PROGRAMMES DE *COMPLIANCE* : DIX BONNES PRATIQUES OBSERVÉES EN FRANCE

par Emmanuel Breen
Avocat au barreau de Paris, maître de conférences à Paris-Sorbonne Universités, co-responsable du DU « Compliance Officer » (Panthéon-Assas), counsel Laurent Cohen-Tanugi Avocats

et Antoinette Gutierrez-Crespin
Expert-comptable, Associée Ernst & Young et Associés, Fraud Investigation & Dispute Services, spécialité Compliance

Dès que l'on parle de *compliance*, les questions fusent : la *compliance*[1], venue des États-Unis, est-elle adaptée aux réalités françaises ? Les « bonnes pratiques » en matière de *compliance* : s'agit-il d'un énième catalogue théorique ? Ces pratiques nécessitent-elles un haut niveau d'exigence, réservé uniquement aux entreprises les plus matures sur ce sujet ? Si l'on connaît le coût d'un tel investissement, qu'en est-il de sa rentabilité ? Ce florilège de questions sous-tend généralement une seule question : « Quelles sont en réalité les pratiques des entreprises françaises en matière de *compliance* ? ».

1. D'origine anglo-saxonne, la notion de *compliance* se traduit littéralement en français par le terme « conformité » mais cela lui fait perdre la dimension culturelle et l'origine anglo-saxonne qui lui est attachée. Dans cet article, nous utiliserons le mot « compliance » étant entendu que certaines entreprises utilisent le terme « conformité ».

Sur ce point nous avons souhaité apporter notre contribution en proposant aux entreprises un *benchmark* des meilleures pratiques en matière d'organisation et de programmes de *compliance*, telles que nous les avons observées ou qu'elles nous ont été décrites.[2] Cette étude n'a pas vocation à constituer une description exhaustive mais à montrer comment les entreprises françaises sont capables de se transformer et d'innover pour faire face aux nouveaux risques éthiques et juridiques.

Les résultats de cette étude ne sont pas issus d'une analyse quantitative et se basent sur nos observations et analyses des bonnes pratiques identifiées au fil de nos expériences respectives, ainsi que sur les résultats d'une enquête qualitative conduite auprès des responsables de la *compliance* d'une dizaine d'entreprises dont le siège social est implanté en France[3]. Cette enquête a été menée au moyen d'entretiens semi-directifs[4] réalisés au cours des 2e et 3e trimestres 2015. Les entretiens ont été réalisés sous condition d'anonymat. Nous remercions chaleureusement toutes celles et ceux qui ont consacré du temps pour répondre à nos questions. Le fait qu'ils aient accepté d'y répondre constitue déjà en soi une bonne pratique : en effet, la capacité de l'entreprise à échanger sur des sujets aussi sensibles et plus généralement à **libérer la parole dans l'entreprise**, est un point de départ et la première des bonnes pratiques que nous avons relevées.

L'une des premières questions abordées avec nos interlocuteurs a porté sur la signification du terme *compliance* et la façon dont ils délimitent leur programme et leurs compétences. Pour la majorité d'entre eux, la *compliance* est avant tout un dispositif interne qui permet à l'entreprise de s'assurer du respect des lois, des réglementations et des règles dont elle s'est dotée, quel que soit le lieu où elle opère. Ainsi, l'éthique et la *compliance* vont de pair, tout en restant distinguées dans l'organigramme de l'entreprise. Quel que soit le choix d'organisation et de gouvernance en la matière, nous sont à cet égard apparues comme des bonnes pratiques la capacité à **coordonner l'Éthique et la *Compliance***, ainsi que celle du *Chief Compliance Officer* (CCO) à exercer un rôle de « **chef d'orchestre** », sans nécessairement être « propriétaire » de l'ensemble des sujets couverts par le programme de *compliance*.

Lors de nos échanges avec les entreprises, nous avons été frappés par les différents niveaux de maturité dans la conception, le développement et la mise en place des moyens de contrôle des dispositifs de *compliance*. Cependant, l'actualité ne cesse de nous rappeler que nous évoluons dans un monde global où il devient difficile de soutenir qu'un groupe n'aurait pas besoin de structurer un programme de *compliance* adéquat et efficace, au motif que les valeurs qui

2. Voir également, notamment : 2013 Ethics & Compliance Leadership Survey Reports, LRN Corporation ; Étude annuelle EY 2016 « Fraud and Corruption, the easy option for growth ».

