

MOT DU RESPONSABLE DE LA COMMISSION

L'objectif de la conférence-débat du 26 septembre 2013 « Programmes de Compliance et droit social : principes de réflexion » est de dresser l'inventaire des réflexes à avoir pour se conformer aux règles imposées par le droit social, lors de la mise en œuvre des programmes de compliance :

- Comment assurer la licéité et l'opposabilité du programme de compliance ?
- Quelles sont les sanctions et incentives du programme de compliance ?
- Quelles sont les règles pratiques pour effectuer des enquêtes efficaces et licites ?
- Quelle est la place des valeurs morales dans la sphère professionnelle ?
- Faut-il définir l'usage des équipements personnels, des réseaux sociaux dans le programme de compliance ?...

Nous avons souhaité profiter de cet événement axé sur le droit social pour réunir dans le présent fascicule les documents de synthèse élaborés par la Commission Gouvernance et Ethique du Cercle Montesquieu :

- Programmes de Compliance : Principes de réflexion (I) ;
- Programmes de Compliance et droit social : Principes de réflexion (II) *;
- Le rôle du Directeur Juridique dans les rapports de l'entreprise avec les intermédiaires commerciaux et autres partenaires (III).

Je remercie vivement pour leur participation à la conférence-débat du 26 septembre 2013 :

- le Cabinet Jones Day, notre partenaire
- les intervenants :
Maître Eliane Chateauvieux, associée du Cabinet Actance
Maitre Emmanuelle Rivez-Domont, associée du Cabinet Jones Day
Madame Sophie Marlange- Employment and Ethics, Legal Director EMEA – DELL
- les membres de la Commission Gouvernance et Ethique du Cercle Montesquieu **

Claire Olive Lorthioir

Responsable de la Commission Gouvernance et Ethique
du Cercle Montesquieu
Administrateur du Cercle Montesquieu
Associate General Counsel France ORACLE

* Les réflexions menées par la Commission Gouvernance et Ethique du Cercle Montesquieu sur les aspects droit du travail, principes de réflexion (II) font suite au document concernant les programmes de compliance, principes de réflexion (I) élaboré sous la présidence de Dominique Laymand.

** *Membres actifs de la Commission Gouvernance et Ethique du Cercle Montesquieu*

Amrei Augustin, Olivier Bertram, Stephane Collinet, Corinne Coscas, Béatrice Davourie, Pascal Durand-Barthez, Catherine Fox, Pierre Giraud, Béatrix Laurent-Moulin, Dominique Laymand, Stephane Lefer, Sophie Loulergue, Claire Olive Lorthioir, Philippe Luttmann, Willy Mathot, Christiane Michel, Aline Montel, Nadine Mondet, Brigitte Piplard, Isabelle Ramus, Carol Xueref. En souvenir de Lydia de Verneix, membre de la commission, disparue en mai 2013.

SOMMAIRE

Mot du Responsable de la Commission	P. X
Programmes de Compliance : Principes de réflexion.....	P. X
Compliance Programmes : Introduction.....	P. X
Programmes de compliance et Droit social : Principes de réflexion .	P. X
Compliance Programmes and Labour Law : Principles of reflection .	P. X
Le rôle du Directeur Juridique dans les rapports de l’entreprise avec les intermédiaires commerciaux et autres partenaires....	P. X
Annexe : Recommandations publiées par les organisations internationales en matière de programmes de compliance.....	P. X

PROGRAMMES DE COMPLIANCE

Principes de réflexion

Le présent document vise à fournir les éléments de base auxquels se référer dans la mise en place et la mise en œuvre des programmes de « compliance » ou de « conformité » en entreprise (pour le reste du texte nous emploierons le terme compliance), dont les directeurs juridiques et, dans les entreprises qui en sont dotées, les directeurs compliance sont des acteurs primordiaux. Il s'agit des mécanismes mis en place par l'entreprise pour conforter le respect par ses salariés des lois et codes professionnels, des procédures internes et de l'éthique.

Ce document, par sa brièveté même, ne peut prétendre offrir ni une analyse didactique du sujet, ni un guide pratique décrivant les étapes de la mise en place des programmes. En effet, le premier impératif est de faire en sorte que le programme de compliance soit aussi adapté que possible aux réalités spécifiques de l'entreprise, aux caractéristiques du secteur dans lequel elle évolue, à sa culture propre, à son « business model », à son mode d'organisation, et donc, l'imposition artificielle de modèles généraux qui seraient plaqués sur ces réalités ne peut qu'être néfaste ou inutile (« one size does not fit all »).

Partie I - Pourquoi mettre en place un programme de compliance ?

Les programmes de compliance s'appliquent à de multiples domaines correspondant aux divers risques juridiques, éthiques ou de réputation auxquels est confrontée l'entreprise, et qui sont passés en revue, de manière d'ailleurs non exhaustive, dans la partie II de ce document.

Nous avons choisi ici d'illustrer notre propos à partir d'exemples tirés du domaine de la concurrence, mais les commentaires s'appliquent *mutatis mutandis* à toutes les matières de compliance concernées.

A) Les raisons de mise en place d'un programme de compliance

La première raison tient naturellement à la conception que l'on se fait du rôle sociétal de l'entreprise, qui ne peut se réduire à la recherche du profit à court terme : la « contribution à une pratique éthique des affaires » est une des missions de la fonction juridique affirmées par le Cercle Montesquieu, et une mission essentielle de la fonction compliance.

Les programmes de compliance apportent également à l'entreprise des avantages indiscutables en termes de protection juridique et en matière d'image, mais ces avantages ne sont ni absolus ni aisément mesurables.

Les programmes de compliance permettent à l'entreprise d'afficher les règles de conduite collective qu'elle entend suivre, ce dont elle ne peut plus s'affranchir aujourd'hui parce que ses obligations sont de plus en plus complexes dans un contexte d'inflation réglementaire permanente et dans celui de

la mondialisation ; on se heurte avant tout à un simple problème d'ignorance des normes. D'autre part, le pouvoir de décision ou d'action, surtout dans la grande entreprise, s'est largement décentralisé et ne revient plus à un groupe restreint d'individus supposés adhérer aux mêmes valeurs morales. L'incitation omniprésente à la performance à court terme, y compris la pression apportée par les nouveaux modes de rémunération variable qui n'affectent pas que les dirigeants, doit nécessairement s'accompagner de l'affirmation que tous les moyens ne sont pas permis pour atteindre cette performance.

Enfin, l'entreprise doit se donner les moyens d'appliquer les règles qu'elle affiche ainsi. Elle ne peut pas se reposer sur la seule autorité étatique pour veiller à leur application, même si ces règles ne diffèrent pas fondamentalement de la simple application de la loi. Et si une infraction est constatée, l'effet produit par la présence d'une charte éthique publiée mais qu'on ne s'est pas soucié d'appliquer est désastreux, tant vis-à-vis du juge, du régulateur ou du public (pour une société cotée) que pour l'image de l'entreprise.

Ces caractéristiques se retrouvent par exemple en matière de droit de la concurrence ; il s'agit de règles souvent complexes à appréhender, qui s'appliquent à toutes les entreprises et ont vocation à protéger le libre jeu de la concurrence et à assurer un fonctionnement efficace des marchés au bénéfice des consommateurs.

Les programmes de compliance en matière de droit de la concurrence ont donc pour premier objectif d'assurer que les principes applicables sont compris et respectés. Ils visent à prévenir et si possible à empêcher les comportements ou pratiques susceptibles de fausser ou restreindre la concurrence sur les marchés, qu'ils prennent la forme d'accords restrictifs de concurrence (ententes) ou de comportements abusifs en position dominante. De telles pratiques peuvent être à l'origine de lourdes sanctions financières (amendes), d'un préjudice pour l'entreprise et son secteur en matière d'image (risque de réputation) ainsi que de la nullité des accords ou décisions anticoncurrentiels, du paiement de dommages et intérêts aux victimes, et de sanctions pénales pour les personnes physiques, dirigeants ou « exécutants ».

Le droit de la concurrence n'est ici qu'un exemple et on pourrait décliner les commentaires ci-dessus en les adaptant à chacun des domaines évoqués dans la partie II du présent document.

L'entreprise qui choisit de mettre en place un programme de compliance visant à rendre plus visible sa politique interne et à disposer de procédures formelles ou informelles permettant de détecter rapidement les comportements illicites, et de les sanctionner de façon appropriée, peut le faire pour plusieurs raisons :

- éviter ou amoindrir les sanctions ;
- rendre plus lisibles par ses salariés des normes complexes et souvent mal connues ;
- le cas échéant, se conformer aux engagements contraignants pris après avoir fait l'objet de procédures ou sanctions par

une autorité de la concurrence, administrative ou judiciaire ;

- faire suite à l'adoption par d'autres sociétés de son secteur de programmes ou à un cas de non conformité médiatisé ;
- valoriser l'image de l'entreprise ;
- obtenir des gains économiques découlant d'un meilleur fonctionnement du marché dans lequel elle opère et faire jouer pleinement les avantages concurrentiels dont elle pense disposer.

B) Les obstacles et les difficultés

La mise en place et l'exécution d'un programme de compliance rencontre des obstacles, dont certains sont spécifiques au contexte français, et que les directeurs juridique et compliance contribuent à aplanir. Ces difficultés sont de trois ordres : culturel, juridique et économique.

Le contexte culturel, qui peut sembler peu accueillant à la compliance (méfiance à l'égard des « donneurs de leçons », répugnance pour des raisons historiques à l'égard des pratiques de dénonciation) évolue grâce à une plus grande sensibilisation de tous à la responsabilité sociétale de l'entreprise dans un contexte concurrentiel et à la pratique internationale.

De même, le droit français génère des difficultés, mais celles-ci sont surmontables, et il évolue. Ainsi, le droit du travail rend difficile d'appliquer une sanction à ce qui n'est pas strictement une infraction à la loi, au règlement intérieur ou au contrat de travail (protection lors de procédures disciplinaires, interdiction de sanctions pécuniaires, liberté d'expression, etc.). Si l'incorporation d'une charte éthique au contrat de travail est mal-

aisée hors le cas d'une entreprise en création, l'adaptation du règlement intérieur n'est pas nécessairement hors de portée, et le pouvoir de direction de l'employeur est généralement un fondement suffisant pour justifier la sanction disciplinaire d'un manquement caractérisé à l'éthique des affaires. On peut rappeler, à titre d'exemple, que le Code du travail interdit désormais de faire subir des « représailles » aux salariés qui auraient dénoncé de bonne foi des faits de corruption ou de harcèlement auprès de la direction de l'entreprise ou des autorités compétentes.

