitement d'orienter ses premières actions de mise en conformité.

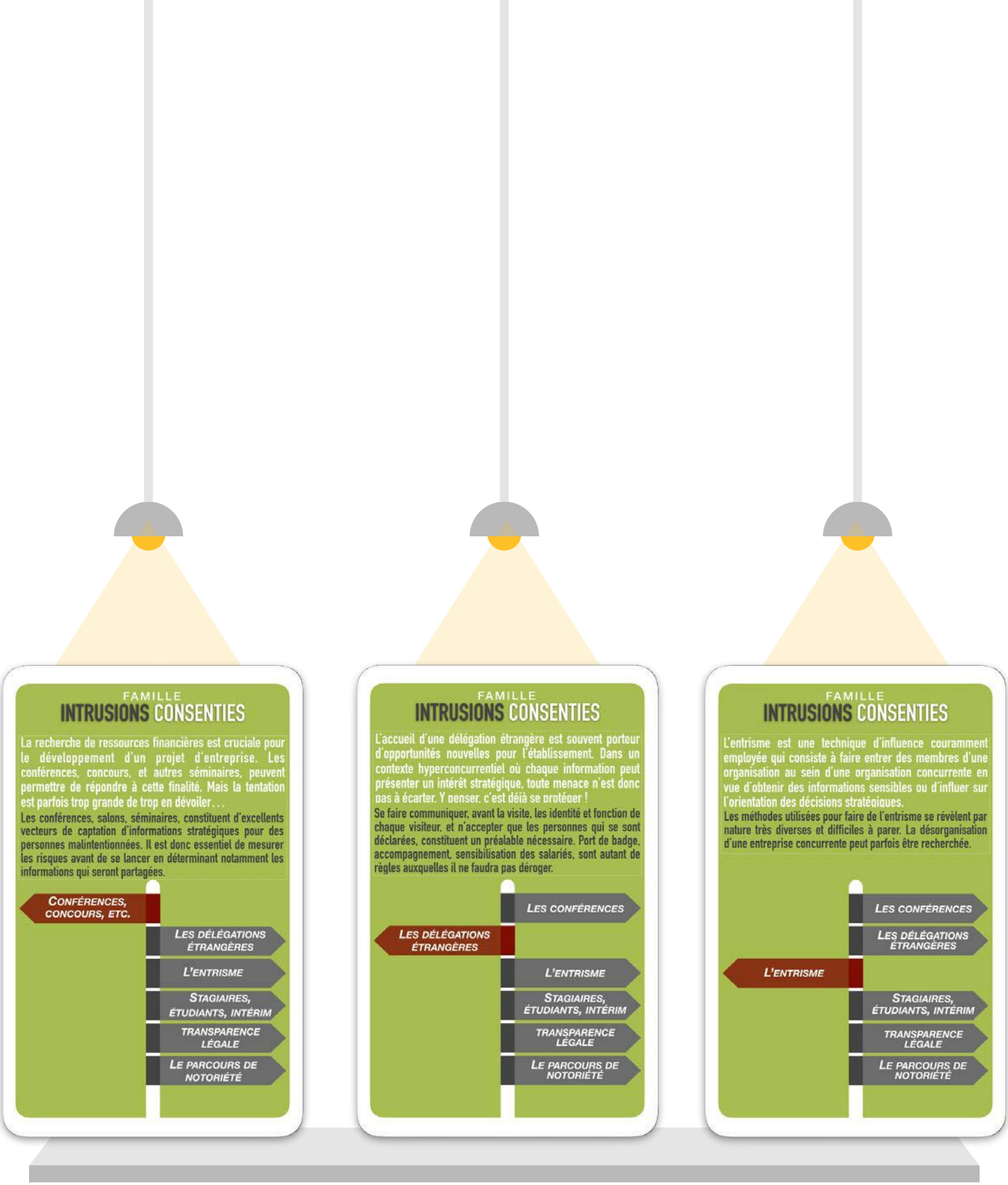
RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour aller plus loin:

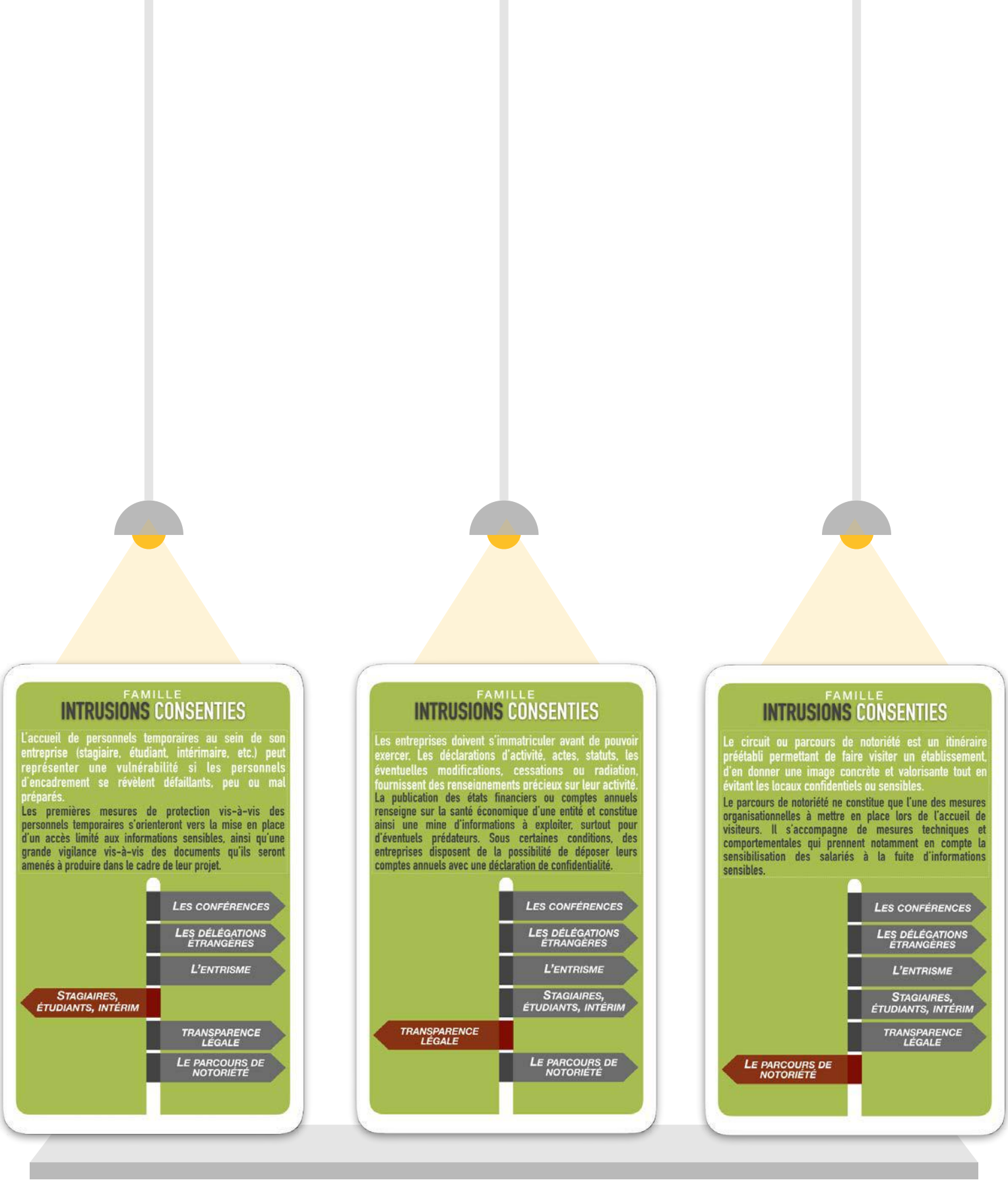
- Le service de l'information stratégique et de la sécurité économiques met à disposition sur le site www.entreprises.gouv.fr une fiche de sensibilisation consacrée à la réception des visiteurs.
- Le site www.cci.fr partage un guide méthodologique, datant de 2013 mais toujours d'actualité.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT



Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.

Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT



Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.

Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES FINANCIERS
Le client prédominant

LA GESTION DU RISQUE CLIENT: PAS UNE OPTION, UNE NÉCESSITÉ !

C'est parce que ***le client occupe une place centrale et prépondérante dans la vie d'une entreprise***, qu'il constitue dans le même temps l'une des ***sources principales des problèmes de trésorerie*** en raison notamment des risques d'impayé ou des retards de paiement. Mais qu'en est-il de ce risque financier lorsque le client est unique ou que sa représentativité dans le chiffre d'affaires le rend prédominant ? Ainsi, l'entreprise qui n'aurait pas été suffisamment vigilante, et qui produirait des biens ou des services pour un client unique, met en danger sa propre pérennité en se rendant totalement ou partiellement tributaire du client concerné.

IDENTIFIER LES FACTEURS DE RISQUE LIÉS AU CLIENT

La diversification du portefeuille clients se révèle parfois difficile

La présence d'un client unique ou prédominant ne doit pas être systématiquement interprétée comme une négligence. Dans de nombreux cas, cette situation se justifie par le fait que le secteur d'activité dans lequel évolue l'entreprise concernée présente peu de clients potentiels.

Les données financières du client ne sont pas toujours fiables ou disponibles

S'informer sur la solvabilité d'un client avant de signer un contrat constitue un préalable nécessaire. Pour autant, cette formalité n'est pas toujours aussi facile à réaliser:

- En France, même si les micro entreprises peuvent effectuer une déclaration de confidentialité, la transparence financière demeure la règle. Il en va autrement à l'international où la législation de certains pays ne favorisent pas toujours cette transparence.
- Dans le cas d'un client étranger, le risque pays ne doit pas être négligé (conformité, embargo).

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

ANTICIPER LES RISQUES ET ÉVITER LE CONTENTIEUX

En France, selon les données fournies par la Médiation du crédit aux entreprises, l***es créances clients représentent en moyenne plus de 40 jours de chiffre d'affaires*** et ***les impayés sont à l'origine d'une défaillance d'entreprise sur quatre***. Dès lors, pour minimiser l'impact du risque lié au client prédominant, il importe de connaitre ses droits et de prendre des mesures préventives.

S'informer et se prémunir du risque d'impayé grâce à l'assurance-crédit

L'assurance-crédit est une assurance qui protège l'entreprise contre le risque d'impayé des biens commandés/livrés et services fournis, en l'informant sur la solvabilité de ses clients et en lui permettant d'être couvert et indemnisé en cas de non-paiement. Le site www.Service-Public-pro.fr met à disposition une fiche (R45836) sur le sujet et oriente vers le guide de l'Assurance-crédit.

Une dépendance économique qui ne doit pas donner lieu à une exploitation abusive

Un client prédominant ne doit pas s'immiscer dans la gestion du sous-traitant dont le chiffre d'affaires dépend quasi exclusivement de ses commandes. L'article L. 420-2 du Code du Commerce réprime ainsi les abus qui peuvent notamment consister en refus de vente, en ventes liées, ou en pratiques discriminatoires.

Pour que cet abus soit caractérisé, ***trois conditions doivent être réunies***:

- l'existence d'une position dominante sur un marché,
- une exploitation abusive de cette position,
- un objet ou un effet restrictif de concurrence sur un marché. L'existence d'effets réels n'est pas indispensable. La potentialité d'effet(s) suffit à caractériser la pratique.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour aller plus loin:

- Lorsque la diversification des clients n'est pas possible, l'un des meilleurs remparts reste d'entretenir des relations saines avec le client prédominant. Le Guide pour la qualités des relations contractuelles clients-fournisseurs publié par le médiateur des entreprises fournit de nombreux conseils pratiques et juridiques.

- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES FINANCIERS
Le fournisseur prédominant

UNE RELATION ASYMÉTRIQUE

C'est peut-être un truisme que de le dire, mais ***les entreprises dépendent aussi bien de leurs clients que de leurs fournisseurs !*** Les évènements récents liés aux catastrophes naturelles survenues en Asie, ou à la crise financière de 2008, ont fait prendre conscience à de nombreuses entreprises de la nécessité de mieux prendre en considération les risques liés à la défaillance d'un fournisseur.

Dans un environnement complexe, aussi variable qu'incertain, la prudence commande dès lors d'éviter certaines situations. ***Le fournisseur prédominant est celui qui occupe une place exclusive, ou quasi exclusive, vis-à-vis d'une entreprise cliente***. De la simple rupture de stocks passagère à l'arrêt complet et durable de la chaîne de production, une mauvaise anticipation de ce risque peut avoir des conséquences irrémédiables et pour le moins entrainer des difficultés de trésorerie.

IDENTIFIER LES FACTEURS DE RISQUE LIÉS AUX FOURNISSEURS

Le fournisseur prédominant (ou exclusif) fait donc naître une relation asymétrique, au préjudice de l'entreprise à laquelle il est lié. D'une manière générale, sans exhaustivité et au delà des risques financiers, ***les risques liés aux fournisseurs peuvent avoir d'autres origines***, au titre desquels:

- Risque ***juridique*** (non respect de la législation en vigueur, non respect de contrat, etc);
- Risque ***technologique*** ou d'ordre logistique (délais de livraison, rupture d'approvisionnement, qualité des produits);
- Risque ***image*** (impact négatif vis-à-vis de la responsabilité sociétale de l'entreprise).
- Risque ***métier*** (met en évidence des carences en termes de gestion opérationnelle ou de pilotage dans la relation avec les fournisseurs).

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Identifier les fournisseurs stratégiques

Fort heureusement, les situations dans lesquelles des entreprises se trouvent confrontées à un fournisseur prédominant restent minoritaires. Pour autant, face à une multiplicité de fournisseurs, il importe de cerner les prestataires qui revêtent un caractère stratégique pour l'entreprise.

- La part que le fournisseur représente dans le volume des achats peut constituer un indicateur;
- La criticité du produit fourni (rareté, haute technologie, etc.) est un indicateur majeur;
- La difficulté de substituer le bien fourni constitue également un indicateur non négligeable;

Quoi qu'il en soit, l'identification des fournisseurs stratégiques ne saurait suffire. Elle devra être complétée par la mise en place d'une veille technologique et juridique sur les produits et un suivi régulier des prestataires les plus sensibles, sous réserve d'en avoir les ressources !