3. Les entreprises rencontrées réalisent leurs activités dans le secteur industriel ou les services. Elles n'ont pas d'activités bancaires ou d'assurance. Il s'agit essentiellement de groupes internationaux présents chacun dans plus d'une cinquantaine de pays.

4. Nous remercions M. Brooks Hickman de son assistance lors de la phase préliminaire de ce projet et Mme Laura Pessanha pour son aide lors de la phase rédactionnelle.

l'habitent suffiraient à le protéger contre des mauvaises pratiques. Or, certaines entreprises françaises n'ont pas encore transcrit dans leur organigramme l'une des données de base d'un programme de *compliance*, qui est l'existence d'un responsable identifié dans l'entreprise, doté de l'indépendance et des moyens nécessaires. D'autres au contraire sont en avance, comme celle-ci, qui a prévu un ***double reporting*** **du CCO au Directeur général et au Président du Comité d'audit**.

Si certaines des entreprises interrogées déploient des trésors d'ingéniosité, mettent en place des outils sophistiqués et cherchent à tester l'efficacité des mesures prises, d'autres n'en sont qu'aux prémisses, c'est-à-dire au stade d'identification des principales actions à déployer. Force est de constater que les groupes très centralisés sont souvent plus avancés en terme de conception du cadre général et de déploiement des procédures et politiques. Ce constat fait sens : plus l'autonomie des filiales est importante, les activités et modèles économiques multiples et les systèmes d'organisation et d'informations internes complexes, plus il est difficile de concevoir et déployer un programme de *compliance*.

Il est donc intéressant de **concevoir ensemble le programme de complicance et la politique de centralisation de l'entreprise**. De manière plus générale, selon le secteur et les réglementations qui le concernent, la taille, l'organisation et les risques spécifiques, le modèle de *compliance* devra être adapté aux opérations. Les efforts devront être dimensionnés en fonction des risques, comme cela est recommandé dans les différentes lignes directrices, tant du côté du Service central de prévention de la corruption français que de celui du FCPA (Foreign Corrupt Practices Act) ou du UK Bribery Act[5]. En quelques mots, à chaque « *business model* » son propre système de *compliance*. Pour autant, la capacité du siège à acquérir une bonne visibilité des risques *compliance* sur l'ensemble du groupe est essentielle. Certains de nos interlocuteurs nous ont ainsi expliqué comment leur entreprise avait pu mettre en place **une cartographie fine des risques, adaptée aux enjeux locaux**, selon une méthodologie développée au niveau du groupe.

Cet enjeu de visibilité concerne en premier lieu **les tiers avec lesquels l'entreprise entre en relation**. Par exemple, si celle-ci utilise certains tiers, tels que des agents, des intermédiaires ou des consultants, pour gagner des marchés, son exposition à des risques tels que la corruption devra être considérée comme élevée. Si le tiers est immatriculé ou opère dans un pays où la perception de la corruption est élevée, le risque sera encore plus prégnant. Des facteurs aggravants peuvent également se rajouter si le tiers effectue sa prestation dans un autre pays que celui où il est payé, si la structure de son actionnariat est opaque, etc. Car aujourd'hui, la responsabilité de l'entreprise ne s'arrête pas aux bornes de ses paiements. L'entreprise est devenue comptable du choix éclairé de ses partenaires. En conséquence, il lui revient de justifier des raisons de la sélection

5. V. not. E. Breen, *FCPA : La France face au droit américain de la lutte anti-corruption*, Lextenso, coll. Joly Pratique des affaires, à paraître janv. 2017.

du tiers selon les nouveaux standards de la *compliance* : vérification de son intégrité et des modèles de rémunérations selon lesquels elle contracte avec ce tiers. Il lui incombe ainsi de procéder aux contrôles adéquats, sur la base de son appréciation du risque, et d'en tirer les conséquences. Certaines entreprises ont d'ailleurs entrepris de créer un **registre informatique des parties tierces**, propre à centraliser l'ensemble des informations pertinentes, en matière notamment d'intégrité et de vérification de l'absence de ces tiers, de leurs actionnaires ou dirigeants sur les listes de sanctions.