Le droit applicable à la protection des données personnelles peut aussi être source de difficultés, notamment en ce qui concerne les procédures d'alerte interne (« *whistle-blowing* ») et la transmission de données à l'étranger éventuellement requise pour la mise en œuvre d'un programme de compliance dans un groupe international. Cependant, les procédures autorisées par la CNIL permettent de surmonter ces difficultés, et

c'est là aussi un champ d'intervention nécessaire de la direction juridique de l'entreprise.

Sur le plan économique, le coût même des programmes de compliance, qu'il soit direct ou indirect (temps passé par les salariés à dispenser et recevoir la formation, etc.) est souvent vécu comme un obstacle, spécialement en période de crise. Ce coût devient prohibitif si le programme, mal maîtrisé, est dominé par les aspects formalistes et se transforme en exercice bureaucratique. Or, la valeur ajoutée du programme et son efficacité sont difficiles à mesurer. Au-delà de l'information visant à éclairer les salariés de bonne foi désorientés par la complexité des règles et à créer des réflexes, les acteurs de la compliance dans l'entreprise, au premier rang desquels les fonctions juridique et compliance, doivent donc souvent faire œuvre de conviction et de pédagogie, si la compliance est étrangère à la culture de l'entreprise, voire si la tolérance à l'infraction est délibérée.

Partie II - Contenu d'un programme de compliance

Les domaines couverts par les programmes de compliance doivent être adaptés aux risques inhérents à chaque entreprise et à l'activité qu'elle exerce.

Le programme de compliance doit constituer un ensemble efficace et cohérent qui doit pouvoir évoluer dans le temps.

Sans prétendre à l'exhaustivité, les domaines suivants trouvent naturellement leur place dans un programme de compliance :

1. Respect des lois, codes professionnels, règles spécifiques applicables à la branche (par

exemple, contrôle des exportations et importations de produits sensibles, santé, etc.)

2. Obligations financières et boursières - probité de l'information financière, sincérité de la comptabilité, lutte contre le blanchiment et les délits d'initiés

3. Conflits d'intérêts concernant l'activité de l'entreprise ainsi que les salariés eux-mêmes

4. Respect des règles de concurrence

5. Anti-Corruption - respect des législations nationales et internationales applicables

6. Confidentialité – Protection de la propriété intellectuelle et protection de la propriété des tiers

7. Responsabilité sociale interne : lutte contre la discrimination et le harcèlement, diversité, protection de la vie privée et des données personnelles, sécurité et santé du personnel

8. Développement durable et responsabilité sociétale de l'entreprise dans sa sphère

d'influence – protection de l'environnement, droits de l'homme.

Il peut être utile de renforcer certains de ces points en ce qui concerne certaines fonctions particulièrement exposées de l'entreprise, par exemple les fonctions achats, finances ou commerciales.

Partie III - Les moyens affectés à la mise en œuvre d'un programme de compliance

Les moyens nécessaires à la mise en place et à la maintenance d'un programme de compliance efficace présupposent une organisation interne adaptée.

A) L'organisation interne doit être solide, indépendante, efficace et compétente

1. Solide : c'est à dire formée à cette expertise.

2. Indépendante : cette indépendance sera d'autant plus garantie que le rattachement hiérarchique sera plus élevé.

La fonction compliance peut être rattachée au directeur juridique, les deux fonctions étant complémentaires, mais la séparation peut se concevoir : la compliance touche un domaine plus large que celui du droit, et il peut être envisagé de séparer le rôle de « régulateur interne » de la fonction compliance et celui de « défenseur » de la direction juridique.

S'il s'agit d'activités réglementées telles que la profession bancaire, le rattachement est prévu par la réglementation elle-même.

En tout état de cause, le positionnement est fondamental comme garant de l'indépendance et par là même des moyens affectés à la fonction compliance.

La préoccupation d'indépendance ne contredit pas la nécessité d'un reporting régulier à la direction générale, qui permet l'implication de celle-ci, condition fondamentale du succès des programmes de compliance (« *tone at the top* »)

3. Efficace : pour cela l'organisation doit être adaptée pour tenir compte des besoins opérationnels de l'entreprise.

La règle doit être vulgarisée de façon compréhensible et précise : elle doit être facile d'accès et utilisable telle une boîte à outils.

4. Compétente : tout ce qui précède dépend de la qualité et de la compétence des personnes en charge de la mise en place.

Pour attirer les personnes qualifiées, la fonction doit donc être bien rémunérée avec une possibilité d'évolution de carrière.

La durée dans la fonction ne doit pas être laissée au hasard : ni trop courte, ni trop longue, pour éviter les écueils dans les deux sens.

B) La fonction compliance doit disposer de moyens adéquats

Ceux-ci peuvent être internes ou externes et sont à déterminer en fonction des besoins particuliers et des spécificités du programme de compliance, ainsi que de l'évaluation des risques lors de la création du programme ou de son évolution.

1. La formation :

- dans un premier temps par une sensibilisation en vue de la création de réflexes et d'une amélioration des connaissances ;
- par l'envoi de notes avec un processus d'acceptation (signature) afin de les rendre opposables aux destinataires ;
- par des actions telles que réunions avec intervention de spécialistes des sujets abordés (par exemple, cellule Tracfin

pour le blanchiment, experts-comptables, spécialistes du droit de la concurrence, etc.) ;

- par e-learning.

Cette formation doit faire l'objet d'une mise à jour périodique d'où l'intérêt d'un registre des signatures.

2. Les moyens de contrôle :

- par l'accès aux courriels, aux contrats, par des pouvoirs d'investigations comme ceux de l'audit...
- par des outils efficaces de monitoring et de contrôle permettant une continuité de contrôle ;
- par un appui sur le règlement intérieur, le cas échéant ;
- par l'accès aux dispositifs d'alerte (*whistle-blowing*) ou de dénonciation (anonyme ou non), mis en place dans l'entreprise.

Partie IV - Monitoring et Reporting

Une fois mis en place, le programme de compliance doit faire l'objet d'une veille permanente visant à contrôler son efficacité et son adéquation à l'évolution de l'activité de l'entreprise, du secteur, ainsi qu'à celle du cadre réglementaire et des bonnes pratiques en vigueur (voir par exemple le guide OCDE¹ dans le domaine de la lutte anti-corruption). Son exécution fait aussi l'objet d'un reporting et d'une communication périodiques, tant internes qu'externes.

On ne peut en effet se contenter d'attendre que surviennent des incidents mettant en lu-

mière des dysfonctionnements éventuels et d'en tirer les conséquences en faisant alors des investigations supplémentaires et en révisant éventuellement le programme.

A) Les plans de monitoring spécifiques à la compliance

Ces plans de monitoring constituent un élément essentiel de qualité et d'efficacité pour un programme de compliance solide.

Le suivi régulier peut s'inscrire dans un calendrier qui lui est propre, avec des plans de monitoring basés sur l'analyse des risques, définissant des actions précises comportant par exemple des vérifications documentaires et

1. <http://www.oecd.org/dataoecd/5/51/44884389.pdf>

des visites sur site, et assurant le suivi des actions d'amélioration qui en résultent. Il peut également s'inscrire dans un calendrier coordonné avec les plans de l'audit interne ou la préparation des rapports annuels.

Ces plans de monitoring sont spécifiques à chaque entreprise et au secteur dans lequel elle opère.

B) Les plans d'audit interne

Les services d'audit interne des entreprises qui en sont dotées établissent généralement des plans de campagne annuels. Ces plans d'audit doivent comporter des éléments relatifs au programme de compliance. A titre d'exemples : évaluation du degré de connaissance de sujet même de la compliance, de la charte d'éthique et du contenu du programme de compliance, contrôle des relations avec les partenaires tels que fournisseurs, sous-traitants, distributeurs ou agents commerciaux.

Les directions juridique et/ou compliance :

- interviennent dans l'élaboration des plans d'audit ;
- veillent à ce que les thèmes de compliance soient abordés en sus des sujets proprement juridiques (tels que délégations de pouvoirs, cartographie des risques sur contrats, etc.) ou financiers ;
- apportent leur soutien à leur exécution, en respectant toutefois la séparation des fonctions et l'indépendance de l'audit ;

S'il existe un système d'alerte professionnelle (*whistleblowing*), l'analyse des informations collectées par celui-ci peut fournir des orientations dans le choix des contrôles à effectuer.

Bien entendu, on ne saurait se reposer totalement sur la fonction d'audit interne pour

assurer le suivi de la mise en œuvre d'un programme de compliance : ni sa finalité ni ses méthodes d'investigation, essentiellement financières, ne permettent de couvrir tous les aspects de la compliance.

Néanmoins, les contrôles prévus tant dans les plans de monitoring que dans ceux d'audit, ne peuvent être efficaces que s'ils comportent la définition d'outils de détection et de vérification adaptés, notamment comptables (versement de montants inhabituels dans une catégorie de paiements, récurrence injustifiée des relations avec un fournisseur, etc.). Ces indicateurs, et éventuellement les outils informatiques permettant de les mettre en œuvre, peuvent être sélectionnés avec l'aide d'intervenants spécialisés externes.

C) La collaboration avec la fonction Ressources Humaines

Cette collaboration doit être étroite et devrait couvrir notamment les domaines suivants :

- introduction de critères de compliance lors des recrutements ou des promotions pour certains postes clés (directeur général, directeur d'unités opérationnelles, directeur de filiales, etc.) ;
- évaluation des salariés de l'entreprise permettant d'estimer leur performance d'un point de vue éthique et compliance ;
- échelle à définir et mise en œuvre des sanctions en cas de manquements des salariés, en respectant la réglementation nationale ;
- organisation et mise en œuvre des formations et de la délégation des pouvoirs de contrôle.

D) Le reporting au conseil d'administration

Outre le reporting à la Direction générale (voir ci-dessus), le conseil d'administration (ou de surveillance) de l'entreprise doit normalement être tenu informé du bon fonctionnement et du suivi des programmes de compliance. A minima pour les sociétés françaises cette implication est nécessaire pour lui permettre de se prononcer valablement sur les éléments « de nature extra-financière » (notamment relatives aux questions d'environnement et de personnel) devant figurer dans son rapport annuel à l'assemblée générale.

Les directeurs juridiques et compliance veillent donc à ce qu'un rapport de situation soit présenté au minimum annuellement soit au conseil, soit au comité compétent de celui-ci (comité d'audit, autre comité chargé des questions de responsabilité sociale). S'il ne leur revient pas de le présenter, ils participent à son élaboration.