Une obligation de vigilance qui pèse sur l'employeur

Les articles L8221-1 et suivants du Code du Travail imposent aux entreprises une obligation de vigilance vis-à-vis de leur cocontractants sur le fondement de la ***lutte contre le travail dissimulé***.

Au cas présent, chaque entreprise ***devra donc obtenir de son fournisseur,*** lors de la conclusion du contrat et tous les six mois jusqu'à la fin de son exécution, toute une liste de documents.

L'article D8222-5 du Code du Travail en définit les modalités précises, sachant que:

- Le dispositif concerne les contrats commerciaux au moins égaux à 5000 euros HT;
- Les particuliers ne sont pas concernés par ce dispositif;
- Le travail dissimulé est sanctionné par l'article L8224-1 du Code du travail (3 ans + 45000€).

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Le contexte d'hyper concurrence et d'internationalisation des échanges (livrer vite, un produit de bonne qualité, à un prix raisonnable) font que la sélection de fournisseurs est devenu une décision stratégique:

- L'identification des facteurs de risques et des acteurs stratégiques devra donner lieu à la mise en place d'un plan d'actions et à des opérations de suivi et d'alerte.
- L'évaluation des fournisseurs sera effectuée sur la base de critères précis et objectifs.
- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES FINANCIERS
L'injection de capitaux

AVOIR DE L'ARGENT DISPONIBLE EST CAPITAL !

Pour se développer et innover, c'est-à-dire continuer d'exister dans un univers hyperconcurrentiel, l'entreprise doit pouvoir compter sur de l'argent disponible. Or, il s'avère que ***l'entreprise n'a pas toujours les moyens financiers d'assurer son propre développement,*** et le recours à l'emprunt bancaire n'est pas toujours possible ou souhaité. Si l'injection de capitaux, sous quelque forme que ce soit, apparait comme essentielle au développement de l'entreprise, elle favorise aussi la ***conquête de nouveaux marchés*** qui, pour certains, se révèlent difficiles à pénétrer par le seul biais des exportations. Toutefois, le ***risque*** d'une perte d'***influence dans la prise de décisions stratégiques***, ne doit pas être négligé.

FINANCEMENTS DES ENTREPRISES: A VOS MARQUES, PRÊT, PARTEZ !

Pour se développer, l'entreprise peut faire le choix d'une ***augmentation de capital social***, une démarche relativement fréquente mais pas anodine. En effet, le capital social est mentionné dans les ***statuts juridiques*** de l'entreprise et son augmentation suppose donc que ces mêmes statuts soient modifiés. Un lourd formalisme est requis. Ainsi, les décideurs pourraient être tentés de ***rechercher des financements alternatifs***. Les dispositifs ci-après apportent quelques réponses.

- Le décret 2016-501 du 22 avril 2016 prévoit le prêt interentreprises. Pour plus d'informations.
- Le financement d'entreprise à son « Guide du routard du financement d'entreprise ».
- Le site Service-Public-Pro.fr (R18133) vous oriente vers le répertoire des aides publiques aux entreprises.
- La banque de France met à disposition un référentiel des financements des entreprises.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LE CONTRÔLE DES INVESTISSEMENTS DIRECTS À L'ÉTRANGER

En 2017, la France a attiré 1 298 nouvelles décisions d'investissements étrangers créateurs d'emploi, soit une progression de 16 % par rapport à 2016. Ces investissements ont permis la création ou le maintien de 33489 emplois.

Les investissements directs à l'étranger (IDE) désignent les investissements par lesquels des entités résidentes d'une économie acquièrent ou ont acquis un intérêt durable dans une entité résidente d'une économie étrangère.

Les ***investissements en capital social*** recouvrent les prises de participation de plus de 10% dans des sociétés.

Le principe: la liberté d'investissement

Le fondement de la procédure des IDE repose en France sur la liberté d'investissement. L'art L151-1 du code monétaire et financier dispose que « les relations financières entre la France et l'étranger sont libres, dans le respect des engagements internationaux souscrits ».

L'exception: l'autorisation préalable d'investissement

Cette liberté de principe souffre tout de même de quelques exceptions. Ainsi, l'art L.151-3 du code monétaire et financier précise que les investissements étrangers dans certaines activités sont soumis à une autorisation préalable du ministre chargé de l'économie.

Depuis le 1er janvier 2019 (Décret 2018-1057), ***la France a étendu le contrôle des investissements étrangers à de nouveaux secteurs***, notamment la sécurité informatique, l'intelligence artificielle, les semi-conducteurs ou encore l'hébergement de données sensibles. Les demandes d'autorisation préalable d'investissement sont instruites par la Direction Générale du Trésor à Bercy en lien avec les ministères et organismes concernés.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour aller plus loin, vous pouvez:

- Prendre connaissance des possibilités offertes par la loi pour la croissance, l'activité et l'égalité des chances économiques. Le site www.economie.gouv.fr vous en précise la portée.
- Consulter le rapport de BusinessFrance sur l'internationalisation de l'économie française.
- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES FINANCIERS
Les escroqueries financières

NE VOUS Y TROMPEZ PAS !

L'article 313-1 du Code Pénal définit l'escroquerie comme le ***fait de tromper une personne physique ou morale afin de l'inciter à remettre des fonds, des valeurs, des services ou un biens quelconque par:***

- L'usage d'un faux nom ou d'une fausse qualité,
- L'abus d'une qualité vraie,
- L'emploi de manoeuvres frauduleuses.

Chaque année, l'Office National de la Délinquance et des Réponses Pénales (ONDRP) publie un rapport sur l'état de la criminalité en France. Dans son rapport 2017, on apprend ainsi que ***les escroqueries et infractions de types économiques ou financières sont parmi les atteintes qui ont le plus évolué ces dernières années*** et notamment celles liées à l'utilisation frauduleuse d'informations bancaires. Si les grandes entreprises victimes parviennent à surmonter ce type d'atteintes, ce n'est pas toujours le cas de nombreuses PME qui, insuffisamment préparées, sont parfois conduites à la faillite.

LES ESCROQUERIES FINANCIÈRES EN LIGNE…DE MIRE !

Les nouvelles technologies et l'essor des médias sociaux fournissent aux escrocs de nouveaux outils qui leur permettent à la fois d'***accroitre le volume potentiel des victimes*** tout en diminuant le risque de se faire prendre en ayant recours à des ***outils d'anonymisation*** (VPN, Proxy, Chiffrement, etc.). Si le mode opératoire de ces escroqueries reste relativement traditionnel, la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC) évoque, dans son dernier rapport sur l'état de la menace lié au numérique, cinq grandes tendances: les faux virements (***FOVI***), les fraudes liées à l'***investissement sur le Diamant***, les faux investissements (***FOREX***), les ***cryptomonnaies*** et les ***fraudes à la carte bancaire***.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LUTTER CONTRE LES ESCROQUERIES DE GRANDE ENVERGURE

Parallèlement à l'action des services de répression judiciaire, il existe en France un service d'enquête administrative chargé de la lutte contre la fraude, le blanchiment d'argent et le financement du terrorisme. Il est connu sous le doux acronyme de TRACFIN.

TRACFIN: un service spécialisé de la communauté du renseignement français

Créé en 1990 sous la forme d'une cellule de coordination au sein de la direction générale des douanes et des droits indirects (DGDDI), TRACFIN devient en 2006 un service à compétence nationale avec une direction propre. Par le décret 2014-474 du 12 mai 2014, TRACFIN intègre le cercle très fermé des services spécialisés de renseignement.

La déclaration de soupçon

L'article L. 561-15 du Code monétaire et financier dispose que « Les personnes mentionnées à l'article L. 561-2 sont tenues, dans les conditions fixées par le présent chapitre, de ***déclarer*** au service mentionné à l'article L. 561-23 ***les sommes inscrites dans leurs livres ou les opérations portant sur des sommes dont elles savent, soupçonnent ou ont de bonnes raisons de soupçonner*** qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou sont liées au financement du terrorisme ».

Outre les escroqueries, sont ainsi concernées l'abus de confiance, la corruption, l'abus de biens sociaux, etc.

ERMES, ne doit pas être considérée comme du luxe !

Le décret n° 2013-480 du 6 juin 2013 fixe les conditions de recevabilité d'une déclaration de soupçon. Une procédure d'irrecevabilité de la procédure peut être décidée si les conditions ou les modalités de sa transmission ne sont pas respectées (utilisation de la plateforme ERMES dédiée).

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Face à l'essor des escroqueries via Internet, des dispositifs de recueil de plaintes en ligne ont été instaurés:

- La plateforme Perceval vous permet de signaler une fraude à la carte bancaire.
- La plateforme Thesee permettra bientôt de porter plainte pour toute escroquerie en ligne.
- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES FINANCIERS
Le manque de trésorerie

DES LIQUIDITÉS POUR NE PAS ÊTRE LIQUIDÉ !

La trésorerie d'une entreprise peut être définie comme l'ensemble constitué des liquidités disponibles en caisse ou en banque, à un instant donné. Elle permet aux entreprises de financer les dépenses courantes. ***Un manque de trésorerie peut, dès lors, avoir des répercussions très préjudiciables, voire empêcher purement et simplement une entreprise d'honorer ses commandes***. La cessation de paiement peut aboutir rapidement à la mise en oeuvre d'une procédure collective comme le redressement ou la liquidation judiciaire. Plusieurs facteurs peuvent conduire au manque de trésorerie. Ce peut-être le cas lorsqu'il est par exemple constaté:

- Un allongement des délais de paiements par les clients,
- Une diminution des délais de paiements aux fournisseurs,
- Un ralentissement de l'activité,
- Une augmentation des stocks,
- Une réduction des marges, etc.

La problématique des paiements tardifs constitue une cause externe majeure pouvant induire un manque de trésorerie. En France, le délai convenu entre les parties pour régler les sommes dues est fixé au 30e jour suivant la réception des marchandises ou l'exécution de la prestation, et ne peut dépasser 60 jours à compter de la date de facturation. Par dérogation, un délai maximal de 45 jours fin de mois à compter de la date d'émission de la facture peut être convenu entre les parties (Article L 441-6 du Code du Commerce). Le site www.Services-Public-Pro.fr dédie une fiche (F23211) aux délais de paiement entre professionnels et pénalités de retard.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

SE PRÉMUNIR CONTRE LES PAIEMENTS TARDIFS

L'affacturage et l'injonction de payer constituent deux mécanismes permettant, soit d'anticiper le risque, soit de contraindre le débiteur.

L'affacturage

Ce mode opératoire permet à une entité de sous-traiter la gestion de ses créances à une entreprise financière extérieure (on parle de *Factor*), laquelle relève généralement de la catégorie des établissements de crédit. L'affactureur va ainsi se substituer à son client pour:

- Assurer le recouvrement des créances,
- Prendre à sa charge le risque de non-paiement (client qui n'honore pas ses factures),
- Verser à l'entreprise les liquidités correspondantes au montant des créances cédées,
- Seules les créances détenues sur une autre entreprise peuvent faire l'objet d'une opération d'affacturage.

L'injonction de payer

Il s'agit d'une procédure de recouvrement relativement simple, rapide et peu onéreuse. Elle ne nécessite pas de recours à un conseil. Toutefois, pour obtenir une injonction de payer, certaines conditions sont requises:

- La créance doit être certaine, liquide (peut-être évaluée) et exigible (dette venue à son terme),
- L'impayé doit reposer sur une cause contractuelle ou résulter d'une obligation statutaire,
- Le tribunal compétent dépend du montant du litige.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous êtes confronté à un manque de trésorerie, vous pouvez:

- Prendre connaissance des dispositifs relatifs aux règles de crédit aux entreprises,
- Consulter la fiche pratique sur les injonctions de payer sur www.Service-Public.fr (F1746),
- Consulter le Guide du Routard du financement des entreprises.

- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES FINANCIERS
La cessation d'activité

QUAND LE MALHEUR DES UNS NE FAIT PAS LE BONHEUR DES AUTRES !

Qu'elle soit ***volontaire ou non***, la cessation d'activité se définit comme étant ***l'arrêt de l'activité d'une entreprise***. Dans le cas d'une entreprise individuelle (dépourvue de personnalité morale), la cessation d'activité peut prendre sa source dans le ***départ en retraite*** de son propriétaire ou son ***décès***. Elle peut découler simplement de la ***vente de la société***. Lorsqu'elle concerne une société par actions, la procédure s'avère plus rigoureuse et un liquidateur doit être nommé.

Quel que soit le cas de figure, la cessation d'activité d'une entreprise a toujours des ***incidences vis-à-vis de l'écosystème*** dans lequel elle évolue (clients, salariés, fournisseurs, prestataires, etc.). La disparition d'un partenaire ***doit donc être appréhendée comme un risque.*** Dans le cas contraire, et plus encore dans le cas ou l'entreprise en question est un client ou un fournisseur prédominant, ***le manque d'anticipation peut conduire à de graves difficultés***.

DES OBLIGATIONS LÉGALES ET FISCALES À RESPECTER

La personne physique ou morale qui cesse son activité dispose d'un ***délai de 30 jours pour effectuer une déclaration*** auprès du Centre de Formalités des Entreprises.

Sur le ***plan fiscal***, les articles 201 à 204 du Code général des impôts précisent les dispositions spéciales applicables en cas de cession, de cessation ou de décès. Ainsi, les contribuables concernés doivent déclarer la cession ou cessation d'activité à l'administration fiscale dans un ***délai de 45 jours***.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

ENTRE PROCÉDURE ALTERNATIVE ET ACTIONS PRÉVENTIVES

La cessation temporaire d'activité (ou mise en sommeil d'une société)

Dans les cas où l'activité d'une entreprise est susceptible de reprendre, tout dirigeant peut recourir à une cessation temporaire d'activité.

Cette alternative offre de nombreux avantages:

- Elle évite la dissolution et la liquidation de l'entreprise;
- Elle évite de régler des frais pour la clôture de la société;
- Elle permet le maintien de l'immatriculation de son entreprise au registre du commerce et des sociétés (RCS);
- Elle permet enfin de conserver le bénéfice de l'exonération de cotisations sociales accordée au titre de l'aide à la création ou à la reprise d'entreprise (ACRE).