La nouveauté qu'introduit l'approche en termes de programme de *compliance* tient aussi à la place et à l'efficacité de la formation interne. Dès lors que l'entreprise s'engage dans une politique de promotion des comportements éthiques et conformes aux attendus, elle revalorise nécessairement la formation, comme l'un des outils permettant de mieux rendre opérationnels les grands principes interdits communiqués. La formation sort ainsi souvent d'un relatif isolement, pour mieux s'articuler avec un ensemble d'actions de prévention et de contrôle. Il nous a semblé intéressant dans ce contexte d'observer que l'une des entreprises que nous avons interrogées avait mis en place sur un support informatique un **outil d'auto-évaluation des pratiques** des collaborateurs en matière de *compliance*, comme instrument de sensibilisation et de formation.

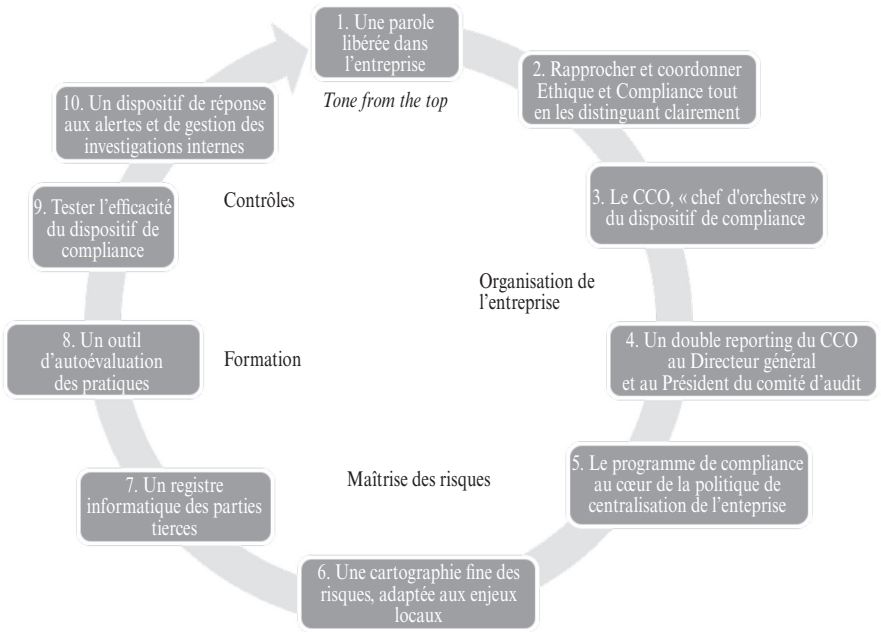
Mais une telle auto-évaluation ne saurait tenir lieu de **vérification de l'efficacité du programme de *compliance***. Cette dimension du contrôle est essentielle et est curieusement souvent peu mise en avant par les responsables *compliance*, qui choisissent d'endosser des habits « amicaux » plus que « répressifs ». Pourtant, aujourd'hui, l'enjeu des programmes de *compliance* ne se réduit pas à la création d'un code d'éthique, d'un corpus de règles et procédures et d'une ligne d'alerte. En effet, la notion d'efficacité et de performance du dispositif de *compliance* devient cruciale pour les régulateurs.

Il va donc devenir difficile d'expliquer aux administrateurs, aux actionnaires et investisseurs publics ou privés, et aux diverses parties prenantes (banquiers, assureurs, etc.), ainsi qu'aux régulateurs tant français qu'étrangers, qu'un groupe a mis en place un dispositif sans le tester. Quant aux tests « grandeur nature » d'efficacité du dispositif – nous y reviendrons ultérieurement – certaines des entreprises rencontrées sont loin des méthodes systématiques mises en œuvre par certains groupes américains. Il est vrai que notre système juridique français n'encourage pas les groupes à détecter des anomalies, en l'absence d'incitation à la « self disclosure ».

Il n'en est pas moins indispensable pour les entreprises d'une certaine taille de veiller, non seulement à mettre en place une ligne d'alerte éthique (*whistleblowing hotline*) mais surtout d'en assurer l'efficacité et le contrôle, par un **dispositif rigoureux de réponse aux alertes et de gestion des investigations internes**.