En outre, la responsabilité sociétale est maintenant un véritable sujet de communication interne et externe pour les sociétés.

Cela implique une présentation des instruments permettant la mise en œuvre des valeurs affichées par la société, au premier rang desquels se trouve le programme de compliance. Les sociétés les plus engagées s'efforcent en outre de figurer dans les indices internationaux de responsabilité sociétale (tels que « FTSE4Good » ou « Dow Jones Sustainability Index »), ou de répondre de manière favorable aux enquêtes des agences de notation spécialisées dans ce domaine (telles que Vigeo ou BMJ Ratings).

En conclusion, les directions juridique et/ou compliance participent, aux côtés des autres parties prenantes (direction de la communication, direction des ressources humaines, développement durable, direction financière, etc.) à la mise en œuvre efficace des programmes de compliance. S'établit ainsi une dynamique complète et continue entre prévention, détection des risques et amélioration du programme de compliance, qui devient ainsi un élément majeur dans la transmission de la culture éthique de l'entreprise lui permettant d'agir avec efficacité dans un environnement compétitif, sûr et positif.

COMPLIANCE PROGRAMMES

Introduction

The purpose of this document is to provide the basic building blocks for implementing and launching corporate “compliance” or “conformity” programmes (for the remainder of this document, we will employ “compliance”), in which legal managers and, for companies who have them, compliance managers, are the key players. These building blocks are mechanisms that a company puts in place to reinforce its employees’ observance of laws and professional codes, internal procedures and ethics.

By virtue of its brevity, this document cannot claim to provide an informative analysis of the subject or to serve as a practical guide with step-by-step instructions on how to implement programmes. Rather, the main goal is to ensure that compliance programmes adapt as much as possible to the specificities of the company and its sector, to the company’s own culture, to its business model, and to its organisational system. Consequently, artificially imposing general models onto these realities could only be harmful or useless (“one size does not fit all”).

Part I - Why implement a compliance programme?

Compliance programmes apply to several domains, which correspond to the diverse legal, ethical or reputation risks encountered by companies. These risks are briefly reviewed, in a rather non exhaustive way, in part II of this document.

We will explain our ideas here using examples from the domain of competition, but the comments apply *mutatis mutandis* to all relevant spheres of compliance.

A) Reasons for implementing a compliance programme

The first reason is naturally related to the notion that people have of the societal role of companies, which cannot be limited to seeking short-term profits: the “contribution to ethical business practices” is proclaimed by the Cercle Montesquieu as being one of the missions of the legal function, and it is also an essential purpose of the compliance function.

Compliance programmes also provide companies with undeniable advantages in terms of legal protection and image, but these advantages are neither absolute nor easy to measure.

Compliance programmes enable companies to display the rules of group conduct that they intend to follow. Companies can no longer live without such rules because their obligations are increasingly complex against a background of ever-expanding regulatory reach and globalisation; more importantly, companies are confronted with the simple problem of ignorance of the rules. Furthermore, the power to decide or act, especially in a large company, is largely

decentralised and therefore no longer resides within a small group of individuals assumed to have the same moral values. With respect to the ubiquitous incentive to produce short-term results, including the pressures resulting from new methods of variable remuneration, which do not only apply to managers, it must be understood that results cannot be allowed to be achieved in any way imaginable.

Finally, companies must equip themselves with the tools they need to apply the rules they display. They cannot solely rely on the government to ensure that such rules are being applied, even if these rules do not inherently differ from applicable law. If an offence is observed, the effects of having a published ethical charter that no one bothers to enforce are disastrous in the eyes of judges, regulatory bodies and the public (for a listed company) and hence, for a company’s image.

These characteristics are found, for example, in antitrust law; they are rules, often difficult to understand, that apply to all companies and serve to protect the free play of competition as well as ensure that markets work efficiently for the consumers.

Therefore, the primary objective of programmes for complying with antitrust law is to ensure that the applicable principles are understood and respected. They aim at identifying and, if possible, preventing behaviour or practices that are likely to distort or restrain competition on markets, whether such behaviour take the form of competition restricting agreements (ententes) or abusive behaviour by those in a dominant position. Such practices can lead to heavy financial sanctions

(fines), damage the reputation of a company and its sector (reputation risk) and overturn anti-competition agreements or decisions, as well as lead to paying damages to victims and to criminal sanctions for individuals, directors or those who carry out the practices.

Antitrust law only serves as an example here and the comments above could be applied to each area mentioned in part II of this document.

Companies deciding to establish a compliance programme to make their internal policies more visible and to implement formal or informal procedures for detecting illegal behaviour early and punishing them accordingly may do so for several reasons:

- to avoid or diminish sanctions,
- to make complex and often poorly understood rules easier to comprehend,
- if applicable, to comply with restrictive commitments undertaken after being subject to procedures or sanctions enacted by an antitrust, administrative or legal authority,
- to follow other companies of the sector that adopted programmes or to follow-up on a case of non-compliance receiving media coverage,
- to enhance the company's image,
- to obtain economic gains from a better-functioning market and to take full advantage of the competitive benefits the companies think they have.

B) Obstacles and difficulties in implementing a compliance programme

There are obstacles to implementing and carrying out a compliance programme,

and certain of these obstacles are specific to the French context. Legal and compliance directors can help smooth over these barriers. There are three types of difficulties encountered: cultural, legal and economic.

The cultural context, which can seem rather hostile to compliance (distrust of “lesson givers”, historical French loathing of denouncing), is evolving due to a general increased awareness of the corporate responsibility of companies in a competitive frame of reference and as a result of international practices.

Likewise, French law creates difficulties, but French law is evolving and the difficulties can be overcome. Consequently, labour law makes it difficult to apply a sanction to what is not strictly considered to be a breach of law, of policies and procedures, or of an employment contract (protection during disciplinary procedures, prohibition of pecuniary sanctions, freedom of expression, and so on). Even though incorporating an ethical charter into employment contracts is difficult, except when a company is being launched, policies and procedures could be adapted, and an employer's management power generally has a sound enough basis to justify disciplinary sanctions against a breach of business ethics. Further, the French Labour Code henceforth prohibits “retaliation” against employees who, in good faith, go to company management or the appropriate authorities to expose corruption or harassment.

The legislation that applies to personal data protection can also be troublesome, especially regarding internal whistle-blowing procedures and dispatching any data internationally that may be required when implementing a compliance programme

within an international group. However, the procedures authorised by the CNIL (the independent French administrative authority for privacy and personal data protection) help overcome these difficulties, and once again, company legal managers can prove to be useful in this area.

Economically-speaking, the very costs related to compliance programmes, whether direct or indirect costs (such as employee time spent providing and receiving training) are often viewed as an obstacle, especially in a period of crisis. These costs become prohibitive if a poorly-supervised

programme is dominated by formalistic actions and becomes a bureaucratic exercise while the added value of the programme and its effectiveness are difficult to measure. In addition to the information that aims both at enlightening well-intentioned employees who are misguided by complex rules and creating reflexive actions, those involved in company compliance, with the legal and compliance functions front and centre, must therefore often demonstrate conviction and act as teachers if compliance is foreign to company culture or if tolerance for offences is deliberate.

Part II - Content of a compliance programme

The areas covered by a compliance programme must be adapted to the risks inherent to each company and each company's activity.

A compliance programme must constitute an efficient, coherent whole that can evolve over time.

Although not exhaustive, the following areas are a natural part of a compliance programme:

1. Respect for laws, professional codes, and specific rules that are applicable to the branch of activity (for example, control for exports and imports of controversial or healthcare products)

2. Financial and stock market responsibilities - integrity of financial information, reliability of accounting, anti-money laundering measures and insider trading prevention

3. Conflicts of interest regarding the company activity or the employees themselves

4. Respect for competition laws

5. Fighting against corruption - compliance with applicable national and international law

6. Confidentiality - intellectual property protection and third-party property protection

7. Internal corporate responsibility: discrimination and harassment prevention, diversity, personal data and privacy protection, personnel health and safety

8. Sustainable development and corporate responsibility within a company's sphere of influence - protection of the environment and of human rights.

It can be useful to reinforce some of these points for certain particularly visible company functions, such as purchasing, finance or marketing and sales.

Part III - Resources allocated for implementing a compliance programme

The resources needed to implement and maintain an effective compliance programme assume that an appropriate internal organisation exists.

A) The internal organisation must be solid, independent, efficient and competent

1. Solid: in other words, trained to have this expertise.

2. Independent: the higher the reporting line, the stronger the guarantee of independence.

The compliance function can report to the legal director, since the two functions are complementary, although a functional separation can be envisaged: compliance applies to a larger domain than law, and a separation of the “internal regulator” role into a compliance function and a “defence” function in the legal department can be foreseen.

If these are regulated activities, such as in the banking profession, the reporting line is provided by the regulations themselves.

In any event, the positioning is crucial for ensuring independence and, at the same time, the resources allocated to the compliance function.

The concerns for independence do not contradict the need to regularly report to general management, thereby keeping management involved - a basic condition for compliance programmes to succeed (“*tone at the top*”).

3. Efficient: to be efficient, the organisation must be able to take the company’s operational needs into consideration.

The rules must be popularised in an understandable, precise way: they must be easy to access and use, like a toolbox.

4. Competent: all the preceding depends on the quality and competence of the people responsible for the implementation.

To attract qualified people, the function must be well-paid and offer the possibility of career development.

The term of the function must not be randomly determined: it should neither be too short nor too long, in order to avoid the pitfalls of both extremes.

B) The compliance function must have adequate resources

These can be internal or external and should be determined according to the particular needs and individual characteristics of the compliance programme, as well as according to the risk assessments performed when creating or modifying the programme.

1. Training:

- In a first phase, train by increasing awareness with a view to creating automatic responses and improving knowledge.

- Train by sending memos that require a signature so that the recipients must acknowledge them.

- Train through actions, such as holding meetings to which specialists in the area under discussion are invited (for

example, invite someone from the Tracfin service of the French Ministry of Finance for discussions on money laundering, chartered accountants, antitrust law specialists, and so on).

- Train through e-learning.

This training must be periodically updated, which is why a list of signatures is useful.

2. Resources for controls:

- obtained by granting investigatory powers (such as to internal auditors), access to e-mails and contracts,

- obtained by using effective monitoring tools for continuous control,
- obtained by referring to policies and procedures, if necessary,
- obtained by having access to alert (whistle-blowing) or exposure (anonymous or otherwise) measures implemented by the company.