Le site Service-Public-Pro.fr précise le cadre légal et la durée de la cessation temporaire d'activité.

La due diligence: entre procédure d'audit préalable et obligation de vigilance

Définitive ou temporaire, la cessation d'activité d'une entreprise constitue un risque auquel il convient de se préparer.

C'est ainsi que la due diligence (concept anglo-saxon):

- Permet à un futur acquéreur d'évaluer la situation précise d'une entreprise avant de se prononcer sur un investissement éventuel;
- Trouve une équivalence dans les procédures d'audit préalable et d'obligation de vigilance.

L'art 17 de la loi 2016-1691 du 9/12/2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, dite ***loi SAPIN II***, impose une obligation de conformité pour certaines entreprises et rend ainsi le concept de due diligence incontournable.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

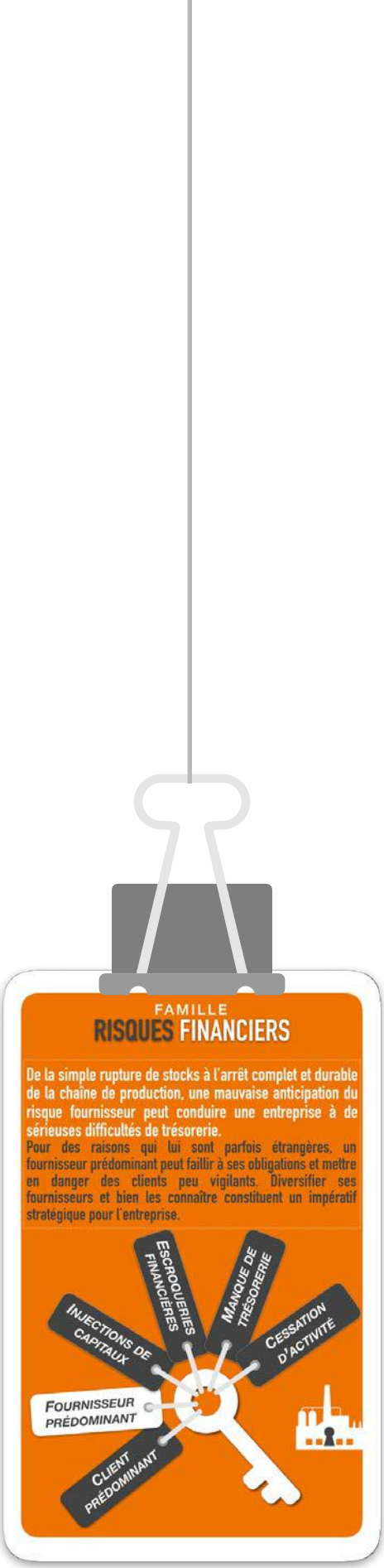
Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

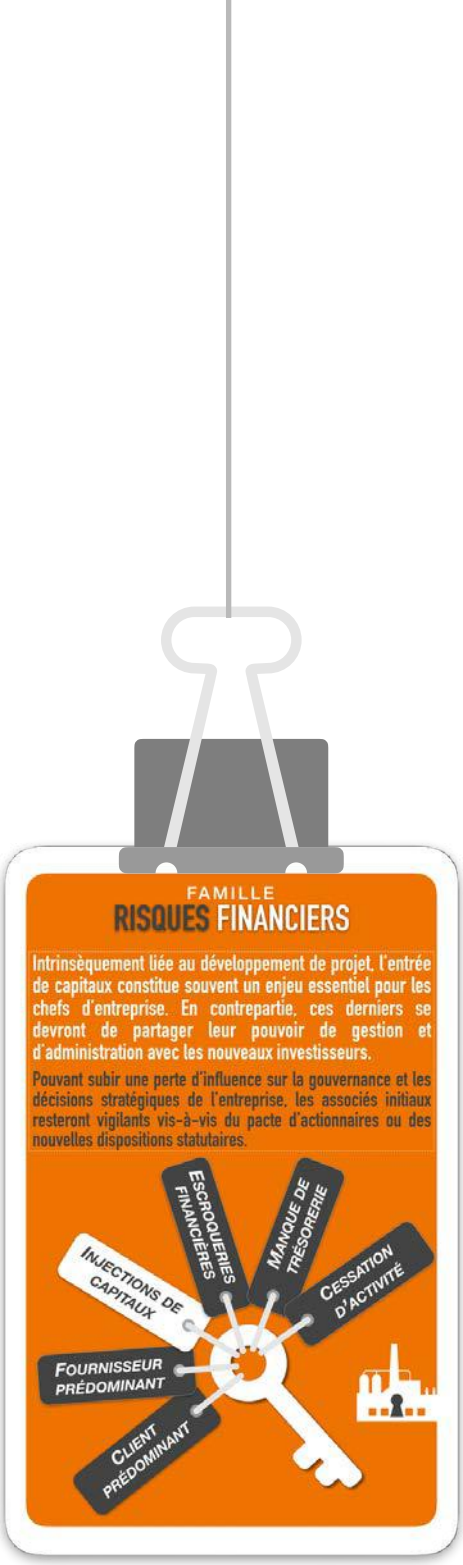
La cessation d'activité a des causes multiples qu'on ne peut pas toujours maitriser (évènements d'origine naturelle par exemple), toutefois:

- Parce que les conséquences humaines et financières d'une cessation d'activité peuvent se révéler d'une particulière gravité, la responsabilité du dirigeant pourra être mise en cause par le tribunal de commerce en cas de décisions contraires à l'intérêt de la société ou des tiers.

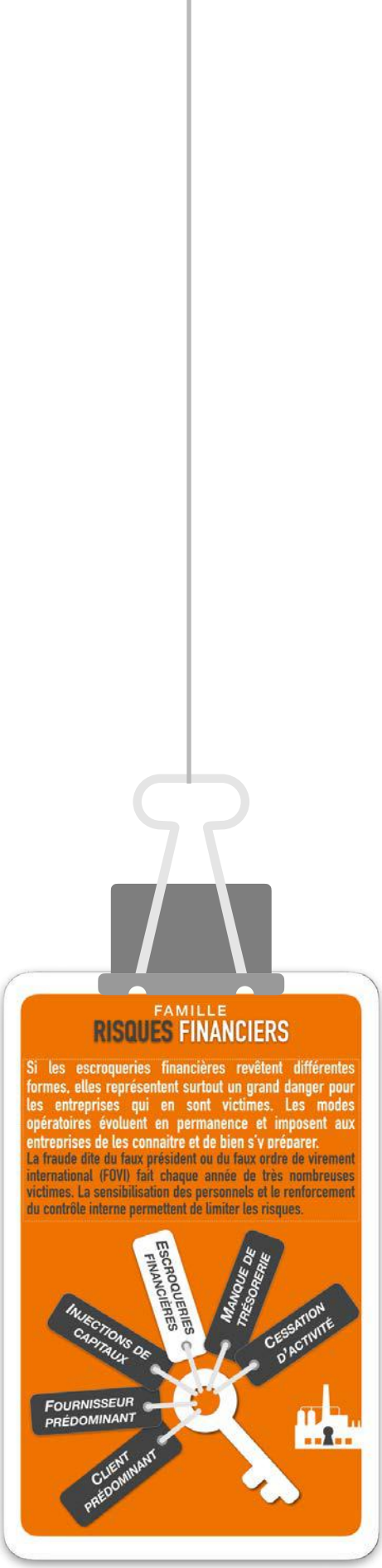
- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

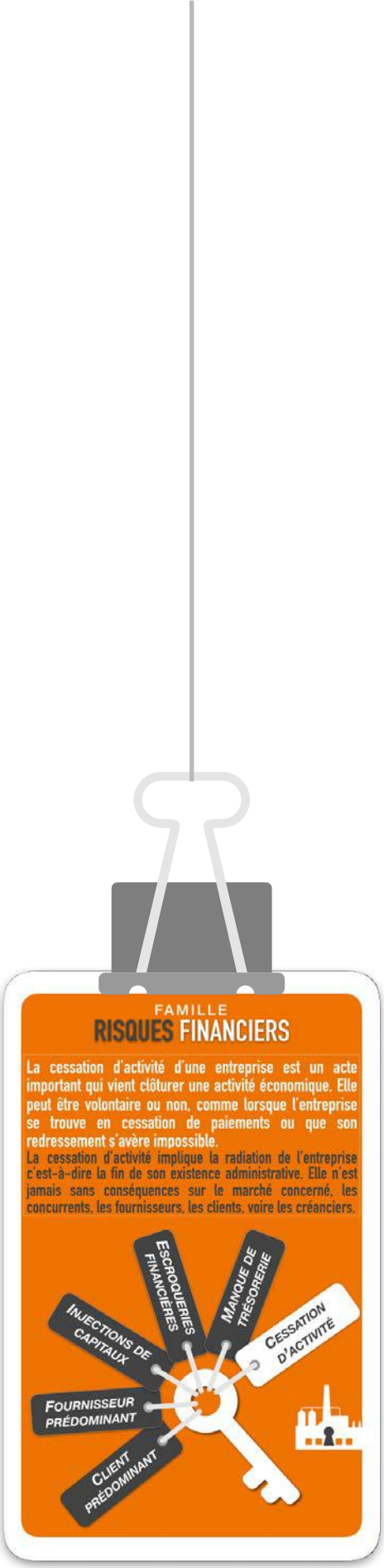
Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT





Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT





Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES INFORMATIQUES
La destruction de données

L'ENTREPRISE: UNE CIBLE PRIVILÉGIÉE

Le rapport de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pour l'activité 2017 nous rappelle combien les notions de sécurité économique et de sécurité numérique sont intrinsèquement liées. Qu'il s'agisse du ***code malveillant Notpetya*** ou du ***rançongiciel Wannacry***, les conséquences se sont révélées majeures pour plus de 250000 entreprises dans le monde, affectant près de 150 pays, avec des dégâts qui dépassent largement les seuls dommages informatiques. La ***destruction, l'altération ou encore le chiffrement de données***, orchestré par un pirate informatique ou un employé malveillant, ***peut s'avérer fatal pour l'entreprise qui en est victime***. Une bonne évaluation des risques en amont constituera un facteur de poids quant à la capacité de résilience.

SÉCURITÉ DES DONNÉES ET MANAGEMENT DU RISQUE

A l'ère du tout numérique, la protection du patrimoine informationnel de l'entreprise, impose que soit préalablement identifié l'information stratégique à protéger. Le service de l'information stratégique et de la sécurité économiques (SISSE) met à votre disposition un ensemble d'outils.

S'appuyant sur une approche systémique et managériale, l'ANSSI a développé la méthode ***EBIOS RISK MANAGER*** en vue de permettre aux organisations d'***identifier et comprendre les risques*** numériques qui leurs sont propres. Cette méthode de management du risque numérique vous est expliquée dans ce guide. Les éditeurs de logiciels ont été appelés à manifester leur intérêt, et les premières labélisations pourraient être délivrées par l'ANSSI en 2019.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

ENTRE RÉSILIENCE DES ENTREPRISES ET RÉSILIENCE DE LA NATION

Pour une entreprise, la résilience au risque cyber se caractérise par sa ***capacité à identifier, prévenir, détecter et parer les attaques informatiques et à se rétablir rapidement*** tout en minimisant l'impact financier de ses attaques autant que les conséquences pour les clients ou la réputation de l'établissement.

En France, l'ANSSI occupe un rôle prépondérant dans le maintien d'une capacité de résilience de la Nation face au risque numérique. Un socle juridique adapté s'est progressivement formé, lequel prend désormais en compte les exigences européennes.

Sécurité des activités d'importance vitale

La France a déterminé 12 secteurs d'activités d'importance vitale répartis en 4 dominantes (humaine, régalienne, économique, technologique). Leur sécurité est placée sous la responsabilité du Premier ministre et du secrétariat général de la défense et de la sécurité nationale (SGDSN).

Opérateurs d'importance vitale (OIV)

La désignation des OIV est définie par l'article R. 1332-1 du code de la défense. On en dénombre plus de 200 sur le territoire national. Pour des impératifs de sécurité nationale, leur identification demeure confidentielle.

Opérateurs de service essentiels (OSE) et fournisseurs de service numérique (FSN)

La directive NIS de 2016 prévoit un cadre de coopération européen pour la cybersécurité des réseaux et des systèmes d'information. Après avoir transposé en 2018 cette directive, la France vient de fixer par arrêté les règles de sécurité qui s'imposent au OSE, ainsi qu'aux FSN.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Toute entreprise doit diminuer son exposition au risque de destruction de données.

- Entreprise, administration ou particulier, en cas d'incident, adressez-vous au bon contact !
- Formations, labélisations, ou certifications, l'ANSSI vous apporte ses recommandations.
- Conscients des enjeux pour la sécurité, la justice et les libertés publiques, l'INHESJ et l'IHEDN ont décidé, avec leurs partenaires, de proposer une formation de haut niveau, candidatez !
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES INFORMATIQUES
Vols d'ordinateurs et de supports de stockage

UNE SÉCURITÉ DES SYSTÈMES À SUPPORT..ER !

Les ordinateurs (entendre sous ce vocable la représentation la plus traditionnelle que l'on s'en fait) occupent une place sans cesse grandissante dans notre vie quotidienne, personnelle ou professionnelle. Si dans l'absolue, on pourrait considérer les ordinateurs et supports de stockage comme de simples outils, ***leur valeur croît en fonction des données qu'ils recèlent***, que celles-ci soient personnelles, sensibles ou confidentielles.
Dès lors, il importe de ***garantir leur sécurité informatique*** en s'assurant que ne soient pas compromis:

- La confidentialité (utilisation du chiffrement),
- L'authenticité (s'assurer de communiquer à la bonne personne),
- L'intégrité (s'assurer que le contenu d'un message n'a pas été modifié),
- La disponibilité (du service utilisé),

En effet, quelles seraient les conséquences d'un simple vol d'ordinateur ou de support de stockage pour tout organisme:

- Si ces dispositifs n'étaient pas protégés ?
- Si des secrets industriels ou professionnels venaient à être dévoilés ?
- Si une porte d'entrée s'ouvrait sur le réseau d'entreprise sans que cette faille soit pour autant détectée ?
- Si la continuité d'activité de l'organisme concerné venait à être remise en cause ?
- Si la réputation venait à être entachée ?