Ainsi, malgré la diversité des approches mises en œuvre dans les différentes entreprises interrogées dans cette étude et les difficultés de la comparaison entre entreprises de cultures, tailles et activités différentes, certaines pratiques, telles

qu'elles nous ont été décrites, sortent du lot et peuvent constituer une source d'inspiration pour tous. Les voici résumées par le schéma suivant, qui adopte la forme circulaire que connaît bien toute la communauté de la *compliance*.



I – BONNE PRATIQUE N° 1 : UNE PAROLE LIBÉRÉE DANS L'ENTREPRISE

Premier enseignement de notre enquête : les entreprises acceptent sans grande difficulté de parler de *compliance*, de risque éthique, de fraude, de sanctions internationales ou de corruption. Les entreprises que nous avons rencontrées ont ainsi été plus discrètes sur la question du budget du département *compliance* que sur celle de la nature des risques auxquels leur entreprise fait face en matière éthique et juridique. Il est donc généralement possible de parler de ces risques, sans tabou particulier. C'est le résultat, pour certaines entreprises, d'une évolution considérable.

C'est le cas de cette entreprise multinationale opérant dans un secteur et dans des pays fortement marqués par la corruption, et qui, confrontée à des poursuites, a initié il y a quelques années un ambitieux programme de *compliance*. Interrogé sur les facteurs de succès de ce programme, le CCO nous a répondu :

> Ce qui me conforte, c'est quand je regarde où on en était lorsqu'on a lancé le programme et où en est maintenant. Par exemple, aujourd'hui on entend parler de compliance au restaurant d'entreprise. Il y a quelques années, le mot "fraude" était un gros mot.

On en parle au restaurant d'entreprise… Voici une bonne pratique qui peut sembler bien modeste, surtout après plusieurs années d'efforts de l'entreprise en matière de *compliance*. Pourtant, chacun sait combien il peut être difficile d'aborder ces sujets, et de changer une culture d'entreprise fondée sur le secret ou la peur.

Le « tone from the top », ce n'est pas en effet seulement un discours ferme et univoque du chef d'entreprise sur les questions d'éthique et de *compliance*. C'est la capacité de ce chef d'entreprise à faire émerger ces questions comme des paramètres à véritablement prendre en compte dans toute la vie de l'entreprise. Le sujet, qui était jadis réservé à un petit « club » de gestionnaires des « affaires sensibles » ne doit pas être transféré exclusivement aux *Compliance Officers*. Tout collaborateur dans l'entreprise doit pouvoir en parler, sur la base d'un vocabulaire et de références communes. Chacun doit pouvoir se positionner sur le sujet.

Mais comment faire pour libérer la parole ?

Le CCO d'une autre entreprise nous explique comment son département *compliance* s'efforce, dans sa communication avec le reste de l'entreprise, de bousculer certaines frilosités :

> On prend nos responsabilités. Avec les équipes, on ne joue pas la comédie : est-ce qu'on l'a fait [une pratique non conforme] ou est-ce qu'on ne l'a pas fait ? Il faut faire quoi pour arrêter ?

Le « tone from the top » est ici fondé sur une forme de « parler vrai », sur des questions et un dialogue. Si en effet les équipes n'arrivent pas elles-mêmes à mettre des mots sur leurs pratiques et à imaginer des solutions, le programme de *compliance* risque de ne pas véritablement « s'enclencher » et de rester à la périphérie de la vie de l'entreprise.

Signalons pour conclure l'écueil inverse, qui guette les entreprises les plus avancées dans leur programme de *compliance :* qu'une ancienne culture du secret soit remplacée par une forme de discours convenu de la *compliance*. Une tendance à l'uniformisation du discours de la *compliance*, autour de formules toutes faites et maintes fois martelées peut ainsi s'observer, en France mais surtout dans d'autres pays globalement plus matures sur ce sujet. Cet écueil pourrait provenir du fait que la *compliance* est, dans certaines entreprises, devenue tellement prioritaire dans l'agenda des dirigeants que personne n'ose faire un pas de côté et donner véritablement son avis sur tel ou tel problème ou tel ou tel aspect du programme.