Part IV - Monitoring and Reporting

Once in place, the compliance programme must be constantly monitored in order to verify its effectiveness and its appropriateness to the company's activity and sector, as well as its adherence to the regulatory framework and current good practices (for example, refer to the OECD guide¹ regarding bribery). There must also be reporting and periodic communication (both internal and external) on its execution.

It is not enough to just wait for incidents to occur to reveal shortcomings and then draw conclusions by performing additional investigations and eventually revising the programme.

A) Implementing specific compliance monitoring plans

These monitoring plans are essential to ensuring the quality and efficiency of a solid compliance programme.

Regular monitoring can have its own schedule based on risk analyses and set forth specific actions, such as verifying documents and performing site visits, as well as ensure follow-up on the resultant improvement actions. Regular monitoring can also be part of a calendar coordinated with the internal audit plans or the schedule for preparing annual reports.

These monitoring plans are specific to each company and to each company's sector.

B) Becoming a part of internal audit plans

For companies that have them, internal audit departments generally establish annual campaigns. These audit plans should

1. <http://www.oecd.org/dataoecd/5/51/44884389.pdf>

comprise compliance programme items, such as assessing the level of understanding of the subject of compliance itself, of the ethics charter and of the content of the compliance programme, and auditing relationships with partners, such as suppliers, subcontractors, distributors and sales agents.

Legal and/or compliance managers:

- participate in drafting audit plans
- ensure that compliance themes are discussed in addition to purely legal (for example, delegation of authority, risk mapping for contracts) or financial subjects
- provide support for carrying out the compliance programme while respecting the separation of duties and the independence of the audit.

If there is a whistle-blowing system, the analysis of the information collected through this system can provide direction in deciding which controls to perform.

Of course, the internal audit function cannot be totally relied on to monitor the execution of a compliance programme: neither the purpose of this function nor its investigatory methods, which are primarily financial, can cover all aspects of compliance.

However, the controls mentioned in both the monitoring plans and the audit plans can only be effective if they define appropriate detection and verification tools, and in particular, accounting tools (for example, the transfer of unusual amounts in a particular payment category, unjustified continuation of relations with a supplier). These indicators, and any IT tools that enable them to be implemented, can be selected using specialised external teams.

C) Collaborating with Human Resources

This cooperation should be close and should cover the following areas:

- introducing compliance criteria into recruitment or promotions for certain key positions (for example, managing director, operational unit director, subsidiary director),
- assessing company employees to determine their performance from an ethical and compliance point of view,
- defining and implementing a scale of sanctions against employee breaches that complies with national regulations,
- organising and implementing training and delegating controlling authority.

D) Reporting to the Board of Directors

In addition to reporting to the general management (see aforementioned), generally the board of directors (or the supervisory board) of a company is also informed of the proper functioning and monitoring of compliance programmes. At the very least, for French companies, this involvement is necessary to allow the board to make valid comments on “non-financial” items (especially those related to the environment and personnel) that need to be mentioned in the annual shareholder’s report.

The legal and compliance managers therefore ensure that a status report is presented at least once a year either to the board or to the appropriate board committee (audit committee or other committee in charge of corporate responsibility issues). If it is not the responsibility of the legal or

compliance managers to present the status report, then they take part in drafting it.

Furthermore, corporate responsibility is now a real subject of internal and external communication for companies. This implies a presentation of the instruments that allow the values displayed by the company to be implemented, with the compliance programme foremost. The most committed companies furthermore attempt to get listed in international corporate responsibility indices (such as the “FTSE4Good” or the “Dow Jones Sustainability Index”) or to respond favourably to surveys conducted by rating agencies that specialise in this area (such as Vigeo or BMJ Ratings).

In conclusion, legal and/or compliance teams participate, side-by-side with other stakeholders (communication teams, human resources teams, sustainable development teams, and financial teams, for example), in effectively implementing compliance programmes. Hence, a complete and continuous dynamic of prevention, risk detection and improvement for the compliance programme, which subsequently becomes a major vehicle for conveying the ethical culture of companies, allows companies to act efficiently in a stable and positive competitive environment.

PROGRAMMES DE COMPLIANCE ET DROIT SOCIAL

Principes de réflexion

Le présent document de synthèse vise à identifier les réflexes qu'il convient d'adopter lorsque l'Entreprise souhaite s'assurer du respect par ses salariés des Programmes de Compliance, lois et codes professionnels, procédures internes et Code d'éthique.

Les contraintes du droit social français auxquelles il convient de se conformer pour assurer l'efficacité du programme de Compliance sont identifiées ci-après.

Par sa brièveté même, le présent document ne prétend pas être exhaustif ni offrir une analyse didactique du sujet, ou un guide pratique.

Ce document s'inscrit dans la continuité des travaux de la Commission Gouvernance et Ethique du Cercle Montesquieu, identifiant les principes à adopter lors de la mise en place d'un programme de Compliance (document de synthèse : programmes de Compliance « Principes de réflexion » - première édition janvier 2011).

I. Codes d’Ethique : quelle efficacité juridique ?

Les Codes d’Ethique témoignent d’une volonté de transparence, d’amélioration de leur image et de prise en compte de leur responsabilité sociale par les entreprises, même si cette pratique s’est développée à la suite d’affaires médiatisées de fraude, de corruption ou de délits d’initiés au sein de grandes sociétés. C’est généralement le premier élément d’un Programme de Compliance, instrument de gestion de l’entreprise désormais incontournable (voir le document de la Commission Ethique et Gouvernance « *Programmes de Compliance : principes de réflexion* » 2011).

Les Codes d’Ethique formalisent un ensemble de normes qui doivent être connues et appliquées par tous les salariés dans l’ensemble des pays où la société est implantée. Il s’agit de règles légales et de déontologie, de « valeurs » et directives internes (*politiques*) de l’entreprise: respect des lois et règlements, conflits d’intérêts, délits d’initiés, protection des actifs de l’entreprise, droit de la concurrence, lutte contre la corruption, etc.

Malgré la légitimité indiscutable de la démarche, se pose la question de leur opposabilité à l’égard des salariés sur le plan du droit du travail.

Les Codes d’Ethique ne font pas l’objet d’une réglementation spécifique. Il n’en est pas fait mention dans le Code du travail. Le régime de ce document purement facultatif dépend de la nature et de la force contraignante des règles qu’il prévoit (circulaire DGT n° 22 du 19 novembre 2008).

Les Codes d’Ethique qui se bornent à énoncer, en termes généraux, des engagements moraux et des valeurs éthiques auxquels

l’entreprise adhère, n’ont pas de réelle portée juridique (comme par exemple un document dans lequel l’entreprise « souhaite proposer des conditions d’emploi durable »...). Ils sont essentiellement conçus comme un outil stratégique de communication avec les salariés et les partenaires commerciaux de l’entreprise (clients, fournisseurs...). Leur élaboration est assez libre, sous réserve de ne pas porter atteinte :

- au principe de non discrimination (art. L.1132-1 du Code du Travail),
- aux droits et libertés individuelles des salariés (L.1121-1 et L.1321-3, 2°), en particulier à la liberté d’expression,
- au droit d’expression directe et collective des salariés (L.2281-1, etc.).

En revanche, certains Codes d’Ethique fixent des règles (normes comportementales) dont les manquements sont assortis de sanctions, ou dont l’application peut entrer en ligne de compte pour le calcul de la rémunération. En outre, certains codes d’éthiques sont assortis de moyens (dispositifs d’alerte) mis à la disposition des salariés pour dénoncer les agissements illégaux sans avoir recours aux voies hiérarchiques traditionnelles. Qu’ils résultent ou non de dénonciation, les manquements décelés peuvent faire l’objet d’enquêtes internes pour déterminer la suite à donner.

Toutes ces pratiques posent des questions au regard du droit du travail et de la protection de la vie privée.

II. Licéité et opposabilité des Codes d’Ethique et dispositifs d’alerte professionnelle

A. Les Codes d’Ethique et droit du travail

- Licéité des Codes d’Ethique

Les programmes de *Compliance*, dont les Codes d’éthique sont des éléments, doivent être considérés comme des « adjonctions au règlement intérieur » pour les parties concernant la discipline (art. L.1321-5 C. trav.). Ils nécessitent de ce fait l’information et la consultation du comité d’entreprise (art. L.432-1 C. trav.). La procédure comporte, dans l’ordre, les étapes suivantes :

- 1) Avis du CHSCT dans les matières relevant de sa compétence
- 2) Avis du comité d’entreprise ou à défaut des délégués du personnel
- 3) Contrôle de l’administration du travail (inspecteur du travail)

En outre, au même titre que le règlement intérieur, le Code d’éthique devra être affiché « à une place convenable et aisément accessible dans les lieux de travail ainsi que dans les locaux et à la porte des locaux où se fait l’embauche » (article R.1321-1 C. trav.).

- Modalités d’intégration des programmes de *Compliance* dans le contrat de travail des employés

Il n’existe pas de règles spécifiques dans le Code du travail quant à la remise du document. Néanmoins, dès lors que le document comporte des obligations pour le salarié, il doit être rédigé en français (art. L.1321-6 C. trav.). La jurisprudence fait de cette règle une application stricte s’agissant de « tout document dont la connaissance est nécessaire au salarié pour la bonne exécution de son travail »¹.

Il est indispensable pour les entreprises de s’assurer de l’opposabilité de ce document aux salariés. A cet effet, il est recommandé de remettre le document lors de l’embauche, par exemple par la signature d’une lettre contre décharge.

Enfin, la compréhension des règles et la prise de connaissance des mises à jour doivent être assurées par des actions de sensibilisation et de formation, et des rappels fréquents.

- Illicéité s’ils réduisent les droits des salariés

Les Codes d’Ethique ne peuvent constituer un moyen de réduire les droits fondamentaux des salariés conformément au principe de l’article L.1121-1 C. Trav. En revanche « *les salariés jouissent dans l’entreprise et en dehors de celle-ci de leur liberté d’expression à laquelle seules les restrictions justifiées par la nature de la tâche à accomplir et proportionnées au but recherché peuvent être apportées* »².

Dans ce cas, ils doivent être mis en place comme des adjonctions au règlement intérieur³.