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

AGIR SUR LES COMPORTEMENTS ET LA PRISE DE CONSCIENCE

Pour vous protéger et agir efficacement sur la protection de vos outils numériques, l'ANSSI a créé le MOOC ***SecNumacademie.gouv.fr***. D'accès gratuit, il vous propose de suivre quatre modules de formation (Panorama de la SSI, sécurité de l'authentification, sécurité sur internet et ***sécurité*** du ***poste de travail*** et ***nomadisme***) et de prendre conscience des bons comportements à adopter.

DE L'IMPÉRATIF DE PROTECTION À L'OBLIGATION DE NOTIFICATION

Le chiffrement de disque pour écrire la bonne partition

Comme l'indique l'ANSSI dans le module 4 de son MOOC, le chiffrement reste la meilleure façon de se protéger de la divulgation de données sensibles suite à la perte ou au vol d'un périphérique amovible. CRYHOD fait partie des solutions logicielles certifiées par l'ANSSI.

Obligation de notifier toute violation à un traitement de données automatisé

Depuis le 25 mai 2018, le Règlement général européen sur la protection des données (RGPD) impose aux entreprises et aux organisations de revoir toute leur architecture de collecte et de traitement des données personnelles de leurs utilisateurs.

Ainsi, l'art 33 du règlement oblige le responsable du traitement de données victime d'une atteinte à son STAD de notifier la violation dans les 72H à l'autorité de contrôle (CNIL), sous peine de sanctions et amendes administratives ! Restez donc vigilant après le vol d'un ordinateur ou d'un périphérique de stockage.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour réduire l'impact d'un vol d'ordinateur ou de support de stockage:

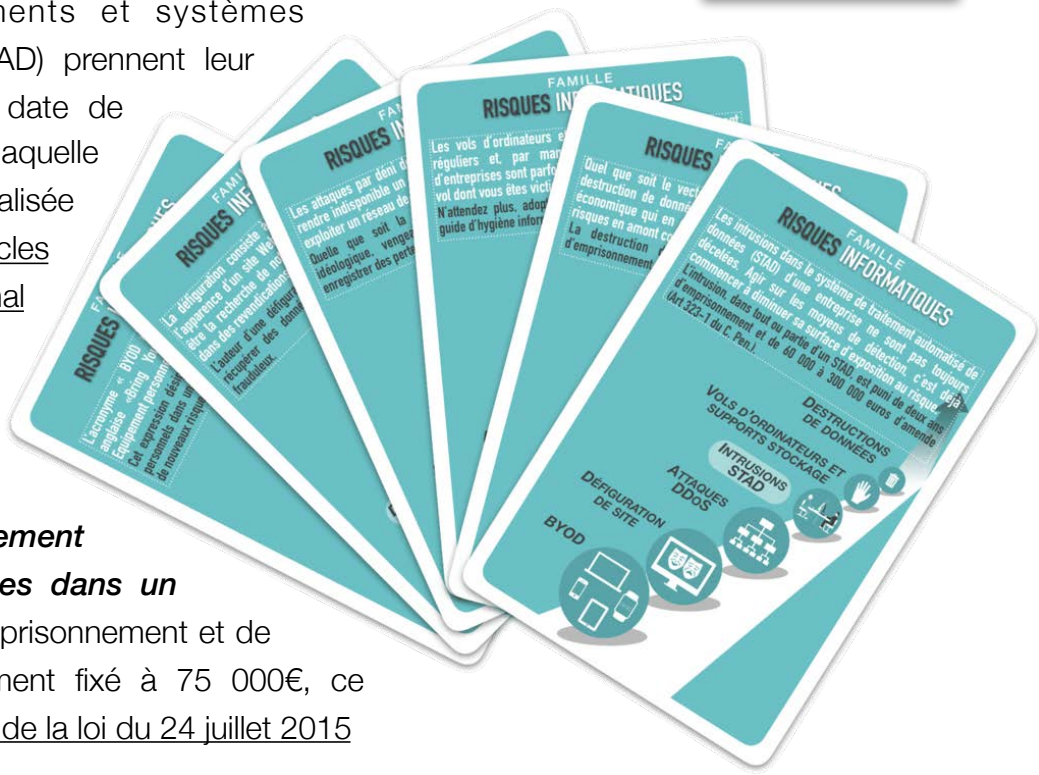
- Bien préparer ses déplacements, et suivre les conseils de prudence édictés dans le passeport de conseils aux voyageurs de l'ANSSI,
- Sensibiliser son entourage et inciter au renforcement des mots de passe en suivant les conseils de l'ANSSI et en appliquant la méthode proposée par la CNIL,
- Conscients des enjeux pour la sécurité, la justice et les libertés publiques, l'INHESJ et l'IHEDN ont décidé, avec leurs partenaires, de proposer une formation de haut niveau, candidatez !
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES INFORMATIQUES
Les intrusions dans les STAD

INTERDIT DE STAD DEPUIS 30 ANS !

Les atteintes aux traitements et systèmes automatisés de données (STAD) prennent leur fondement dans une loi qui date de 1988, à savoir: la loi Godfrain, laquelle a bien évidemment été actualisée depuis cette date. Les articles 323-1 et suivants du Code pénal prévoient notamment que l***e fait « d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données (…) » contenues dans un STAD est puni*** de 5 ans d'emprisonnement et de 150 000€ d'amende (initialement fixé à 75 000€, ce montant a été révisé par l'art 4 de la loi du 24 juillet 2015 relative au renseignement.



DÉTECTER, RÉAGIR, RÉPRIMER

CSIRT/CERT: des centres (et des experts) pour répondre aux attaques informatiques

Parce que les attaques sont sans cesse plus nombreuses, il importe de les détecter et de réagir au plus tôt. CERT-FR est le centre gouvernemental de veille, d'alerte, et de réponse aux attaques informatiques géré par l'ANSSI. Il publie quotidiennement des Avis de sécurité, des Bulletins d'actualité et des Notes d'information pour prévenir d'un danger immédiat ou d'une vulnérabilité, et donner les moyens de s'en prémunir.

Organisation judiciaire: ça roule pour la Section F1 du TGI de Paris

Depuis 2014, le Parquet de Paris comporte une section dédiée à la cybercriminalité: la section F1. Cette juridiction spécialisée dispose, depuis la loi du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement [..], d'une ***compétence nationale concurrente*** en matière d'atteintes aux STAD.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LA SÉCURITÉ DES « SI » À L'ÉCHELLE EUROPÉENNE

ENISA: l'agence européenne chargée de la sécurité des réseaux de l'information

Créée en 2004 et implantée en Grèce, l'ENISA agit en collaboration avec les instances nationales et les institutions européennes pour développer une culture de la sécurité des réseaux d'information dans toute l'Union.

Cette agence répertorie au niveau européen, et sous la forme d'une cartographie interactive, l'ensemble des CSIRT/CERT par pays.

Europol EC3: la coopération judiciaire

Inauguré le 11 janvier 2013, le centre européen de lutte contre la cybercriminalité a vocation à protéger les entreprises et les citoyens européen contre la cybercriminalité. Il se concentre sur les activités illicites en ligne menées par des organisations criminelles, soutient les enquêtes et promeut les solutions à l'échelle de l'Union Européenne.

RGPD: la protection des données personnelles des citoyens européens

Depuis le 25 mai 2018, le Règlement général européen sur la protection des données (RGPD) impose aux entreprises et aux organisations de revoir toute leur architecture de collecte et de traitement des données personnelles de leurs utilisateurs.

Ainsi, l'art 33 du règlement oblige le responsable du traitement de données victime d'une atteinte à son STAD à notifier la violation dans les 72H à l'autorité de contrôle (CNIL), sous peine de sanctions et amendes administratives !

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

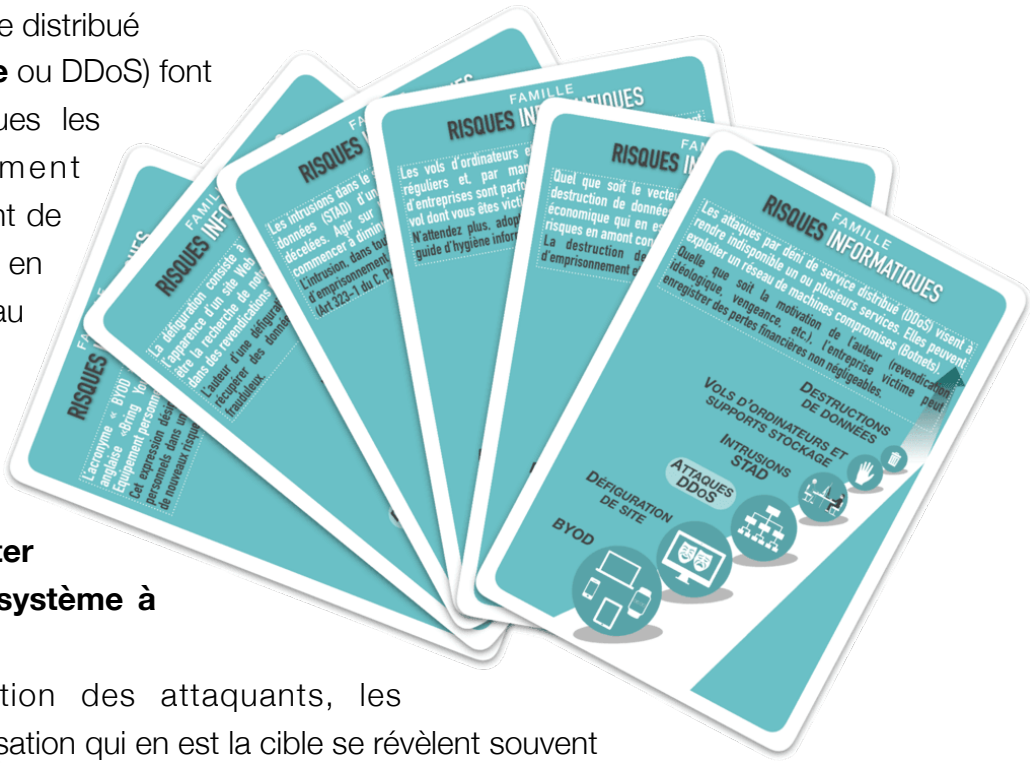
Si vous êtes victime d'une atteinte à votre système de traitement automatisé de données:

- Entreprise, administration ou particulier, en cas d'incident, adressez-vous au bon contact !
- Formations, labélisations, ou certifications, l'ANSSI vous apporte ses recommandations.
- Lire les rapports de l'ANSSI et de la DMISC pour prendre en compte l'état de la menace cyber.
- Conscients des enjeux pour la sécurité, la justice et les libertés publiques, l'INHESJ et l'IHEDN ont décidé, avec leurs partenaires, de proposer une formation de haut niveau, candidatez !
- L'ONDRP vous renseigne sur l'évolutions des atteintes aux STAD dans la Note n°21.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES INFORMATIQUES
Les attaques DDoS

VOUS EMPÊCHER DE RENDRE UN SERVICE !



Les attaques par déni de service distribué (**Distributed Denial of Service** ou DDoS) font partie des risques informatiques les plus fréquents, actuellement constatés, en raison notamment de leur relative simplicité de mise en oeuvre et leur faible coût au regard de leur efficacité.

L'ANSSI définit l'attaque DDoS, dans son glossaire, comme l'**action ayant pour effet d'empêcher ou de limiter fortement la capacité d'un système à fournir le service attendu**.

Quelle que soit la motivation des attaquants, les conséquences pour une organisation qui en est la cible se révèlent souvent très préjudiciables. Prendre conscience des risques, c'est par exemple pour un dirigeant, de protéger ses infrastructures et recourir à des technologies adaptées.

EN MODE ZOMBIE

Pour qu'une attaque DDoS soit couronnée de succès, elle doit reposer sur la puissance et les bandes passantes de centaines ou de milliers d'ordinateurs, afin d'envoyer d'énormes quantités de trafic vers un site Web, en vue de le rendre inopérant.

Les attaques DDoS peuvent être lancées à partir de réseaux de machines compromises appelés ***botnets ou machines zombie***, contrôlées à distance par un pirate informatique.

La méthode la plus simple et la plus rapide pour infecter un ordinateur reste l'infection par courrier électronique. La vigilance humaine vis-à-vis de certains liens hypertextes suspects et la mise à jour régulière de ses logiciels antivirus constituent la base d'un début de protection.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

DES MENACES POUR LA E-ADMINISTRATION

Estonie 2007: quand l'administration de tout un pays se trouve perturbée

Figurant au rang des pays précurseurs en matière « d'administration en ligne », l'Estonie a subi, le 27 avril 2007 et pendant plus d'un mois, une vague d'attaques massives en déni de service distribué, lesquelles ont perturbé le fonctionnement de la vie courante du pays.

Le rapport d'information du Sénat sur la cyberdéfense de 2012, rapporté par JM. Bockel en dresse un récit.

France: Action publique 2022

Le 13 octobre 2017, le gouvernement français marquait ses ambitions en dévoilant le programme de transformation Action publique 2022. Ce programme vise notamment à ***moderniser l'environnement de travail*** des agents publics, renforcer la relation de ***confiance*** avec les usagers, et faire ***baisser la dépense*** publique.

La transformation numérique constitue l'un des chantiers majeurs et doit tendre vers ***100% de démarches administratives numérisées*** à l'horizon 2022. Dans un tel contexte, la protection des services en ligne contre les attaques en déni de service distribué (DDoS) constitue un enjeu majeur de souveraineté nationale.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour appréhender au mieux des attaques en déni de service:

- L'ANSSI fournit un guide destiné aux responsables de sécurité des systèmes d'information pour comprendre et anticiper les attaques DDoS,
- Vous pouvez suivre les conseils d'assistance et de prévention de cybermalveillance.gouv.fr et consulter notamment la fiche guide relative aux attaques DDoS de site web,
- Vous devez déposer plainte, si vous êtes victime, au commissariat de police ou à la brigade de gendarmerie le plus proche. Les articles 323-1 à 323-7 du Code pénal prévoient une sanction en cas d'entrave à un système de traitement automatisé des données (STAD).
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES INFORMATIQUES
La défiguration de site

OU COMMENT PERDRE LA FACE !