II – BONNE PRATIQUE N° 2 : RAPPROCHER ET COORDONNER ÉTHIQUE ET *COMPLIANCE* TOUT EN LES DISTINGUANT CLAIREMENT

Plusieurs entreprises rencontrées distinguent deux départements : l'un pour l'éthique et l'autre pour la *compliance*, chacun ayant son propre périmètre d'action. Historiquement, en effet, beaucoup d'entreprises françaises ont disposé

d'un directeur de l'éthique, ou d'un comité d'éthique, avant d'identifier dans leur organigramme une fonction *compliance*. Ces deux fonctions ont bien un rôle et des objectifs nettement différents. Mais aujourd'hui, la dimension juridique est devenue cardinale : les mauvaises pratiques n'engagent pas seulement l'éthique personnelle ou la réputation de l'entreprise mais, plus que jamais, le risque d'un procès pénal. En particulier, l'irruption de la justice américaine dans la répression des entreprises françaises a très nettement relevé le niveau du risque perçu et conduit les entreprises à envisager les problèmes en termes de conformité au droit autant que d'éthique. En matière d'organisation, la difficulté consiste, pour beaucoup d'entreprises, à faire une place à un nouveau département *compliance*, dont le périmètre d'action tienne compte des structures et personnes déjà en place, bien sûr, en matière d'éthique. Il ne s'agit pas de remplacer des fonctions performantes de l'entreprise, et qui traitaient déjà de sujets éthique ou *compliance*, mais d'identifier les risques auxquels l'entreprise est exposée et qui ne sont pas couverts.

Par ailleurs, des rapprochements et des articulations sont souhaitables. Ainsi, l'un des groupes rencontrés, où la *Compliance* se cherche encore une place face à l'Éthique, a créé un comité « éthique et *compliance* » qui couvre les deux domaines, en assurant la cohérence et la complémentarité. Cet effort pour coordonner l'Éthique et la *Compliance*, sans pour autant les fusionner entièrement, nous semble aller dans le bon sens.

Un rapprochement peut également concerner les réseaux de correspondants dans l'entreprise. Ainsi, par exemple, dans cette entreprise qui n'a pas connu de grave crise en matière de *compliance*, la fonction *Compliance* est relativement récente, et postérieure à la fonction Éthique. La fonction *Compliance* a commencé à se développer à partir du moment où l'entreprise a été soumise aux exigences de SOX et a pris sa place en tant que telle dans l'organigramme de l'entreprise en 2012 seulement. Mais l'interlocuteur insiste sur le fait que depuis peu, l'Éthique et la *Compliance* « sont ensemble », et que l'objectif de l'entreprise est de les rapprocher. Ici aussi, le « comité d'éthique » est chargé aussi bien de l'éthique que de la *compliance*, même si leurs objectifs restent différents. Le CCO y est considéré comme pleinement compétent sur des questions de déontologie professionnelle, sans être en principe en concurrence avec un « Directeur de l'Éthique ». Et les deux réseaux de correspondants existant actuellement (correspondants Éthique et correspondants *Compliance*) ont vocation à être fusionnés.

Par contraste, d'autres organisations apparaissent davantage marquées par une division du travail et des frontières entre Éthique et Compliance, qui semblent s'expliquer essentiellement par l'histoire de l'entreprise.

Ainsi, dans ce groupe sensibilisé depuis très longtemps aux questions d'éthique et où coexistent aujourd'hui un directeur de l'Éthique et un CCO, le premier est chargé des principes et de la « Charte éthique » et il revient au deuxième de mettre en œuvre ces principes. Le CCO nous explique : « je dis au directeur de l'Éthique : « toi, tu es Moïse ! ». Le CCO insiste ainsi sur la

nature essentiellement opérationnelle de son activité et son positionnement sur les procédures et les outils. Mais des compétences essentielles en matière de *compliance*, comme le suivi des alertes, lui échappent et restent dans le giron du directeur de l'Éthique. Cette situation semble d'ailleurs assez fréquente dans les entreprises où coexistent un directeur de l'Éthique et un CCO.

Dans une autre entreprise encore, où il n'existait préalablement aucune organisation de l'Éthique, la fonction *compliance* se développe plus facilement. Mais cela peut être au risque d'une certaine déconnexion de la *Compliance* et de l'Éthique :

> Chez nous, il n'y a pas de formalisation de l'éthique. Nous avons choisi une approche opérationnelle, fondée sur des outils, davantage qu'une approche déontologique.