B. Dispositifs d’alerte professionnelle, droit du travail et protection de la vie privée.

- Procédure d’adoption et de mise en œuvre des dispositifs

oct. 2010 (n°08/23998)

2. Cass. Soc. 8 déc. 2009 (n°08-17.191).

3. Cass. Soc., 28 mai 2008.

1. C.A. Versailles, 2 mars 2006 (n°05-1344) ; C.A. Paris, 1^{er}

Si le Code d'Ethique comporte un dispositif d'alerte professionnelle (selon la circulaire DGT n° 22 du 19 novembre 2008, il s'agit d'un système mis en place par un organisme public ou privé pour inciter les salariés ou tout autre personne exerçant une activité dans l'entreprise à signaler au chef d'entreprise ou, éventuellement, à d'autres personnes désignées à cet effet « des problèmes pouvant sérieusement affecter son activité ou engager gravement sa responsabilité »), la procédure d'adoption doit être la suivante :

- autorisation préalable de la CNIL (selon la délibération de la CNIL n°2005-305)
- information consultation du CHSCT (article L.4612-8 du Code du travail),
- information consultation du CE (article L.2323-32 du Code du travail).

La mise en œuvre du dispositif nécessite l'information individuelle des salariés, en application de la Loi informatique et libertés et de l'article L.1222-4 du Code du travail qui dispose qu'« aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance ».

• Rappel des règles édictées par la CNIL

La CNIL a adopté le 8 décembre 2005 une délibération n° 2005-305 autorisant les dispositifs d'alerte professionnelle s'ils sont conformes aux conditions de l'Autorisation Unique AU-004 annexée à la délibération. Si le dispositif envisagé n'est pas conforme à l'Autorisation Unique, l'entreprise doit déposer auprès de la CNIL une demande d'autorisation; à défaut le dispositif est à tout

le moins inopposable aux salariés, voire illicite s'il repose sur la collecte de données personnelles.

Le champ d'application des dispositifs autorisés était initialement restreint aux « domaines financier, comptable, bancaire et de la lutte contre la corruption » (y compris les domaines couverts par la loi américaine Sarbanes-Oxley), sauf mise en jeu de « l'intérêt vital » de l'entreprise ou de « l'intégrité physique ou morale de ses employés ». La jurisprudence en a fait une application stricte (arrêt Dassault Systèmes⁴).

La CNIL a ultérieurement modifié l'autorisation AU004, par délibération du 14 octobre 2010, essentiellement en étendant le champ au domaine de la concurrence.

Si l'entreprise souhaite mettre en place un dispositif s'étendant hors du champ d'application, par exemple pour y inclure les pratiques de discrimination, elle doit déposer une demande d'autorisation individuelle qui fera l'objet d'un examen par la CNIL au cas par cas. Après l'autorisation de la CNIL, les étapes de procédure décrites ci-dessus doivent être suivies.

Les salariés qui veulent signaler un fait non couvert par l'autorisation (unique ou individuelle) de la CNIL devront utiliser les voies classiques (voie hiérarchique, information des représentants syndicaux ou des services de ressources humaines) et non le dispositif d'alerte.

4. Cass. Soc., 8 déc. 2009 (n° 08-17.191).

III. Les enquêtes internes

A. Pour quelles raisons l'entreprise peut-elle avoir à conduire une enquête interne ?

Les objectifs d'une enquête interne peuvent être la qualification d'infractions aux législations applicables (locales ou ayant une portée extraterritoriale) ou à son Code d'Éthique afin d'impliquer les différents départements de l'entreprise et les conseils extérieurs appropriés (juridiques et autres) et d'identifier les juridictions compétentes, et/ou la recherche de preuves dans la perspective d'une procédure interne ou externe (la charge de la preuve incombe à l'employeur !)

L'entreprise peut y être conduite dans différentes circonstances :

- L'entreprise est alertée d'une activité répréhensible dont elle serait victime : fraude, atteinte à sa propriété intellectuelle, délit ou manquement d'initié, violation du règlement intérieur, de son Code d'Éthique ou d'autres règles internes de fonctionnement (harcèlement, discrimination, rémunération, etc.).
- L'entreprise est alertée d'une activité répréhensible dans laquelle sa responsabilité serait impliquée (délit ou autre infraction réglementaire, infraction à la concurrence, autre manquement à son Code d'Éthique).
- *Discovery* dans le cadre d'une procédure civile ou pénale de *common law*, dans laquelle par obligation ou par choix l'entreprise doit fournir à l'autre partie tous les éléments se rattachant au dossier.

B. Quelles obligations doit-elle respecter en conduisant son enquête interne ?

Si l'enquête peut déboucher sur des sanctions disciplinaires, la procédure applicable doit être respectée.

- Droit du travail

La suspension du contrat de travail à titre conservatoire est possible pour une durée limitée (qui ne cadre pas forcément avec la longueur d'un processus d'enquête).

Le délai de prescription pour l'exercice par l'employeur de son pouvoir disciplinaire (pouvoir de sanction ou de licenciement - article L.1332-4 C. trav.) est de deux mois, ce qui implique l'identification précise de la date à laquelle l'employeur a eu connaissance du comportement fautif, la convocation rapide du salarié à un entretien préalable, l'exposé précis des griefs retenus lors de l'entretien et la notification rapide des sanctions (art. L.1332-2 C. trav.).

Le salarié a droit à une assistance lors de l'entretien.

A l'étranger, de nombreuses juridictions exigent une information claire et transparente des droits et obligations des salariés interrogés dans le cadre d'une enquête; par exemple, aux Etats-Unis, la lettre d'avertissement « Upjohn »⁵.

5. *Upjohn v. U.S.*, 449 U.S. 383 (1981). Cette lettre a pour but d'informer le salarié que l'avocat qui va l'interroger représente l'employeur et que les éléments pourront être confidentiels mais que l'entreprise conserve la possibilité de renoncer à cette confidentialité et transmettre les éléments découverts à l'administration. Elle n'a pas de valeur en dehors des Etats-Unis mais clarifie le contexte.

- Protection de la vie privée

Les principes de base du respect de la vie privée (art. 9 du C. Civ., art. 8 de la CEDH), la règle de la proportionnalité des restrictions à la liberté aux buts recherchés (art. L.1121-1 C. Trav.), et la Loi Informatique et Libertés doivent être respectés.

Les dossiers et fichiers créés par le salarié grâce aux outils informatiques mis à sa disposition par l'employeur sont présumés avoir un caractère professionnel, de sorte que l'employeur peut avoir accès aux courriels hors la présence du salarié⁶.

En revanche, il est interdit à l'employeur de prendre connaissance des messages personnels, au nom du droit au respect de la vie privée (arrêt Nikon⁷), à condition qu'ils soient identifiés comme tels. Il est alors interdit d'exploiter les courriels personnels pour motiver une sanction disciplinaire sauf diffusion ou enregistrement, ou transmission à l'employeur par un autre salarié ou autre source légitime. Le caractère personnel doit être apparent ou explicite, la rubrique « mes documents » ne signifie pas nécessairement personnel⁸.

Ces principes s'appliquent non seulement à l'ordinateur mis à disposition du personnel par l'employeur, mais par exemple à des clés USB connectées à l'outil informatique ou à des appareils personnels utilisés dans la sphère professionnelle (pratique dite « BYOD » (Bring you own device) ou « AVEC » (Traduisible par « Apportez Votre Équipement personnel de Communication »^{9 10}).

- En cas de transfert des résultats à l'étranger

Diverses législations étrangères ont une portée extraterritoriale, en particulier aux Etats-Unis (*Foreign Corrupt Practices Act*, législations sur le contrôle des exportations, droit antitrust, loi Sarbanes Oxley, lois relatives aux vices cachés ou à la sécurité des produits), et au Royaume-Uni (*Bribery Act 2010*).

Le transfert à l'étranger des résultats d'une enquête interne diligentée dans le cadre d'une procédure en application de ces législations est limité par le droit français :

- Loi Informatique et Libertés
- « Loi de blocage » (L. 26 juil. 1968/16 juil. 1980), interdisant la communication de toute information se rattachant à l'activité économique des entreprises sous peine de sanction pénale, sauf sous certaines conditions, notamment dans le cadre des traités internationaux (essentiellement la Convention d'entraide judiciaire internationale de La Haye de 1970).

C. Principales recommandations pratiques

- Etablir les « chartes informatiques » ou autres éléments du programme de *Compliance* comme des éléments du contrat de travail, en ayant présent à l'esprit l'éventualité d'une enquête interne et afin d'obtenir des preuves opposables lors de l'enquête.

- Il est essentiel de définir dans la charte informatique (annexée au règlement intérieur) et régulièrement mise à jour les règles de sécurité et l'utilisation des moyens informatiques mis à la disposition de l'employé par l'entreprise mais aussi de définir l'usage professionnel des outils personnels de l'employé.¹¹

6. Cass. Soc. 18 octobre 2006, n° 04-47.400

7. Cass. Soc. 2 octobre 2001, n° 99-42.942

8. Cass. Soc. 10 mai 2012, n° 11-13.884F-PB

9. *Bring Your Own Device* ou « Apportez Votre Équipement de Communication » ; arrêt Cass. Soc. 23 mai 2012, n° 10-23.521

10. Cass. Soc. 12 février 2013, n° 11-28649

11. Cass. Soc., 05/07/2011, n°10-14.685 commenté dans revue mensuelle LexisNexis 01/2012

En particulier, y définir l'usage professionnel dans le cadre de pratiques et techniques telles que le télétravail, réseaux sociaux, blogs, BYOD, etc.

- Répartition précise des responsabilités internes lors de l'enquête interne :

- désignation dans chaque unité opérationnelle ou fonctionnelle du responsable qui sera chargé d'aviser les dirigeants de l'entreprise, en urgence ou après première vérification des éléments de vraisemblance, en fonction de la gravité des faits signalés,
- désignation du responsable interne de l'enquête, constitution d'une cellule ad hoc (éléments de gestion de crise) ;
- établissement d'un cadre pour la documentation de l'enquête (fiches d'incident, etc.) pour éviter la consignation intempestive de réactions spontanées, et constituer des éléments de preuve exploitables et traçables ;
- rappel aux intervenants des règles applicables (obligations visées *supra*).

- Sélection des intervenants extérieurs éventuels et définition précise de leurs re-

sponsabilités (engagement de respecter la loi, règles de confidentialité, etc.) dans une lettre de mission qui doit rester évolutive en fonction des développements de l'enquête.