La défiguration d'un site web se caractérise par une ***altération visuelle*** de l'une de ses pages par un attaquant dont les motivations peuvent être très diverses**.** La nouvelle apparence du site web attaqué peut alors comporter des messages, images et vidéos sans rapport avec l'objet initial du site. Si l'attaque revêt un caractère virtuel, le préjudice subi peut quant à lui avoir des conséquences bien réelles sur la continuité de l'activité de l'entité visée (discrédit, vol de données, perte d'exploitation, etc.).

ENTRE QUÊTE DE NOTORIÉTÉ ET IDÉOLOGIE

Dans la très grande majorité des cas, l'auteur d'une défiguration de site web cherchera à la revendiquer et à faire la démonstration de son « exploit ». Ses motivations peuvent être toutefois de plusieurs natures, à savoir:

- Rechercher à accroitre sa ***notoriété*** dans l'univers des hackers,
- Transmettre un ***message*** à caractère ***idéologique*** ou ***politique***,
- Entamer ***la réputation*** de l'entité visée,

Quelles que soient ses motivations, l'attaquant pourra profiter de l'accès frauduleux au système de traitement de données automatisé (STAD) pour commettre un ***vol de données sensibles***, pour ensuite les revendre ou poursuivre ses activités frauduleuses.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

ENTRE SANCTIONS ET OBLIGATIONS

Réprimer les atteintes aux systèmes de traitement automatisé de données (STAD)

Fondées à l'origine sur la loi dite « Godfrain » de 1988, la sanction des atteintes aux STAD a depuis été sensiblement renforcée. Les articles 323-1 et suivants du Code pénal prévoient notamment que le fait « *d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données (…)* » contenues dans un STAD est puni de 5 ans d'emprisonnement et de 150 000€ d'amende (initialement fixé à 75 000€, ce montant a été révisé par l'art 4 de la loi du 24 juillet 2015 relative au renseignement).

Obligation de notifier toute violation à un traitement de données automatisé

Depuis le 25 mai 2018, le Règlement général européen sur la protection des données (RGPD) impose aux entreprises et aux organisations de revoir toute leur architecture de collecte et de traitement des données personnelles de leurs utilisateurs.

Ainsi, l'art 33 du règlement oblige le responsable du traitement de données victime d'une atteinte à son STAD de notifier la violation dans les 72H à l'autorité de contrôle (CNIL), sous peine de sanctions et amendes administratives !

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous êtes victime d'une défiguration de site web, ou souhaitez réduire votre exposition au risque, vous devez:

- Observer une politique rigoureuse de sécurité de vos systèmes d'information et tenir régulièrement à jour votre système d'exploitation,
- Suivre les conseils d'assistance et de prévention de cybermalveillance.gouv.fr et consulter notamment la fiche guide relative à la défiguration de site web,
- Sensibiliser votre entourage et inciter au renforcement des mots de passe en suivant les conseils de l'ANSSI et en en appliquant la méthode proposée par la CNIL,
- Conscients des enjeux pour la sécurité, la justice et les libertés publiques, l'INHESJ et l'IHEDN ont décidé, avec leurs partenaires, de proposer une formation de haut niveau, candidatez !
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES RISQUES INFORMATIQUES
Les risques liés au BYOD

SÉCURISER ET MAITRISER SON RÉSEAU

L'acronyme « *BYOD* » est l'abréviation de l'expression anglaise «***Bring Your Own Device***» («Apportez Votre Propre Matériel»). Cet expression désigne ***l'emploi d'équipements informatiques personnels dans une sphère professionnelle.*** Véritable casse-tête pour les responsables en charge de la sécurité des systèmes d'information, la gestion des risques informatiques leur impose de prendre aussi bien en compte les évolutions technologiques que sociétales ou juridiques. On oublie trop souvent que ***si le réseau permet de partager des informations, il peut aussi propager les infections*** de codes malveillants.

SÉPARER LES USAGES PERSONNELS DES USAGES PROFESSIONNELS

L'utilisation d'équipement personnel à des fins professionnelles constitue un ***risque pour la sécurité et la confidentialité des données de l'entreprise***, en ce sens que les moyens de contrôle de l'employeur devront nécessairement se heurter au respect des libertés individuelles des salariés. L'ANSSI et CPME préconisent ainsi, dans leur guide des bonnes pratiques de l'informatique (règle n°11), de séparer les usages personnels des usages professionnels comme par exemple:

- Ne pas faire suivre ses messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles,
- Ne pas héberger de données professionnelles sur des équipements personnels,
- Eviter de connecter des supports amovibles personnels aux ordinateurs de l'entreprise.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

DOIT-ON CHOISIR ENTRE SÉCURITÉ, VIE PRIVÉE ET MOBILITÉ ?

Le dilemme

Les risques liés au phénomène BYOD se situent à la convergence de plusieurs éléments qui tiennent à la fois à:

- La démocratisation des équipements informatiques personnels, lesquels sont souvent plus performants ou récents que les équipements mis à disposition dans les entreprises,
- Aux situations de mobilité des salariés et à leur volonté d'utiliser des terminaux ou logiciels qu'ils maitrisent.

Ainsi, une gestion trop stricte par le responsable informatique peut conduire au mécontentement des salariés, voire entamer les avantages que l'on peut tirer de leur mobilité.

Télétravail

Dans la prévention des risques liés au BYOD, la sécurité des systèmes d'information doit désormais ***prendre en compte le télétravail***. Intégré dans les dispositions de l'article L1222-9 du code du travail, il constitue une ***évolution tant sociétale que légale***.

Le site Service-Public.fr met à disposition une fiche pratique (F13851) des plus instructives sur le sujet.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Si vous souhaitez réduire les risques liés aux BYOD, vous pouvez:

- Vous intéresser davantage à la protection des données en limitant, par exemple l'accès à partir d'appareils ou en direction de répertoires considérés comme sensibles.
- Prendre des mesures sur le plan organisationnel (gestion des accès, formation, mise à jour des logiciels, etc.), et vous préparer à une gestion de crise.
- L'élaboration un plan de continuité d'activité (PCA) peut contribuer au renforcement de la résilience de votre entreprise,
- Engager une véritable réflexion sur la responsabilisation de chaque salarié au regard des risques informatiques et des contrats d'assurance souscrits par l'entreprise. La Fédération Française de l'Assurance a rédigé un guide qui pourra vous accompagner dans cette réflexion.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.

Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.

Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILITÉS HUMAINES
L'ingénierie sociale

PERSUASION OU MANIPULATION ?

L'ANSSI définit l'"ingénierie sociale comme une « ***manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité*** de tierces personnes ». Approche à la fois psychologique et systémique, l'ingénierie sociale permet à des personnes malintentionnées de ***manipuler un individu, en vue d'obtenir de sa part des informations stratégiques ou des comportements inadaptés***.
Constituant l'un des moyens les plus exploités par les auteurs d'escroqueries économiques et financières pour parvenir à leurs fins, l'ingénierie sociale fragilise chaque année de nombreuses entreprises, quand elle n'entraine pas tout simplement leur perte. Les personnes physiques qui en sont victimes subissent un réel traumatisme qu'elles ont beaucoup de mal à surmonter.

DES ATOUTS POUR CONVAINCRE

Technique de communication par nature intrusive, ***l'ingénierie sociale n'est pas pour autant illégale***. Dans la plupart des cas, elle s'appuie sur une étude préalable des environnements personnel et professionnel de la future victime. La personne malintentionnée cherchera alors à établir dans un premier temps une relation de confiance avant d'entrer ensuite en ***contact direct*** avec son interlocuteur, soit par ***médias sociaux*** interposés, soit par ***courrier électronique***, soit par ***téléphone***. Même si elle expose son auteur à davantage de risques, la recherche d'une relation directe par contact physique ne doit pas être écartée.
Dans son rapport sur l'état de la menace lié au numérique pour l'année 2018, le délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces (DMISC) rappelle que les techniques d'ingénierie sociale et les vulnérabilités résiduelles touchent une entreprise sur deux !

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

FAUX PRÉSIDENT, FAUX VIREMENT, MAIS VRAIE ESCROQUERIE !

L'ingénierie sociale permet, à ceux qui en exploitent les ressorts et les ressources, de commettre des escroqueries toujours plus sophistiquées. Pourtant, dans la majeure partie des cas, les fraudeurs ***exploitent une faille humaine et des faiblesses organisationnelles***.

A titre d'exemple, l'escroquerie dite des faux ordres de virement internationaux ou du faux président, vise à obtenir par des moyens frauduleux (faux nom ou fausse qualité, mise en scène, etc.) la remise de fonds par virement bancaire.

Quelques mesures simples suffisent parfois à réduire les risques:

- Toujours vérifier l'identité de son interlocuteur par un rappel sur des coordonnées identifiées,
- Vérifier systématiquement l'adresse courriel de son correspondant,
- Instaurer une procédure de séparation des pouvoirs en matière de saisie et de validation,
- Exclure les paiements de fin de semaine afin être en mesure de réagir rapidement auprès des banques en cas d'atteinte avérée, etc.
- N'hésitez pas à suivre les conseils de la fédération bancaire française.
- Par ailleurs, l'ANSSI et CPME mettent à disposition un guide de bonne pratique des plus utiles.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour limiter les risques de fraude liée à l'ingénierie sociale, vous devez en interne:

- Limiter la perte de données sensibles en rappelant à chaque salarié et collaborateur de l'entreprise la nécessité de conserver un usage prudent des réseaux sociaux,
- Préserver les bases clients et fournisseurs en instaurant des procédures de sécurité des systèmes d'information rigoureuses,
- Sensibiliser sur les indices qui peuvent alerter (demande de changement de compte, changement de coordonnées, incitation à faire un test de virement, demande de prise de contrôle à distance, etc.), et renouveler régulièrement ces séances de sensibilisation,
- Former les équipes en charge de la trésorerie et des opérations de comptabilité,
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILITÉS HUMAINES
La pression ou menace sur client

DÉFAIRE LE MYTHE DE L'ACHETEUR TOUT PUISSANT

Dans une relation commerciale, les acheteurs ont naturellement ***tendance à penser qu'ils se situent en position de force*** vis-à-vis de leur fournisseur. Pourtant, la réalité apparait comme un peu plus nuancée, les clients pouvant être ***exposés à de nombreux risques et pressions***. C'est notamment le cas lorsque le fournisseur se trouve dans une position monopolistique ou lorsque la demande s'avère supérieure à l'offre.

GÉRER LE RISQUE FOURNISSEUR

Fournisseur prédominant ou monopolistique

- Le fournisseur prédominant ne revêt ***pas forcément un caractère nuisible*** en ce sens que la relation commerciale qu'il entretient avec son client peut être de nature tout à fait saine, et ne mettre en évidence aucun rapport de force. En revanche, parce que ce fournisseur constitue l'***unique sous-traitant***, ou parce qu'il représente la ***majeure partie du chiffre d'affaires*** de son donneur d'ordres, le risque qu'il fait porter à ce dernier peut être fatal en cas de défaillance.
- Indépendamment de sa taille, un fournisseur peut constituer un risque pour le client du fait de sa ***position monopolistique*** liée à la ***détention d'un brevet ou une avance technologique***. Toutefois, l'article L. 420-2 du Code du Commerce réprime l'abus de positionnement dominante comme le refus de vente ou des ventes liées à des conditions discriminatoires. Pour que cet abus soit caractérisé, ***trois conditions*** doivent être réunies:
    - l'existence d'une position dominante sur un marché,
    - une exploitation abusive de cette position,
    - un objet ou un effet restrictif de concurrence sur un marché. L'existence d'effets réels n'est pas indispensable. La potentialité d'effet(s) suffit à caractériser la pratique.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Conditions Générales de Vente (CGV) versus Conditions Générales d'Achat (CGA)

L'article L441-6-I du Code du Commerce dispose que « Tout producteur, prestataire de services [..] ***est tenu de communiquer ses conditions générales de vente à tout acheteur*** de produits ou tout demandeur de prestations de services qui en fait la demande pour une activité professionnelle ». Ces conditions comprennent notamment les conditions de vente, le barème des prix unitaires, les réductions de prix, et les conditions de règlement.

Si la loi précise donc que les CGV constituent le socle de la négociation, ***le client reste libre d'imposer en lieu et place ses Conditions Générales d'Achat***. Tout début d'exécution de la commande vaudra alors acceptation expresse des CGA et renonciation du fournisseur à ses propres conditions.

LA MÉDIATION POUR APAISER LES TENSIONS !

Lorsque la gestion des risques fournisseur n'est pas suffisamment prise en compte par les directions achat, le recours à un dispositif de médiation peut être une sage décision.

Le médiateur des entreprises: un dispositif récent et efficient pour les TPE/PME

Le médiateur des entreprises se propose de résoudre de façon amiable, un différend entre deux acteurs économiques. Efficace dans 75% des cas, la médiation offre les bénéfices d'une procédure ***gratuite***, ***rapide***, ***impartiale*** et ***confidentielle***.

Le Médiateur des entreprises reste par ailleurs ***neutre*** et ***indépendant***. Depuis le décret n° 2018-919 du 26 octobre 2018, ce dispositif de médiation a été ***étendu aux litiges opposant les entreprises avec l'administration.***
Il peut être mis en oeuvre à l'initiative de l'une ou l'autre des parties.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

A titre complémentaire, nous vous informons de l'existence:

- D'un Guide pour la qualité des relations contractuelles clients-fournisseurs,
- D'un Kit de confiance pour des relations fournisseur responsables. Commun aux deux parties, il vise à guider clients et fournisseurs dans leur première rencontre. Axé autour de sept objectifs, ce kit présente de manière succincte les thèmes à aborder.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILITÉS HUMAINES
La pression ou menace sur fournisseur

LE CLIENT N'EST PAS TOUJOURS ROI !