Cependant, et c'est l'un des rares traits communs pour la majorité des entreprises rencontrées, la *compliance* est considérée comme un thème moins porteur que l'éthique, car elle véhicule l'idée d'une *conformité* imposée et plus généralement, d'un frein potentiel au développement et à la créativité. Un CCO nous explique ainsi la différence qu'il fait entre l'éthique et la *compliance* : « L'éthique ça vient de l'intérieur de l'entreprise, et de vous. La *compliance*, ça s'impose à vous ». La *compliance* n'est donc pas encore suffisamment perçue ici comme un outil de compétitivité, de différenciation par rapport aux concurrents, de bonne gouvernance et favorisant le progrès.

III – BONNE PRATIQUE N° 3 : LE *CHIEF COMPLIANCE OFFICER* (CCO), « CHEF D'ORCHESTRE » DU DISPOSITIF DE *COMPLIANCE*

Nous avons souhaité aborder avec nos interlocuteurs une question fort structurante mais souvent laissée dans l'implicite par les entreprises : quel est exactement le périmètre des sujets dont le département *compliance* est responsable, et quelle est, à leur égard, la nature du rôle du CCO ?

Parmi les domaines que peuvent traiter les départements *compliance* des entreprises rencontrées, figurent souvent l'anti-corruption, l'*export control* et les sanctions internationales, les données personnelles et le respect des règles de la concurrence. S'y ajoutent parfois d'autres sujets de conformité juridique, mais aussi le développement durable, la responsabilité sociétale, les droits de l'Homme ou des questions liées aux ressources humaines. Un de nos interlocuteurs, qui est responsable à la fois de la *compliance*, de la responsabilité sociétale et des droits de l'Homme au niveau groupe, établit une distinction :

> On n'a pas mis les droits de l'Homme dans la *compliance* car il ne s'agit pas seulement du "droit dur". Nous n'avons pas encore sur ce sujet le niveau de maturité qui permet d'être aussi strict qu'en *compliance*.

En effet, le cœur d'un programme de *compliance*, c'est le respect des règles, et nombre de CCO définissent leur fonction comme concernant potentiellement

l'ensemble des règles auxquelles l'entreprise est soumise, ou qu'elle s'engage à respecter. Cela nous semble être souvent la bonne approche, à condition de préciser que la responsabilité globale du CCO ne signifie nullement que le CCO et son département *compliance* sont directement chargés de l'ensemble des sujets. Dans ce contexte, les *Compliance Officers*, lorsque nous leur avons demandé de se décrire, ont pu se comparer à un « chef d'orchestre » entre plusieurs départements, un « super » *risk officer* sur certains domaines transverses, ou encore un « gardien d'une deuxième ligne de défense ».

Autant que les métaphores, les modalités de cette fonction de coordination d'ensemble peuvent être variées. Ainsi, par exemple, dans une grande entreprise industrielle, le responsable de la *compliance* réglementaire travaille seul, sans équipe propre, en lien avec d'autres fonctions de contrôle (éthique, risques, juridique, audit interne, notamment) et avec les responsables de chacun des domaines réglementés. Mais son travail est structuré par la tenue d'une matrice des risques en matière de conformité réglementaire : ces risques sont identifiés systématiquement par le responsable conformité. Pour chaque risque, une fiche de risque détermine, selon une méthode harmonisée, leur niveau de gravité sur une échelle de 1 à 4 et retrace la démarche de surveillance et d'amélioration : le risque est-il suffisamment mitigé, et comment ? Le responsable de la *conformité* réglementaire, sans avoir de responsabilité directe sur aucun chapitre de la *compliance*, dispose d'une « vision à 360° » pleinement transversale sur tous les sujets, et travaille en réseau avec toutes les autres fonctions de contrôle. Parmi les améliorations récentes de cette matrice figure la mise en place de plans de surveillance pour les risques classés 3 ou 4 (suivi des incidents et résultats des contrôles).