- Veiller au respect par les intervenants sélectionnés des règles applicables : confidentialité, respect des délais pour les sanctions, nécessité des consultations avec les représentants du personnel, assistance durant les entretiens, etc., tout en gardant à l'esprit que :

- l'employeur a le droit et l'obligation de contrôler ses salariés pendant le temps de travail, ce qui lui donne accès à des documents identifiés « privés/personnel » à condition que ce soit en présence de l'intéressé (et d'un témoin) ou que cette présence ait été requise, et en ayant le cas échéant recours à l'intervention du juge en référé (en France, art. 145 du Code de procédure civile), et aux systèmes d'information gérés par des tiers ;
- les moyens mis en œuvre et les effets « collatéraux » de l'enquête sur le fonctionnement des services concernés doivent être proportionnés à l'objectif pour suivi.

IV. L'impact du programme de Compliance sur la rémunération

La mise en œuvre de programmes de *Compliance* efficaces peut impliquer des conséquences affectant « en plus ou en moins » les rémunérations des salariés, soit qu'il s'agisse de sanctions en cas de non-respect du Programme de Compliance, soit qu'il s'agisse d'incitations pécuniaires.

A. Sanctions du non-respect du Programme de Compliance

Les salariés doivent être informés des sanctions encourues en cas de violation du Programme de Compliance.

Il n'est pas souhaitable de dresser un inventaire des sanctions déjà prévues par la législation (par exemple: délit d'initié),

Pour les sanctions non prévues par la législation, il importe de préciser que la violation des règles peut donner lieu à sanction et les définir dans un barème intégré au règlement intérieur.

En revanche, lors de la mise en œuvre des sanctions, un tel « barème » ne doit pas faire l'objet d'une application automatique. Il convient de procéder à une appréciation « au cas par cas » en fonction des circonstances de fait, des fonctions du salarié concerné, de son niveau de responsabilité dans l'entreprise et de son niveau de connaissance de ces règles ; ni de rester imprécis en indiquant dans le code d'Ethique que l'application des règles se fera en fonction des lois de chaque pays.

L'adjonction de ce barème des sanctions au règlement intérieur permet d'une part d'avoir un document opposable à tous et de faciliter la compréhension par les salariés de l'importance relative des règles figurant dans le code d'Ethique, en fonction de la sévérité des sanctions qui leur sont attachées.

B. Le cas particulier du non-versement de commissions, sanction de la « non-Compliance »

Dans certains cas, le non-versement de commissions constituant la rémunération des « commerciaux » salariés est la sanction prévue en cas de violation du code de conduite de l'entreprise. Ce système est à proscrire pour les raisons suivantes :

- le droit français interdit les sanctions pécuniaires prises à l'encontre du salarié (effet direct sur la rémunération) ;
- il n'est pas possible d'envisager une « double peine » : il est préférable de choisir

une sanction disciplinaire pouvant aller jusqu'au licenciement ;

- le retrait de la commission peut être une sanction insuffisante par rapport à la faute commise (faits de corruption par exemple).

C. La Compliance appréhendée dans la notation lors d'entretiens annuels

Les critères d'évaluation doivent être précis, objectifs et en lien avec l'exercice de la fonction (un critère comportemental tel que « qualité de communication » est légitime pour un manager ou un commercial¹²).

En revanche, il convient d'exclure la notation subjective portant sur les « valeurs de l'entreprise » lors des entretiens et de ne pas établir un lien direct entre la note globale et cette appréciation des valeurs.

Si l'entretien annuel fait apparaître des violations du code de conduite (faits de corruption par exemple), il faut appliquer rapidement les sanctions correspondantes (licenciement, mise à pied etc.) de façon à respecter les obligations de bref délai après le moment où l'employeur a connaissance de la faute (voir paragraphe III.B ci-dessus).

D. Rémunérations incitatives

Le respect du Programme de Compliance peut-il donner lieu à des rémunérations incitatives (incentives, bonus) ?

Des bonus peuvent encourager des actions qui visent à assurer la « promotion » de la Compliance par les managers, ou récompenser des résultats mesurables d'actions positives

12. Cass. Soc. 20 février 2008

prises dans le cadre de principes affirmés par le Programme de Compliance (par exemple, diminution du nombre d'accidents du travail en tant qu'élément des engagements de l'entreprise vis à vis de ses salariés).

En revanche, le strict respect des règles de *Compliance* est une obligation essentielle du salarié et ne doit pas se traduire par une rémunération spécifique.

COMPLIANCE PROGRAMMES AND LABOUR LAW

Principles of reflection

The purpose of this summary document is to identify the reflexes that should be adopted when a Company wishes to ensure that its employees adhere to Compliance Programmes, professional laws and codes, internal procedures and Code of Ethics.

The constraints of French labour law, which must be complied with in order to ensure the efficiency of a Compliance Programme, are identified below.

By its very brevity, this document does not claim to be exhaustive or to offer a didactic analysis of the subject or a practical guide.

This document is part of the ongoing work of the Cercle Montesquieu's Governance and Ethics Commission, identifying the principles that should be adopted when implementing Compliance Programmes (summary document: Compliance Programmes "Principles of reflection" - first edition January 2011).

I. Codes of Ethics: What is their legal efficacy?

Codes of Ethics bear witness to a desire by companies for transparency, improvement of their image and taking into account their social responsibility, even if this practice is developed following cases that have received a lot of media coverage regarding fraud, corruption and insider trading within large companies. It is generally the first element of a Compliance Programme and one the company's management instruments that is now unavoidable (see the document by the Ethics and Governance Commission "*Compliance Programmes: principles of reflection*" 2011).

Codes of Ethics formalise a set of standards, which must be known and applied by all employees in all countries where the company is established. This involves the company's legal rules and deontology, "values" and internal directives (policies): adherence to laws and regulations, conflicts of interest, insider trading, protection of the company's assets, competition law, fight against corruption, etc.

Despite the undeniable legitimacy of the approach, the question remains of their opposability on employees with regard to the employment law.

Codes of Ethics do not form part of specific regulations. There are not mentioned in the Labour Code. The regime of this purely optional document depends on the nature and the binding force of the rules it provides for (DGT [General Directorate of Labour] circular no. 22 of 19 November 2008).

Codes of Ethics that are confined, in general terms, to listing the moral commitments and

ethical values to which the company adheres, do not have true legal impact (as for example a document in which the company "wishes to propose sustainable employment conditions", etc.). They are essentially conceived as a strategic tool for communication with the company's employees and business partners (clients, suppliers, etc.). They are drafted rather freely subject to not causing harm to:

- the principle of non-discrimination (Art. L.1132-1 of the Labour Code),
- the personal rights and liberties of the employees (L.1121-1 and L.1321-3, (2)), in particular the freedom of expression,
- the employees' rights to direct and collective expression (L.2281-1, etc.).

On the other hand, certain Codes of Ethics set the rules (behavioural standards) of which the failure to comply with are accompanied by sanctions, or the application of which could come into consideration when calculating remuneration. In addition, certain codes of ethics are accompanied by means (warning systems) made available to the employees to blow the whistle on illegal wrongdoings without having recourse to the traditional hierarchical ladder. Whether or not they result from whistle-blowing, the violations detected may be the subject of internal investigations in order to determine what steps are to be taken.

All of these practices raise questions with regard to employment law and protection of private life.

II. Lawfulness and opposability of Codes of Ethics and professional warning systems

A. Codes of Ethics and employment law

- Lawfulness of Codes of Ethics

Compliance Programmes, of which Codes of Ethics are elements, must be considered as “additions to internal regulations” for the parties regarding discipline (Art. L.1321-5 Labour C.). Due to this, information and consultation is required from the works council (Art. L.432-1 Labour C.). The procedure involved, in order, the following steps:

- 1) Opinion of the CHSCT [Committee for Health, Safety and Working Conditions] in matters falling under its jurisdiction
- 2) Opinion of the works council or failing this staff representatives
- 3) Inspection of labour administration (labour inspector)

In addition, as with internal regulations, Code of Ethics must be displayed “*in a suitable place that is easily accessible in the workplace as well as in the rooms and on the doors of the rooms where hiring takes place*” (Article R.1321-1 Labour C.).

- Modes of integrating Compliance Programmes in employment agreement

There are no specific rules in the Labour Code as to the delivery of the document. Nevertheless, once the document contains obligations for the employee, it must be written in French (Art. L.1321-6 Labour C.). Case law strictly applies this rule with regard to “any document which the employee must be aware of in order to properly carry out his/her work”¹.

It is essential for companies to ensure the opposability of this document to employees. For this purpose, it is recommended to hand over the document upon hiring, for example through the signature of a letter against receipt.

Finally, the understanding of the rules and knowledge of the updates must be ensured by awareness and training actions, and frequent reminders.

- Unlawfulness if it reduces the rights of employees

Codes of Ethics cannot constitute a means of reducing the fundamental rights of employees in accordance with the principle of Article L.1121-1 Labour C. On the other hand, “*employees enjoy their freedom in the company and outside it and only restrictions justified by the nature of the task to be accomplished and in proportion to the required goal may be made to it*”².

In this case, they must be implemented as additions to internal regulations³.

B. Professional warning systems, employment law and protection of private life

- Adoption procedure and implementation of systems

If the Code of Ethics contains a professional warning system (according to DGT circular

1. C.A. Versailles, 2 March 2006 (no. 05-1344); C.A.

Paris, 1st Oct. 2010 (no. 08/23998)

2. Cass. Soc. 8 Dec. 2009 (no. 08-17.191).

3. Cass. Soc., 28 May 2008.

no. 22 of 19 November 2008, this involves a system put in place by a public or private organisation to encourage employees or any other persons carrying out an activity in the company to alert the company head, or, possibly, other persons appointed for this purpose “of problems that could critically affect its activity or hold it seriously liable”), the adoption procedure must be the following:

- prior authorisation from the CNIL [Commission on Information Technologies and Liberties] according to the deliberation of the CNIL no. 2005-305)
- consultation information of the CHSCT (Article L.4612-8 of the Labour Code),
- consultation information of the CE (Article L.2323-32 of the Labour Code).

The implementation of the system requires that employees be personally informed of, in application of the Data Protection Act and Article L.1222-4 of the Labour Code which sets out that “*no information personally concerning an employee may be collected by a system which is not brought to his/her attention in advance*”.

• Reminder of the rules promulgated by the CNIL

On 8 December 2005, the CNIL adopted deliberation no. 2005-305 authorising professional warning systems if they are compliant with the conditions of the Single Authorisation AU-004 appended to the deliberation. If the planned system is not compliant with the Single Authorisation, the company must file an authorisation application with the CNIL. Failing this, the system is at the very least not binding on the employees, and even unlawful if it is based on the collection of personal data.