Satisfaire ses clients doit demeurer la ***préoccupation principale de toute entreprise*** qui souhaite évoluer et prospérer dans un contexte commercial où la concurrence et la pression se veulent sans cesse plus prégnantes. Dans la plupart des cas, la satisfaction client s'inscrit surtout dans une stratégie d'amélioration continue. Pour autant, s'il on a l'habitude de clamer que le client est roi, il peut être utile de rappeler que ***les droits dont il dispose sur son fournisseur sont limités et*** notamment ***encadrés*** par le Code Civil, le Code du Commerce et la loi de 1975 relative à la sous-traitance. Interdire les mauvaises pratiques demeure l'un des effets majeurs recherchés.

SUIVEZ LE GUIDE !

Chaque année, nombreux sont les chefs d'entreprise qui soulignent le déséquilibre des relations entre donneurs d'ordre et sous-traitants.

- S'appuyant sur un Rapport du Médiateur des relations inter-entreprises industrielles et de la sous-traitance de 2010, un ***Guide pour la qualité des relations contractuelles clients-fournisseurs*** a été réalisé.
- Ce guide ***illustre*** les différents ***comportements abusifs ou mauvaises pratiques d'entreprises*** qui sont régulièrement constatés et ***rappelle*** succinctement les ***règles applicables*** en matière de commande, de relation contractuelle, de prix, de réception et de facturation, de paiement, ou encore de propriété intellectuelle.
- Retrouver davantage de publications et d'informations sur le site du Médiateur des entreprises.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

VISER DES COMPORTEMENTS ET ACHATS RESPONSABLES

La Norme ISO 20400 pour des acheteurs responsables

Fruit d'un consensus international pour lequel près de 90 pays ont contribué, l'ISO 26000 est l'unique norme internationale qui vise à ***fournir aux organisations les lignes directrices*** de la responsabilité sociétale des entreprises.

Publiée en 2017 par l'organisation internationale de la normalisation, la Norme ISO 20400 l'enrichit en fixant des lignes directrices pour des Achats Responsables. Son objectif est d'***aider les organisations à assumer leurs responsabilités*** en matière de responsabilité sociétale en leur permettant d'appréhender la notion d'achat responsable, comprenant notamment les impacts de leur mise en oeuvre.

Le Label Relations Fournisseurs & Achats Responsable

S'inscrivant dans le prolongement de la mise en oeuvre d'une Charte Relations Fournisseurs Responsables, ce Label certifie et distingue les entreprises et les acteurs publics ayant fait la preuve de leur attachement à des pratiques d'achats responsables et vertueuses. Il a été décerné pour la première fois en 2012 par la Médiation des entreprises et le Conseil National des Achats.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

A titre complémentaire, nous vous rappelons que:

- Parce que certains clients se révèlent nuisibles à l'entreprise (les négociateurs trop féroces, les mauvais payeurs, etc.), les identifier, et rompre les relations commerciales qui vous lient, favorisera, dans la plupart des cas, la sortie d'un contexte d'insécurité économique.
- Chaque année, le « Prix des délais de paiement » récompense les acteurs publics et les entreprises qui oeuvrent à la réduction des délais de règlement.
- Le Baromètre Médiateur des entreprises - Sidetrade publie chaque trimestre le taux de factures bloquées pour les sociétés ainsi que la durée moyenne de résolution des anomalies.
- Destinée aux fournisseurs de biens ou de services, la clause de réserve de propriété permet, sous certaines conditions, de revendiquer une créance lorsque le débiteur est concerné par une procédure collective (liquidation judiciaire ou redressement), permettant ainsi de contourner les dispositions de l'article L 622-7 du Code du Commerce.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILITÉS HUMAINES
Les dérives personnelles

QUAND LES COMPORTEMENTS INDIVIDUELS PEUVENT NUIRE À L'ENTREPRISE…

Les dérives personnelles regroupent des ***comportements individuels qui par leur nature peuvent nuire à l'image ou au bon fonctionnement d'une entreprise***. Les manifestations de ces dérives peuvent prendre leur source dans des origines très diverses, qu'il s'agisse d'actes de délinquance, de conduites addictives (alcoolisme par exemple), de diversité culturelle ou parfois même de conflits familiaux. Chacun des acteurs de l'entreprise peut être concerné, qu'il soit cadre dirigeant ou juste salarié. La prévention et la prise en compte au plus tôt de ces situations conflictuelles peut contribuer à réduire considérablement les risques.

DES MANIFESTATIONS TRÈS DIVERSES

Quand la famille part à la dérive !

Les entreprises familiales sont souvent citées en exemple pour leur capacité de résilience et leur très grande stabilité. Profitant d'un management plus proche et de la fidélité des salariés, la prise de décisions stratégiques y est souvent rendue plus aisée. Pour autant, ce cadre idyllique peut très vite disparaitre lorsque des divergences ou des dissensions familiales se font jour, pouvant conduire à des situations de blocage ou de paralysie.

Il importe dès lors que la responsabilité de chaque dirigeant soit clairement établie et que les questions relatives à la succession soient, par exemple, préparées en amont. Les spécialistes du sujet préconisent notamment de solliciter un regard extérieur à la famille pour disposer d'une vision dépassionnée de la situation conflictuelle.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Les dérives liées aux mouvements sectaires

En matière de risque sectaire, la dérive comportementale se trouve renforcée par une emprise mentale sur la personne concernée. ***L'influence sur les décisions stratégiques de l'entreprise et la réalisation d'escroqueries économiques et financières*** sont les conséquences le plus souvent observées.

La Mission interministérielle de vigilance et de lutte contre les dérives sectaires (***MIVILUDES***) met à disposition sur son site un ensemble de guides, dont celui de « ***L'entreprise face au risque sectaire*** » qui vous permettra de repérer ce risque, de mieux le prendre en compte, et d'y remédier de la manière la plus efficiente, le cas échéant.

LES OBLIGATIONS DE L'EMPLOYEUR

Les articles L4121-1 et suivants du Code du Travail imposent à l'employeur de prendre les mesures nécessaires pour assurer la sécurité et la santé physique ou mentale des salariés. Il doit ainsi prévenir toute forme de harcèlement.

Le cas des agissements sexistes

Définis à l'article L1142-2-1 du Code du travail, les agissements sexistes ne sont pas pénalement sanctionnés. La responsabilité de l'employeur demeure entière sur le plan civil et des sanctions disciplinaires peuvent être prises à l'encontre de la personne incriminée.

De nouvelles obligations en matière de harcèlement sexuel

Depuis le 1er janvier 2019, l'employeur doit prendre certaines mesures pour prévenir et mettre fin aux cas de harcèlement sexuel. ***Pour les entreprises de plus de 250 salariés, un référent doit être désigné***.

Le site Service-Public-Pro.fr (A13219) rappelle ces obligations, lesquelles sont définies aux articles 222-33-2-2 du Code Pénal et L1153-1 et suivants du Code du Travail.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour aller plus loin en matière de dérives personnelles, n'oubliez pas que:

- Le règlement intérieur de l'entreprise revêt une importance toute particulière dans la mesure où il fixe les obligations à respecter par l'employeur et les salariés. Le site Service-Public-Pro.fr (F1905) en dresse les contours et vous rappelle les dispositions légales du Code du Travail.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILITÉS HUMAINES
L'absentéisme

DES COÛTS POUR LA SOCIÉTÉ, DES RISQUES POUR L'ENTREPRISE

Il n'existe pas de définition universelle de l'absentéisme au travail. Mais quelle qu'en soit la définition, ***l'absentéisme ne saurait être réduit à la seule absence de son poste de travail***, cette absence pouvant être par ailleurs justifiée. Si les critères de comptabilisation de l'absentéisme sont assez bien définis, il est souvent très ***utile pour les entreprises d'en déterminer les causes, qu'elles soient techniques, organisationnelles ou comportementales***. Le dernier rapport de la Commission des comptes de la Sécurité sociale nous apprend ainsi que les seules indemnités pour arrêts-maladie versées dans le secteur privé ont atteint plus de 10 milliards d'euros en 2017 (+4,4% en un an). Les coûts estimés de l'absentéisme pour la fonction publique seraient équivalents.

UN ÉLÉMENT DU BILAN SOCIAL ET ÉCONOMIQUE DE L'ENTREPRISE

Pour toutes les entreprises d'au moins 50 salariés, l'employeur est tenu de mettre en oeuvre une base de données économiques et sociales au profit du comité ad hoc et des représentants des personnels. Le site Service-Public-Pro (F32193) vous fournit des éléments de compréhension sur cette base de données.

L'absentéisme: un critère d 'évaluation pour les entreprises d'au moins 300 salariés

L'article R2323-1-3 du Code du Travail dispose que ***les entreprises d'au moins trois cents salariés, sont tenues de mettre en oeuvre une base de données*** qui comporte une présentation de la ***situation de l'entreprise***, notamment le chiffre d'affaires, la valeur ajoutée, le résultat d'exploitation et le résultat net. Cette base de données qui se veut exhaustive, doit faire apparaitre les éléments relatifs à ***l'absentéisme*** (A-Investissements / g) Conditions de travail).

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Les critères de calcul du taux d'absentéisme

Le taux d'absentéisme peut être évalué par les organisations de diverses manières:

- Soit en prenant en compte seulement l'absentéisme pour raison de santé, c'est-à-dire, les accidents de travail, les arrêts maladie et maladies professionnelles et les congés maternité),
- Soit en prenant également en compte les autres évènements familiaux, les grèves, les retards et absences injustifiées.

L'article R2323-17 du Code du Travail fournit la liste des informations précises qui devront figurer dans le bilan social d'entreprise et dans le bilan social d'établissement (voir § 1.8).

DÉPISTER LES SITUATIONS PROBLÉMATIQUES AU TRAVAIL

L'Institut national de recherche et de sécurité pour la prévention des accidents du travail et des maladies professionnelles (INRS) indique dans une étude récente que ***l'absentéisme constitue un indicateur fréquemment utilisé dans le dépistage des situations de travail problématiques*** du point de vue des risques psychosociaux.

L'étape suivante consistera dès lors à en comprendre les causes, lesquelles peuvent prendre leur origine dans:

- Une usure professionnelle (pénibilité, lassitude, etc.),
- Une dégradation des conditions de travail liée à un management mal adapté, une pression trop forte sur les salariés, etc,
- Une communication insuffisante et une absence de perspective à moyen et long terme, etc.

Les articles L4121-1 et suivants du Code du travail ***obligent l'employeur*** à prendre les mesures nécessaires pour ***assurer la sécurité et protéger la santé physique et mentale des travailleurs***. De son côté, tout travailleur confronté à un danger grave et imminent pour sa vie ou sa santé dispose d'un ***droit de retrait***, conformément à l'article L4131-1 du Code du Travail.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Vous êtes employeur et vous souhaitez lutter contre l'absentéisme tout en agissant pour la sécurité et la santé au travail:

- Le site Service-Public.fr (N492) consacre un dossier sur les conditions de travail dans le secteur privé, avec de nombreuses questions-réponses.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES FRAGILITÉS HUMAINES
La clause de confidentialité

ALLER PLUS LOIN QUE LE CONTRAT DE CONFIANCE

L'information est une ressource stratégique, et le ***patrimoine immatériel*** développé au sein d'une entreprise ***doit être protégé de toute action prédatrice.*** Aussi, un employeur pourra s'engager dans une démarche de sécurité juridique qui dépasse les seuls liens de confiance créés avec les salariés.

La clause de confidentialité en constitue l'un des exemples concrets. Inséré dans un contrat de travail, elle ***impose au salarié de garder confidentielles certaines informations*** qui lui ont été communiquées dans le cadre professionnel et peut s'insérer dans n'importe quel contrat de travail.

- La clause de confidentialité s'applique au salarié dans sa relation avec des tiers, que ce soit en interne ou en dehors de la société.
- La Cour de Cassation précise dans un jurisprudence de 2008 que l'obligation faite au salarié se poursuit après la rupture du contrat de travail, sous réserve d'avoir été spécifiée dans la clause.

DROITS ET OBLIGATIONS EN MATIÈRE DE CONFIDENTIALITÉ

L'obligation de confidentialité: un principe légal

Même en l'absence de toute clause signée entre l'employeur et son salarié, l'article 1112-2 du Code Civil dispose que ce dernier est soumis à une ***obligation légale de confidentialité vis-vis-vis de son entreprise***. Toutefois, en cas de non respect, l'employeur devra prouver le lien de causalité entre le préjudice subi et la divulgation de l'information confidentielle, s'il veut prétendre à l'obtention de dommages et intérêts. ***Cette obligation*** faite au salarié cesse ***à la rupture du contrat de travail***.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

La clause de confidentialité: des conditions de fond et de forme à respecter

Pour être opposable au salarié, la clause de confidentialité doit respecter un certain formalisme:

- ***Sur le fond***, la nature exacte des informations que le salarié s'engage à ne pas divulguer doit être mentionnée. L'employeur pourra évoquer des informations spécifiques ou rester plus évasif en évoquant par exemple « toute information de nature à nuire à l'entreprise ».
- L'article L1121-1 du Code du Travail impose à l'employeur deux contraintes: justifier la clause par la nature de la tâche à accomplir et rester proportionné par rapport au but recherché.
- ***Sur la forme***, la clause de confidentialité doit être univoque et rédigée par écrit à défaut de nullité. Les conventions collectives peuvent imposer un formalisme particulier.

La clause de confidentialité doit être différenciée d'autres dispositifs juridiques

- A la différence d'une ***clause de non-concurrence***, la validité d'une clause de confidentialité n'exige pas le versement par l'employeur d'une contrepartie financière au salarié.
- La ***divulgation de savoir-faire*** constitue un acte de concurrence déloyale qui expose son auteur à des dommages et intérêts sur le fondement légal de l'article 1240 du Code Civil. Par ailleurs, l'article L1227-1 du Code du Travail sanctionne les ***atteintes au secret de fabrication***.
- Les ***atteintes au secret professionnel*** sont réprimées par l'article 226-13 du Code Pénal.

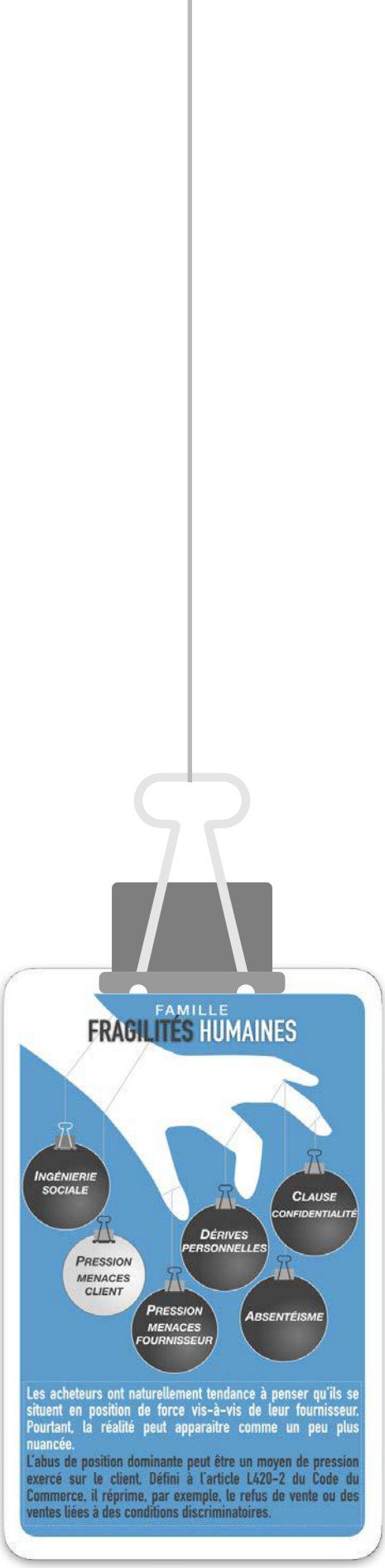
RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

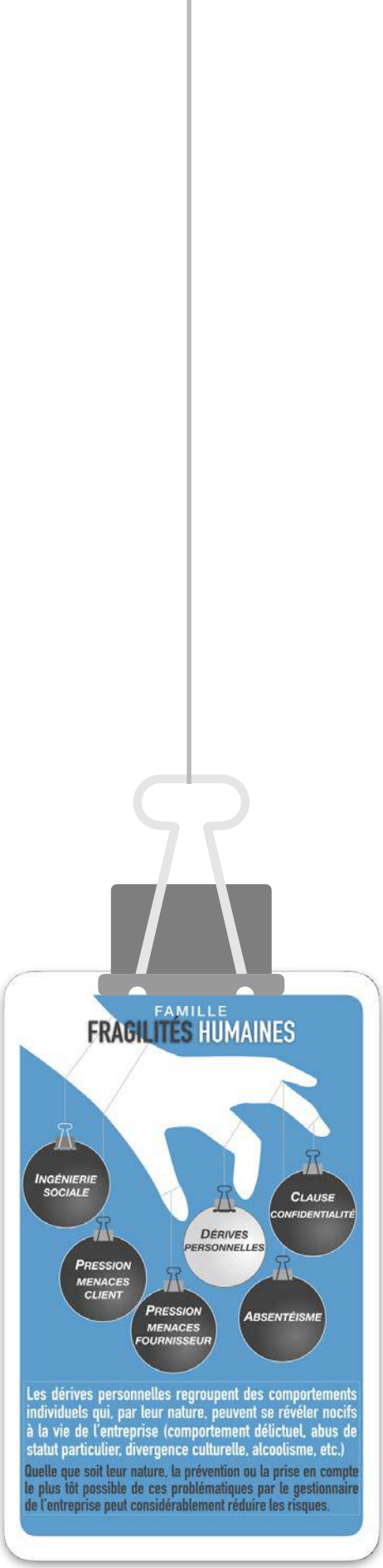
En cas de litige relatif à une clause de confidentialité, vous devez savoir que:

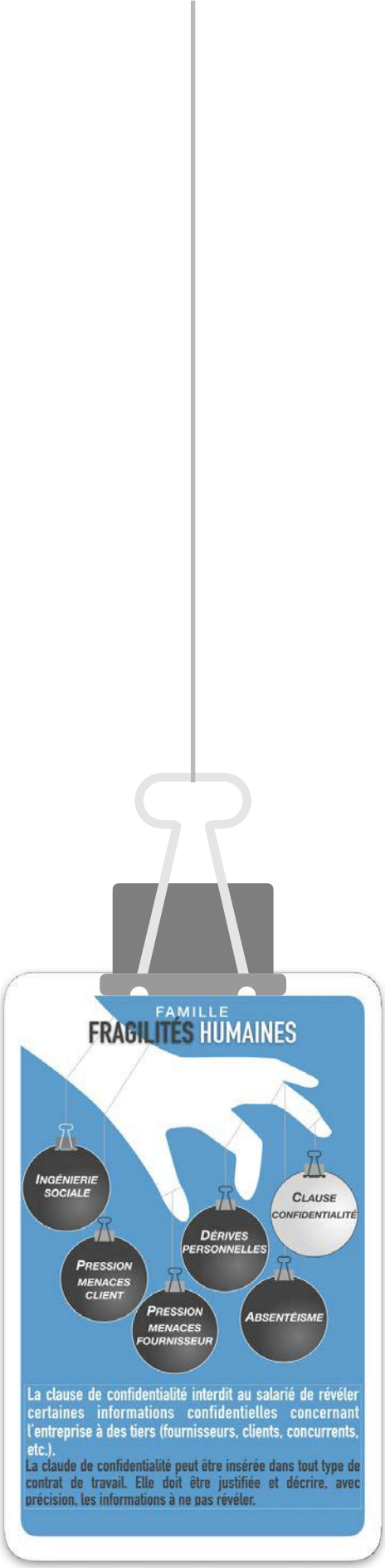
- Indépendamment des infractions à la loi pénale qui pourraient être constatées, le non-respect d'une clause de confidentialité pourra être porté devant le Conseil des Prud'hommes. Le site Service-Public.fr (F1052) vous explique le déroulement d'une procédure.
- La Circulaire NOR JUSC1614424C du 27 mai 2016 précise en détail la procédure prud'homale et son traitement judiciaire. 13 fiches techniques figurent en annexe de cette circulaire.
- Quelle que soit la situation, le recours aux services d'un avocat-conseil devra être privilégié, notamment s'il s'agit de matérialiser au mieux un acte de concurrence déloyale, de faire valoir la portée et la nature d'un préjudice ou de démontrer la faute lourde du salarié.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT



Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT





Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES À LA RÉPUTATION
Les attaques informationnelles

L'INFORMATION: UNE ARME PAR DESTINATION

Une attaque informationnelle consiste en l'utilisation de la connaissance pour attaquer un adversaire. ***Les médias sociaux sont alors exploités comme une caisse de résonance.*** Elle vise à nuire intentionnellement à une entité identifiable (personne physique ou morale, marque, technologie, etc.), ou à ses intérêts. L'auteur d'une attaque informationnelle peut-être un particulier agissant par colère, vengeance, frustration, ou autre motivation personnelle. Il peut aussi s'agir d'individus agissant au service d'intérêts concurrents. L'attaque informationnelle peut être menée de manière directe, ou de manière indirecte par l'utilisation d'intermédiaires qui s'approprient le contenu de l'attaque. Généralement les attaques informationnelles sont basées, en grande majorité, sur des éléments réels, tangibles et vérifiables. La véracité de l'information utilisée est gage du succès de l'attaque.

TYPOLOGIE DES ATTAQUES INFORMATIONNELLES ET ENJEUX

Le développement des nouvelles technologies de l'information et de la communication, la numérisation de l'économie, la facilité d'accès à l'information et le faible coût de sa mise en œuvre, font de l'attaque informationnelle un outil extrêmement puissant et accessible à tous. Identifier et contrer des attaques informationnelles constitue un enjeu crucial pour la survie des entreprises victimes.

Les attaques informationnelles peuvent se matérialiser sous la forme:

- d'avis négatifs,
- de rumeurs,
- de fausses informations ou d'un dénigrement.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

UN EXEMPLE D'ATTAQUE INFORMATIONNELLE

Action offensive d'ONG françaises et américaines sur le secteur de l'aquaculture marine française.

Récemment, le secteur de l'aquaculture marine française a été victime d'attaques informationnelles de la part d'une ONG française. Cette dernière dénonce l'utilisation de poissons sauvages pour produire de l'alimentation animale destinée aux poissons d'élevage. Elle collabore avec de nombreuses ONG internationales, essentiellement américaines, et mène des actions de lobbying auprès des Institutions européennes dans le but de réglementer la pêche minotière et l'utilisation des huiles et farines de poissons à d'autres fins que l'alimentation humaine.

Orientées vers l'aquaculture française et du sud de l'Europe, ces attaques informationnelles se caractérisent par une manœuvre de déstabilisation et la volonté d'affaiblir la filière. L'argumentaire employé repose sur une information vraie (poissons sauvages pour nourrir des poissons d'élevage) et s'appuie sur des relais écologistes via les réseaux sociaux notamment.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Les attaques informationnelles peuvent avoir un effet dévastateur pour l'entreprise. Si vous en êtes victime, et souhaitez en amenuiser les effets, vous devez:

- Prêter une attention toute particulière à ce qui se dit sur vous ou votre entité (veille),
- Définir une ligne éditoriale visant à maitriser votre communication,
- Vous préparer à ester en justice en identifiant les actes réprimés par la loi pénale comme par exemple la diffamation, l'injure, ou le dénigrement,
- Vous préparer à la communication de crise (être réactif, mais ne pas agir de manière irréfléchie),
- Pour information, la loi 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information vise à garantir une information juste et loyale des citoyens pendant les élections.
- Par ailleurs, les départements Intelligence et Sécurité Économiques et Risques et Crises de l'INHESJ vous proposent des formations de haut niveau qui incluent la mise en place d'une veille informative et la gestion de crise en mode dégradé.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES À LA RÉPUTATION
Les attaques sur l'identité de l'entreprise

L'IDENTITÉ DE L'ENTREPRISE: UN MARQUEUR ESSENTIEL

Aborder l'identité d'une entreprise peut parfois faire débat dans la mesure où cela interroge sur les fondements d'une histoire, d'une culture, d'un projet, voire d'une image. Dans bien des cas, elle traduit une stratégie de positionnement vis-à-vis de ses concurrents. Quel que soit le cas, ***l'identité de l'entreprise correspond aux traits marquants qui permettent de la reconnaître***, à savoir:

- Son design, sa marque ou son logo,
- Sa communication, en interne comme en externe, et par le truchement des médias sociaux,
- Son comportement, notamment déontologique et environnemental.

Ainsi, une simple attaque sur l'identité de l'entreprise peut suffire à entamer sa réputation, et distendre un lien de confiance qui aura pourtant mis du temps à s'établir avec les clients et autres partenaires. Se préparer à cette éventualité, c'est prendre les dispositions nécessaires pour en diminuer les effets.

DIFFAMATION, INJURE OU DÉNIGREMENT ?

Les attaques sur l'identité de l'entreprise peuvent prendre plusieurs formes. Les situations de diffamation, d'injure ou de dénigrement sont fréquemment rencontrées et il importe, dès lors, d'en définir plus précisément leur portée. La diffamation est l'allégation ou l'imputation d'un fait qui porte ***atteinte à l'honneur ou à la considération*** d'une personne physique ou morale, cette dernière étant souvent la principale victime du propos malveillant. ***Le fait allégué doit être vérifiable, car à défaut il relèvera de l'injure***. Le dénigrement se distingue de la diffamation et de l'injure en ce sens qu'il traduit un ***acte de concurrence déloyale*** (article 1240 du Code Civil). Par ailleurs, les faits de diffamation publique se prescrivent par 3 mois (1 an pour les diffamations racistes ou sexistes), alors que ce délai est porté à 5 ans pour le dénigrement.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

MÉDIAS SOCIAUX: ATTENTION DANGER !

Si la manipulation de l'information peut être considérée, à bien des égards, comme aussi ancienne que l'information elle-même, force est de constater que les médias sociaux sont devenus un véritable terrain de jeu pour la manipulation de l'information.

Vous avez dit obsfucation ?

Vous découvrez peut être ce mot et pourtant vous êtes régulièrement confronté à ses effets ! L'obsfucation est un ***procédé*** qui consiste essentiellement à publier, en grand volume, des informations orientées dans le sens que l'on souhaite, en vue de ***masquer ou dissimuler*** d'autres données. Technique employée au service de la protection de la e-réputation d'une entreprise, elle favorise par exemple la dissimulation de commentaires peu élogieux sur les forums et avis clients.

Promulgation d'une loi relative à la lutte contre la manipulation de l'information !

Les entreprises ne sont pas les seules à être confrontées à la transformation numérique qui s'opère et aux effets parfois déstabilisants des médias sociaux.

Conscients que les confrontations se constatent parfois à des niveaux inter-étatiques et qu'elles peuvent menacer le jeu démocratique, les parlementaires français se sont saisis du sujet pour aboutir, le 22 décembre 2018 à la promulgation de la ***loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*** et sa loi organique n° 2018-1201.

Par ailleurs, en septembre 2018, le centre d'analyse, de prévision et de stratégie (***CAPS***) et l'Institut de recherche stratégique de l'École militaire (***IRSEM***) rendaient public un rapport sur la manipulation de l'information, fruit d'une enquête menée dans 20 pays et mettant en exergue les risques pour nos démocraties.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Les entreprises ont largement investi les médias sociaux qui, bien que fourmillant d'opportunités, font peser de nombreux risques sur leur identité :

- La mise en place d'un dispositif de veille devra être recherchée en vue de se protéger, en priorité, d'un détournement de marque et toute usurpation d'identité.
- Pour toute autre question, la brigade numérique de la gendarmerie est à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES À LA RÉPUTATION
L'usurpation d'identité

UN MASQUE ET DES MAUX

Avec l'essor des nouvelles technologies de l'information et de la communication, les atteintes à la réputation se sont multipliées de manière exponentielle. L'usurpation d'identité en constitue l'un des vecteurs les plus significatifs.

Mais de quoi parle-t-on ?