The scope of application of the authorised systems was initially restricted to the “*financial, accounting and banking fields and the fight against corruption*” (including the fields covered by the American Sarbanes-Oxley law), except for the involvement of the “*vital interest*” of the company or the “*physical or moral integrity of its employees*”. Case law has made a strict application of this (Dassault Systèmes ruling⁴).

The CNIL at a later stage amended authorisation AU004, by deliberation of 14 October 2010, essentially by broadening the scope of the field of competition.

If the company wishes to implement a system reaching beyond the scope of application, for example to include discrimination practices therein, it must file an individual authorisation application, which will be examined by the CNIL on a case-by-case basis. After authorisation from the CNIL, the steps of the procedure described above must be followed.

The employees who wish to report an event not covered by the CNIL authorisation (single or individual) should use traditional methods (hierarchical ladder, informing the union representatives or the human resources departments) and not the warning system.

4. Cass. Soc., 8 Dec. 2009 (no. 08-17.191).

III. Internal investigations

A. For what reasons would the company be led to conduct an internal investigation?

The objectives of an internal investigation can be the legal classification of violations to applicable legislation (local or with an extraterritorial application) or to its Code of Ethics in order to involve the various departments of the company and the relevant outside counsels (legal and other) and to identify the competent courts, and/or to find proof in view of an internal or external procedure (the onus of proof rests on the employer!)

The company can be led to this in various circumstances

- The company is informed of an objectionable activity of which it would be the victim: fraud, breach of intellectual property, insider trading or misfeasance, violation of internal regulations, its Code of Ethics or other internal rules of operation (harassment, discrimination, remuneration, etc.).
- The company is informed of an objectionable activity in which it would be held liable (offence or other regulatory violation, competition violation, other breach to its Code of Ethics).
- Discovery as part of civil or criminal proceedings in common law, in which, either by obligation or by choice, the company must provide the other party with all the elements related to the case.

B. What obligations should it adhere to when conducting its internal investigation?

If the investigation can result in disciplinary sanctions, the applicable procedure must be respected.

• Employment law

The suspension of the employment agreement as a protective measure is possible for a limited period (which does not necessarily tally with the length of the investigation process).

The limitation period for the employer to exercise its disciplinary power (power of sanction or dismissal - Article L.1332-4 Labour C.) is two months, which involves the specific identification of the date on which the employer became aware of the wrongful behaviour, the speedy notification to the employee to attend a preliminary interview, the exact statement of the grievances noted during the interview and the speedy notification of the sanctions (Art. L.1332-2 Labour C.).

The employee is entitled to be assisted at the interview.

Abroad, several courts require the clear and transparent information of the rights and obligations of the employees being interviewed as part of an investigation; for example, in the United States, the “Upjohn” warning letter⁵.

• Protection of privacy

The basic principles of respect for privacy (Art. 9 of the Civ. C., Art. 8 of the ECHR [European Court of Human Rights]), the rule of proportionality of the restrictions

5. Upjohn v. U.S., 449 U.S. 383 (1981). The purpose of this letter is to inform the employee that the lawyer who is going to interview him represents the employer and that the information may be confidential but that the company reserves the option to waive this confidentiality and to communicate the information discovered to the administration. It only has value in the United States but clarifies the context.

to freedom for the intended purposes (Art. L.1121-1 Labour C.), and the Data Protection Act must be respected.

The documents and files created by the employee due to the IT tools made available to him/her by the employer are presumed to be of a business-related nature, so that the employer may have access to e-mails when the employee is not present⁶.

On the other hand, the employer is prohibited from perusing private messages, in the name of the right to respect privacy (Nikon ruling⁷), provided that they are identified as such. It is thus prohibited to use personal e-mails to motivate a disciplinary sanction except for distribution or registration, or transmission to the employer by another employee or other legitimate source. The personal nature must be apparent or explicit, the heading “my documents” does not necessarily mean personal⁸

These principles apply not only to the computer made available to the staff by the employer, but for example to the USB keys connected to the IT tool or the personal devices used in the business sphere (in practice called “BYOD” (Bring your own device),⁹)¹⁰

• In the event of communicating the findings abroad

Various foreign legislations have an extra-territorial impact, in particular in the United States (Foreign Corrupt Practices Act, legislations on controlling exportation, anti-

trust laws, Sarbanes Oxley law, laws relating to hidden defects or the safety of products), and in the United Kingdom (Bribery Act 2010).

The transfer abroad of the findings of an internal investigation launched as part of proceedings in application of these legislations is limited by French law:

- Data Protection Act
- “Blocking statute” (L. 26 Jul. 1968/16 Jul. 1980), prohibiting the communication of any information relating to the economic activities of companies subject to criminal sanction, except under certain conditions, in particular as part of international treaties (mainly The Hague International Judicial Assistance Convention 1970).

C. Main practical recommendations

• Draw up the “IT policies” or other elements of the Compliance Programme as elements of the employment agreement, and bearing in mind the possibility of an internal investigation and in order to obtain binding proof during the investigation.

• It is essential to define rules for the security and use of the IT equipment made available to the employee by the company in the IT policy (attached to the internal regulations) and regularly update them but also to define the business use of the employee’s personal tools.¹¹

In particular, to define the business use therein as part of the practices and techniques such as telecommuting, social networks, blogs, BYODs, etc.

6. Cass. Soc. 18 October 2006, no. 04-47.400

7. Cass. Soc. 2 October 2001, no. 99-42.942

8. Cass. Soc. 10 May 2012, no. 11-13.884F-PB

9. Bring Your Own Device; ruling by Cass. Soc 23 May 2012, no. 10-23.521

10. Cass. Soc. 12 February 2013, no. 11-28649

11. Cass. Soc., 05/07/2011, no. 10-14.685 commented on in the monthly review, LexisNexis 01/2012

- Specific distribution of internal responsibilities during an internal investigation:
 - appointment of the manager in each operational or functional unit who will be in charge of informing the company's managers, as a matter of urgency or after first verification of the elements of likelihood, depending on the seriousness of the events reported,
 - appointment of the internal investigation manager, forming an ad hoc committee (crisis management elements);
 - establishing a framework for the investigation documentation (incident forms, etc.) to prevent the untimely consignment of spontaneous reactions, and to constitute elements of proof that can be used and traced;
 - reminding participants of the applicable rules (obligations mentioned above).
- Selection of the possible external participants and specific definition of their responsibilities (commitment to respect the law, rules of confidentiality, etc.) in a mission

letter which must remain evolutive according to the developments of the investigation.

- See to it that the selected participants adhere to the applicable rules: confidentiality, adhering to the time limits for sanctions, need for consultations with staff representatives, assistance during interviews, etc., while bearing in mind that
 - the employer has the right and obligation to monitor its employees during work hours, which gives it access to documents identified as "private/personal" provided that this is done in the presence of the interested party (and a witness) or that this presence was required, and if applicable, having recourse to the intervention of the summary proceedings judge (in France, Art. 145 of the Code of Civil Procedure), and to the information systems managed by third parties;
 - the means implemented and the "collateral" effects of the investigation on the functioning of the services concerned must be in proportion to the objective sought.

IV. The impact of a Compliance Programme on remuneration

The implementation of efficient Compliance Programmes can involve consequences "more or less" affecting the remuneration of employees, whether it involves sanctions in the case of non-adherence to the Compliance Programme, or monetary incentives.

A. Sanctions for the non-adherence to a Compliance Programme

Employees must be informed of the sanctions incurred in the event of violation of a Compliance Programme.

It is not recommended drawing up an inventory of sanctions already provided for by legislation (for example: insider trading),

For the sanctions not provided for by legislation, it should be specified that the violation of rules can give rise to a sanction and to define them in a scale integrated into the internal regulations.

On the other hand, when implementing sanctions, such a “scale” must not be automatically applied. A “case-by-case” assessment should be conducted according to the circumstances of fact, the duties of the employee concerned, his or her level of responsibility in the company and his/her level of knowledge of these rules. A specification should also be indicated in the Code of Ethics that the application of the rules will be according to the laws of each country.

Adding this scale of sanctions to the internal regulations on the one hand provides a document binding on all and to facilitate the understanding by employees of the importance relating to the rules found in the Code of Ethics, depending on the seriousness of the sanctions related to them.

B. The specific case of non-payment of commissions, as a sanction of “non-Compliance”

In certain cases, the non-payment of commissions constituting the “commercial” remuneration of employees is the sanction provided for in the event of violation of the company’s code of conduct. This system is prohibited for the following reasons:

- French law prohibits monetary sanctions taken against an employee (direct effect on remuneration);
- it is not possible to foresee a “double penalty”: it is preferable to choose a

disciplinary sanction which could lead to dismissal;

- the withdrawal of commission can be an insufficient sanction in connection with the offence committed (for example, acts of corruption).

C. Compliance understood in the rating during the annual interviews

Assessment criteria must be specific, objective and in connection with carrying out the duty (a behavioural criterion such as “quality of communication” is legitimate for a manager or a salesman¹²).

On the other hand, the subjective rating based on the “company’s values” during interviews should be excluded and a direct link between the overall rating and this assessment of values does not have to be established.

If the annual interview shows violations to the code of conduct (for example, acts of corruption), the corresponding sanctions should immediately be applied (dismissal, lay-off, etc.) so as to adhere to the obligation of immediacy once the employer has found out about the offence (see paragraph III.B above).

D. Incentive remuneration

Can adherence to a Compliance Programme give rise to incentive remuneration (incentives, bonuses)?

Bonuses can encourage actions which intend to ensure the “advocacy” of Compliance by a manager, or rewarded by the measurable outcomes of the positive actions taken as part

12. Cass. Soc. 20 February 2008

of the principles affirmed by the Compliance Programme (for example, reduction in the number of workplace accidents as an element of the company's commitments towards its employees).

On the other hand, strict adherence to the rules of Compliance is an essential obligation of the employee and must not result in specific remuneration.

Le rôle du Directeur Juridique dans les rapports de l'entreprise avec les intermédiaires commerciaux et autres partenaires

1. Le présent document s'inscrit dans la ligne des travaux du Cercle Montesquieu sur les questions d'éthique et de gouvernance, qui ont donné lieu notamment à la publication en janvier 2011 du document « *Programmes de compliance : principes de réflexion* ». Il vise à préciser le rôle du directeur juridique dans la prévention des risques inhérents aux relations de l'entreprise avec ses intermédiaires commerciaux et autres partenaires¹,

spécialement en matière de corruption et d'infractions au droit de la concurrence. Il ne concerne pas les fonctions de responsable Compliance proprement dites, même si celles-ci sont parfois exercées par le directeur juridique lui-même ou sous son autorité.

1. Les agents et autres intermédiaires commerciaux ne sont pas la seule catégorie de partenaires de l'entreprise pouvant générer des risques, et la prévention des risques de corruption n'est pas la seule préoccupation que doivent poursuivre les programmes de compliance. Par exemple, l'association avec un distributeur indélicat peut entraîner des risques de droit

de la concurrence, le recours à un sous-traitant dans un pays insuffisamment régulé peut mettre en jeu la responsabilité de l'entreprise en matière de droits de l'homme. C'est pourquoi la pratique anglo-saxonne utilise le vocable de « *third parties* », que la CCI a transposé en français (« tierces parties ») et qu'elle définit dans le document « Règles d'ICC pour combattre la corruption » référencé en annexe, mais que nous avons préféré écarter en raison de son caractère excessivement vague. Dans le présent document, nous utilisons le terme « Intermédiaires » pour couvrir toutes ces catégories.

2. Les Intermédiaires sont un outil souvent indispensable pour les entreprises, notamment à la grande exportation quand les implantations directes sont inadaptées ou trop récentes. Ils sont cependant porteurs de risques importants : les commissions d'agents, en particulier, peuvent être un véhicule privilégié de la corruption, aux côtés des contrats de sous-traitance ou d'études factices, quand elles ne correspondent pas à des services réellement rendus et servent à la dissimulation de versements illicites.

Certains groupes, sensibles à la gravité de ces risques, ont décidé l'abandon du recours aux agents commerciaux, préférant affronter les conséquences immédiates de cette démarche sur leurs ventes dans certains secteurs et les changements qu'elle impliquait éventuellement à leur modèle économique. Toutes les entreprises ne peuvent naturellement pas franchir ce pas pour des raisons liées au degré de maturité de leur développement international, à la fragilité de leurs ventes ou à la nature du marché, ou ne le jugent pas nécessaire en fonction de leur appréciation du risque.

Elles doivent donc mettre en œuvre les moyens nécessaires pour prévenir ce dernier. Alors que les statistiques des O.N.G. spécialisées montrent que la corruption dans le monde ne recule pas, les risques ne font qu'augmenter pour les entreprises convaincues ou soupçonnées de corruption dite « active ». En effet, outre qu'il n'est pas possible de fonder durablement la croissance ou même la survie d'une entreprise sur des pratiques condamnables sur le plan éthique, les nouveaux moyens de communication sociale et l'intérêt des media pour ces questions maximisent le risque en matière d'image

et de réputation. En outre, les instruments juridiques répressifs internationaux qui se sont multipliés ces dernières années ont maintenant des effets sensibles. On rappellera simplement la Convention de l'OCDE du 17 décembre 1997, transposée en France par la loi du 30 juillet 2000, et les effets extra-territoriaux du *Foreign Corrupt Practices Act* américain et du *Bribery Act* britannique.

3. Le rôle du directeur juridique dans les programmes de prévention des risques liés aux Intermédiaires est particulièrement sensible. D'un côté, il ne peut assumer la responsabilité du choix et du contrôle de ceux-ci : il s'agit clairement d'une responsabilité opérationnelle et il ne dispose ni des connaissances sectorielles ni des moyens de contrôle financier nécessaires à cette tâche. S'il y participe (par exemple parce qu'une procédure interne prévoit qu'il doit donner son « visa » aux contrats d'agents), la portée exacte de sa responsabilité doit être définie. D'un autre côté, le directeur juridique ne peut être absent du processus : le contrôle des relations avec les Intermédiaires est un élément important du programme de *compliance* dont il est impérativement partie prenante, et qui s'inscrit dans sa mission générale de prévention des risques.

4. Le présent document n'a évidemment pas pour objet de proposer des lignes directrices ou recommandations quant à la structuration et la mise en œuvre des programmes de *compliance* relatifs aux relations avec les Intermédiaires.

On se contentera donc de renvoyer aux principaux documents édités par les organisations internationales qui prodiguent

de telles recommandations, lesquelles peuvent généralement se résumer ainsi :

- il est essentiel d'effectuer une revue aussi détaillée que possible de « *due diligence* » avant de conclure un contrat avec l'Intermédiaire ;
- le contrat doit comporter toutes les précautions nécessaires pour établir clairement que le partenaire est pleinement responsable de respecter non seulement la loi, mais aussi les principes d'éthique du mandant ou entrepreneur principal ;
- un contrôle doit s'opérer lors de la conclusion et lors de l'exécution du contrat quant à la cohérence entre les sommes versées (notamment sous forme de pourcentage d'un contrat principal) et les services réellement rendus : cette règle est particulièrement difficile à respecter concernant les contrats d'agents, en raison de la difficulté de mesurer le service rendu, du fait qu'un « *success fee* » rémunère non seulement les efforts déployés pour le succès d'une affaire mais ceux déployés en vain pour d'autres affaires, et de la réticence extrême des intermédiaires à donner accès à leur comptabilité.

Les principaux documents des organisations internationales sur ce sujet sont référencés en annexe.

5. Le directeur juridique doit s'assurer de la présence, de la pertinence et du maintien d'un processus de prévention des risques applicable aux relations avec les Intermédiaires (mais, comme dit plus haut, il ne lui appartient ni de le gérer ni d'en garantir l'efficacité) :

a) *sélection des Intermédiaires :*

Celle-ci reste la responsabilité des services opérationnels, mais il importe qu'il existe un processus de *due diligence* complet et dûment documenté afin d'éliminer les partenaires présentant des risques susceptibles d'être identifiés avant la mise en place de la relation. Le directeur juridique doit :

- participer à la définition de la procédure (analyse de la typologie des risques, vérification de l'implication des responsables compétents, nature des informations devant être recueillies, recours éventuel à des tiers évaluateurs) ;
- fournir les éléments proprement juridiques de ce processus : validation des méthodes d'investigation éventuellement utilisées, vérifications auprès des registres du commerce, etc.

b) *conclusion des contrats :*

Le directeur juridique est responsable de l'édition et de la mise à jour (en liaison avec les responsables de la compliance et les services opérationnels) de contrats-types obligatoires. Les contrats doivent en effet intégrer non seulement les mesures de protection de l'entreprise (par exemple conditions de paiement, clauses de résiliation automatique, interdiction de céder ou sous-traiter le contrat, etc.), mais aussi des dispositions facilitant la mise en œuvre de ces protections (obligation de signaler les éléments modifiant les données sur la base desquelles la sélection a été opérée, audits obligatoires, etc.).

Le directeur juridique doit également s'assurer qu'il existe des procédures contraignantes de centralisation et de validation (avec une définition claire de la

portée de la responsabilité de chacun) pour la signature, le renouvellement, la modification ou l'expiration des contrats : approbation par l'ensemble des services compétents, absence de procédures dérogatoires permettant de contourner l'application des règles, etc.

De même, il doit s'assurer de l'existence et du maintien d'une procédure fiable de contrôle des paiements et de la réalité des services rendus, qui reste la responsabilité des services opérationnels concernés sous le contrôle des services financiers.

6. Le directeur juridique doit s'assurer que les questions relatives à la prévention des risques de corruption et autres dans la gestion des Intermédiaires sont bien prises en compte par le programme de compliance, dont le processus de sélection et de gestion des Intermédiaires visé ci-dessus est un des éléments.

En particulier, il participe activement :

- à la conception et à la mise en œuvre des programmes de formation destinés aux opérationnels concernés, et éventuellement aux Intermédiaires eux-mêmes (sessions

de formation, codes de conduite, modules interactifs, outils du type « RESIST » de la CCI, etc.) ;

- aux contrôles (assistance aux renouvellements des *due diligences*, audits internes et éventuellement externes, alertes ou déclenchement d'enquêtes si nécessaire).

7. Il revient naturellement au directeur juridique d'assurer son rôle normal de conduite de la défense de la société en cas d'incidents :

- contentieux avec les intermédiaires dans le cadre de l'exécution de leur contrat ;
- contentieux avec des tiers (clients, fisc, actionnaires, etc.) mettant en cause le rôle de l'intermédiaire.

En conclusion, il est important et nécessaire, tant pour l'image de sa société que pour le positionnement adéquat de sa fonction, que le directeur juridique participe activement aux initiatives professionnelles (sectorielles ou générales) de promotion des programmes de compliance, en particulier en matière de lutte contre la corruption.

Annexe

Recommandations publiées par les organisations internationales en matière de programmes de compliance

- OECD : « Guide de bonnes pratiques pour les contrôles internes, la déontologie et la conformité » annexé à la Recommandation du Conseil visant à renforcer la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales (<http://www.oecd.org/dataoecd/11/40/44176910.pdf>)

- CCI : « Règles d'ICC pour combattre la corruption » (éd. 2011), http://www.iccwbo.org/uploadedFiles/ICC/policy/business_in_society/Statements/ICC_Rules_on_Combating_Corruption_2011edition.pdf,

- « Principes Directeurs d'ICC sur les dispositifs d'alerte éthique », [http://www.iccwbo.org/uploadedFiles/ICC/policy/anticorruption/Statements/French%20version%20of%20ICC%20Whistleblowing%20Guidelines.dot\(1\).pdf](http://www.iccwbo.org/uploadedFiles/ICC/policy/anticorruption/Statements/French%20version%20of%20ICC%20Whistleblowing%20Guidelines.dot(1).pdf)

- Manuel ICC « Fighting Corruption » (éd. 2008) <http://iccwbo.org/uploadedFiles/Bookstore/678%20table%20of%20content.pdf>

- Plus précisément : « ICC Guidelines on Agents, Intermediaries and other third parties » (19.11.10) <http://www.iccwbo.org/uploadedFiles/ICC/policy/anticorruption/pages/195-11%20Rev2%20ICC%20Third%20Parties%20FINAL%20EN%2022-11-10.pdf>

- « RESIST - Résister aux extorsions de fonds et aux sollicitations dans le cadre des transactions internationales », outil d'entreprise pour la formation des salariés développé conjointement par ICC, Transparency International, le Global Compact des Nations Unies et le World Economic Forum : http://www.iccwbo.org/uploadedFiles/ICC/policy/business_in_society/pages/RESIST_FR_text.pdf

- Norme ISO 26000 sur la responsabilité sociétale : http://www.iso.org/iso/fr/iso_catalogue/management_and_leadership_standards/social_responsibility/sr_discovering_iso26000.htm.