Selon la CNIL, « L'usurpation d'identité consiste à ***utiliser, sans votre accord, des informations permettant de vous identifier*** [..]. Ces informations peuvent ensuite être ***utilisées à votre insu***, notamment pour souscrire sous votre identité un crédit, un abonnement, pour ***commettre des actes répréhensibles ou nuire à votre réputation*** ».

Employée par exemple à des fins d'escroquerie, l'usurpation peut porter préjudice à deux types de victimes, celle dont l'identité a été usurpée (et qui voit sa réputation entachée) et le tiers qui aura été trompé.

QUAND UN DÉLIT PEUT EN CACHER UN AUTRE !

Les personnes mises en cause pour des faits d'usurpation d'identité sont rarement poursuivies par les tribunaux civils et pénaux sur ce seul fondement juridique. Les préjudices subis par les personnes morales ou physiques peuvent être conséquents, et imposent que soient réunis les éléments matériels des infractions connexes. Parmi les infractions les plus fréquemment relevées, on trouve notamment:

- Les escroqueries au sens de l'article 313-1 du Code Pénal (5 ans + 375 000€ d'amende).
- Les faux et usages de faux au sens de l'article 441-1 et suivants du Code Pénal (jusqu'à 15 ans de réclusion criminelle + 225 000€ d'amende).

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

L'USURPATION DE L'IDENTITÉ NUMÉRIQUE: UNE RÉALITÉ…

L'article 434-23 du code pénal: l'usurpation d'identité avec intention de nuire !

L'article 434-23 du Code Pénal punit de cinq ans d'emprisonnement et de 75 000 euros d'amende « Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales ».

Autrement dit, l'auteur du délit usurpe l'identité de la victime dans le but de lui faire courir une mise en cause au plan pénal. A la lumière des faits constatés sur les canaux numériques, on observe que l'intention de nuire n'est pas toujours recherchée par l'auteur, ce qui limite l'emploi de ce fondement juridique.

L'article 9 du Code Civil pour faire cesser une atteinte à l'intimité de la vie privée !

Cet article 9 du Code civil dispose que « Les juges peuvent, [..], prescrire toutes mesures, [..], propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée [..] ».

L'article 226-4-1 du Code Pénal: l'usurpation d'identité numérique, un délit autonome !

Il aura fallu attendre 2011 et la loi d'orientation et de programmation pour la performance de la sécurité (LOPPSI 2) pour renforcer les moyens de lutte contre la cybercriminalité et créer un délit autonome d'usurpation de l'identité numérique. L'article 226-4-1 du Code Pénal réprime ce délit par un an d'emprisonnement et 75 000 € d'amende.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

En cas d'usurpation d'identité:

- Vous devez déposer plainte auprès du service d'enquête territorialement compétent,
- Si l'usurpation est relative à l'enregistrement de noms de domaine, l'Afnic procédera, après votre dépôt de plainte, au gel du nom de domaine. Le nom de domaine sera supprimé dès lors que le bureau d'enregistrement n'aura pu valider l'identité du titulaire, confirmant ainsi l'usurpation. Un guide de l'ayant droit est mis à disposition par l'Afnic.
- Suivez les conseils de la CNIL en cas d'usurpation d'identité en ligne et demandez au site d'intervenir sur Google, Facebook, Twitter, Snapchat,
- Pour toute autre action malveillante sur Internet, trouvez le contact qu'il vous faut,
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES À LA RÉPUTATION
Le respect de l'environnement

LA PROTECTION DU BIEN COMMUN

Constituant l'un des ***piliers majeurs de la responsabilité sociétale de l'entreprise*** (RSE), le respect de l'environnement figure par ailleurs ***au rang des principes constitutionnels*** ! En effet, la loi constitutionnelle 2005-205 du 1er mars 2005 a permis d'intégrer la charte de l'environnement de 2004 dans le préambule de la Constitution du 4 octobre 1958.

L'activité des entreprises et des organisations peut affecter plus ou moins durablement ***leur environnement*** naturel, voire humain. Il importe donc pour celles-ci, d'en maitriser les contours et de respecter les obligations légales environnementales auxquelles elles sont soumises. À défaut, leur réputation pourra s'en trouver durablement affectée.

LES PRIX ENTREPRISES ET ENVIRONNEMENT

Organisés chaque année par le ministère de la Transition écologique et solidaire (MTES) et l'Agence de l'environnement et de la maitrise de l'énergie (ADEME), sous la forme d'un ***concours national***, « les prix entreprises et environnement » ***récompensent les actions et projets exemplaires portés par les entreprises dans le domaine de l'environnement***. Ce dispositif représente un vecteur de communication non négligeable pour tout acteur économique.

- Ce prix correspond à l'étape française qui permet de concourir ensuite au niveau européen,
- Les associations ou groupements d'entreprises peuvent se porter candidats,
- Les prix entreprises et environnement comporte ***5 catégories*** (Économie circulaire, Lutte contre le changement climatique, Meilleure déclaration de performance extra-financière volet environnemental, Biodiversité et entreprises, Innovation dans les technologies et les modèles économiques).
- Consultez les modalités de dépôt d'un dossier de candidature.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

PROTECTION DE L'ENVIRONNEMENT: PRINCIPES ET OBLIGATIONS

Les développements ci-dessous ne constituent que quelques uns des dispositifs existant qui peuvent s'imposer aux entreprises et ne prétendent donc pas à l'exhaustivité.

Le principe de la responsabilité élargie des producteurs

Le principe de la responsabilité élargie des producteurs (REP) est fixé par les dispositions législatives de l'article L541-10 du Code de l'Environnement. Ce dernier impose aux producteurs, importateurs et distributeurs de produits ou éléments et matériaux générant des déchets, « de pourvoir ou de contribuer à la prévention et à la gestion des déchets qui en proviennent ».

Le risque économique lié à l'obligation de remise en état

Dans les cas où l'activité de l'entreprise relève d'une exploitation industrielle, les contraintes environnementales peuvent être plus élevées et faire naitre de nouvelles obligations en cas de cession ou cessation d'activité (remise en état). L'article L 512-6-1 du Code de l'Environnement précise même que le Préfet pourra, le cas échéant, « fixer des prescriptions de réhabilitations plus contraignantes ».

Le principe de pollueur-payeur et la responsabilité environnementale

La loi 2008-757 dite LRE du 1er août 2008 transpose en droit français la directive 2004/35/CE du Parlement européen et du Conseil du 21 avril 2004 sur la responsabilité environnementale.

Elle établit un cadre juridique fondé sur le principe du «pollueur-payeur» et ***vise à prévenir et réparer en nature les dommages environnementaux causés par les activités professionnelles*** qui peuvent concerner les masses d'eau, les espèces et les habitats protégés ou encore les sols.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Le respect de l'environnement est devenu au fil des ans un enjeu de santé publique à l'échelle mondiale et un facteur prépondérant pour la réputation des entreprises. Pour vous accompagner:

- L'ADEME précise les grands principes de la réglementation européenne sur les déchets.
- La fédération française des assurances (FFA) dresse un point de situation sur la responsabilité des entreprises du fait du préjudice écologique et de la responsabilité environnementale.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES À LA RÉPUTATION
La protection des données personnelles

UNE PROTECTION HARMONISÉE AU NIVEAU EUROPÉEN

Depuis le 25 mai 2018, le règlement (UE) 2016/976 relatif à la protection des données personnelles (RGPD) s'impose à l'ensemble des pays de l'Union Européenne et ***bouleverse,*** en grande partie, ***l'approche des entreprises*** en matière de ***traitement des données personnelles***.

Les entreprises sont tenues d'assurer une ***protection optimale des données*** à chaque instant et d'être en mesure de la ***démontrer en documentant leur conformité***. Des sanctions effectives, proportionnées et dissuasives peuvent être délivrées pour toute violation du règlement européen, indépendamment des conséquences engendrées sur la réputation pour l'entité concernée.

LES PRINCIPES DE LA PROTECTION DES DONNÉES PERSONNELLES

La protection des données personnelles est un ***droit fondamental*** qui a notamment été consacré en France par la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. ***La loi 2018-493 du 20 juin 2018 en constitue la nouvelle émanation*** et intègre les évolutions liées à la mise en oeuvre du RGPD.

La CNIL détermine 5 grands principes de protection des données personnelles, à savoir:

- Le principe de finalité (but bien précis, légal et légitime)
- Le principe de proportionnalité et de pertinence (strictement nécessaires au regard de la finalité)
- Le principe d'une durée de conservation limitée (durée de conservation précise).
- Le principe de sécurité et de confidentialité (accès aux seules personnes autorisées)
- Les droits des personnes (information et transparence)

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

QUELQUES ÉLÉMENTS DE COMPRÉHENSION

Que sont les données à caractère personnel ?

Elles recouvrent toutes les informations permettant, directement ou indirectement, l'identification d'une personne physique:

- Exemple: nom, prénom, téléphone, immatriculation, adresse IP, diplômes, etc.,
- Toutes les définitions sont mentionnées à l'art 4 du RGPD sur le site de la CNIL ou de l'UE.

Qu'est-ce qu'un traitement de données à caractère personnel ?

Toute opération ou ensemble d'opérations portant sur des données, soit:

- Les traitements automatisés,
- Les traitements non automatisés, si les données personnelles figurent dans des fichiers.
- L'art 5 du RGPD sur le site de la CNIL ou de l'UE, évoque les principes relatifs aux traitement de données à caractère personnel.

Pourquoi un Data Protection Officer (DPO) ?

La désignation d'un délégué à la protection des données est obligatoire dans les cas suivants:

- Le traitement est effectué par une autorité publique ou un organisme public,
- Les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement (suivi régulier, systématique, à grande échelle..),
- Suivi à grande échelle de données sensibles (révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, etc..),
- Voir art 37 du RGPD sur le site de la CNIL ou de l'UE.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour préserver votre réputation et aller encore plus loin dans la protection des données personnelles, vous pouvez:

- Découvrir ce qui change pour les professionnels en se rendant sur le site de la CNIL,
- Se préparer en 6 étapes en suivant les conseils de la CNIL,
- Appréhender le RGPD de manière interactive avec la Commission Européenne.
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

LES ATTEINTES À LA RÉPUTATION
La responsabilité sociétale de l'entreprise

QUAND L'ENTREPRISE INTERAGIT AVEC LA SOCIÉTÉ

La responsabilité sociétale des entreprises (RSE) s'est longtemps caractérisée par « ***L'intégration volontaire, par les entreprises, de préoccupations sociales*** et ***environnementales*** à leurs ***activités commerciales*** et leurs ***relations avec leurs parties prenantes*** ».

En 2011, la Commission européenne retenait, dans une Communication au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, une définition simplifiée de la RSE, à savoir « ***La responsabilité des entreprises vis-à-vis des effets qu'elles exercent sur la société*** », faisant ainsi disparaitre la notion "d'intégration volontaire ».

Si pour autant la RSE ne revêt pas, stricto sensu, un caractère obligatoire, force est de constater que la réglementation française et européenne s'est considérablement renforcée au cours des dernières années, rendant de fait obligatoire l'intégration de certains de ses aspects. ***Les enjeux en terme de réputation restent très élevés*** pour les entreprises qui seraient amenées à faire preuve de négligences dans ce domaine.

SUIVEZ LE GUIDE…DE L'ISO 26 000 !

Publiée en 2010, et fruit d'un consensus international pour lequel près de 90 pays ont contribué, l'ISO 26 000 est l'unique norme internationale qui vise à ***fournir aux organisations les lignes directrices de la responsabilité sociétale***. Elle n'est pas destinée à des fins de certification.

- Elle décrit les principes de la RSE et propose une méthode d'appropriation et de mise en oeuvre pour les organisations de toutes tailles et de tous secteurs.
- L'AFNOR vous propose de mieux cerner les contours de l'ISO 26 000 en 10 questions.

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

UN CADRE LÉGISLATIF ET RÉGLEMENTAIRE SOLIDE

Des enjeux environnementaux certains

Le Ministère de la Transition écologique et Solidaire précise sur son site que le cadre législatif et réglementaire de la France prend notamment en compte le pilier environnemental de la responsabilité sociétale des entreprises. Ainsi, il peut être utile de rappeler notamment:

- Les exigences faites aux entreprises cotées en Bourse d'indiquer, dans leur rapport annuel, certaines informations relatives aux conséquences sociales et environnementales de leurs activités (Art 116 de la loi du 15 mai 2001),
- Les obligations de transparence des entreprises en matière sociale et environnementale issues du décret 2012-557 du 24 avril 2012,
- Les obligations de reporting en matière d'enjeux climato-énergétique, d'économie circulaire et de gaspillage alimentaire issue de la loi 2015-992 du 17 août 2015 relative à la transition énergétique pour la croissance verte. La liste de ces obligations est prévue à l'art. R 225-105 du code du commerce.

La Plateforme nationale d'actions globales pour la RSE.

En juillet 2012, seize organisations représentatives des employeurs, des salariés et de la société civile, se sont entendues pour demander au Premier ministre la création, auprès de lui, d'une ***plateforme nationale de dialogue et de concertation*** en matière de RSE.

Installée au sein de France Stratégie depuis juin 2013, son rôle est précisé par l'article 5 du décret 2013-333 du 22 avril 2013 modifié.

- France Stratégie vous présente la structure et met à disposition toute une documentation.
- Cette plateforme dispose d'un secrétariat permanent.

RÉAGIR FACE À UNE ATTEINTE À LA SÉCURITÉ ÉCONOMIQUE

Parce qu'elles ne sont pas nécessairement liées à l'existence d'une infraction à la loi pénale, les atteintes à la sécurité économique se révèlent parfois difficiles à comprendre ou à identifier pour le dirigeant d'une petite ou moyenne entreprise ou par des salariés.

Pour aller plus loin en matière de responsabilité sociétale des entreprises et comprendre le positionnement de la France:

- Découvrez et suivez les publications de France Diplomatie,
- Pour toute autre question, la brigade numérique de la gendarmerie se tient à votre disposition sur www.gendarmerie.interieur.gouv.fr

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.

Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT

Ce document a été réalisé par la DGGN et l'INHESJ à des fins pédagogiques.
Auteur: Lcl TORRISI Contributeurs: MORTIER-BANCON-CLEMENT-ARCHAMBAULT