Bien que légère, cette fonction est utile en ce qu'elle cherche à clôturer et hiérarchiser l'univers des risques de non-conformité. Le risque serait cependant qu'à vouloir trop embrasser le CCO reste trop extérieur à ses sujets et tombe dans une forme de procéduralisme insuffisamment efficace. Raison pour laquelle, particulièrement dans les entreprises intervenant sur des marchés régulés, la réglementation sectorielle est laissée en dehors du champ de compétences du département *compliance*. Cette réglementation sectorielle est en effet gérée depuis longtemps par ailleurs dans l'entreprise.

Dans une autre entreprise, le CCO insiste sur son rôle de facilitateur :

> Nous avons une burette d'huile. Il y a des sujets dont nous ne sommes pas propriétaires, mais sur lesquels nous nous assurons que le sujet est bien traité (…) Il y a des sujets dont nous sommes propriétaires, d'autres, par exemple l'anti-trust, que nous suivons de plus loin (…) Mais notre périmètre est global, potentiellement [sur toute la conformité légale et réglementaire] (…) Par exemple, récemment nous avons identifié un nouveau sujet. Nous avons alors trouvé un responsable, réuni les *stakeholders* et produit un nouveau document de référence.. Une approche qui fait penser à celle que développent les directions de la qualité.

Un autre interlocuteur, à la tête d'un important département *compliance*, insiste sur l'importance qu'il y a à désamorcer les conflits de territoire :

> L'anti-trust est fait par le juridique, mais il est soumis à l'analyse de risque de la *Compliance*. Si je vois un problème avec l'anti-trust, je le dis, mais ce n'est pas pour autant que je vais essayer d'élargir mon empire.

Ces périmètres et les modalités du travail en réseau gagnent à être explicités au moment de la nomination. Certains CCO ont ainsi expliqué qu'ils disposaient d'une lettre de mission spécifique du dirigeant précisant les attentes en matière de *compliance* et, pour l'une d'entre elles, spécifiant également les modalités d'interactions avec l'Audit interne, le département Juridique ou les Ressources humaines.

IV – BONNE PRATIQUE N° 4 : UN DOUBLE REPORTING DU CCO AU DIRECTEUR GÉNÉRAL ET AU PRÉSIDENT DU COMITÉ D'AUDIT

Toutes les lignes directrices s'accordent sur ce point : un programme de *compliance* doit bénéficier du soutien de la direction au plus haut niveau et d'une capacité à remonter les problèmes identifiés de manière appropriée.

Certaines des entreprises interrogées ont expliqué les raisons de la création du département *compliance* et des modalités de rattachement. Nous avons noté que sa création avait bien souvent été demandée par le Conseil d'administration (ou équivalent), que le *Chief Compliance Officer* (CCO), s'il est rarement membre du Comité de direction, a, en général, une ligne directe vers le Directeur général du groupe, rapporte une ou deux fois par an au Conseil d'administration ou équivalent, et a également un accès direct, selon les cas, au Comité d'audit/des risques/éthique.

Dans nombre d'entreprises, toutefois, on observe une réticence à l'idée que le CCO puisse avoir une relation fonctionnelle avec le Président du Comité d'audit qui lui permet d'assurer son indépendance par rapport au Directeur général. Ainsi par exemple dans l'une des entreprises que nous avons rencontrée, la fonction *compliance* est exercée en « tandem » par deux personnes issues l'une de la direction des risques (qui rapporte *dotted line* au COMEX et au Comité d'audit), l'autre de la direction juridique, toutes deux rapportant *solid line* au Secrétaire général. Dans d'autres entreprises, la fonction est exercée directement par le Secrétaire général ou le Directeur juridique, sans être toujours individualisée dans l'organigramme. Dans d'autre cas encore, le CCO est rattaché à une direction multiple qui couvre la Direction des risques, le Contrôle Interne et l'Audit interne, ou rapporte au Directeur financier, avec la possibilité de saisir le Directeur général directement.

Le choix d'une des entreprises rencontrées exprime une particulière maturité. Son CCO explique qu'il a un double rattachement, en ligne directe avec le Directeur général ainsi qu'avec le Comité d'audit (double reporting, *solid line*, au Directeur général et au Président du Comité d'audit). Nous compre-

nons également que certains de ses objectifs, ainsi que son évaluation annuelle ne dépendent pas du Directeur général, ce qui permet au CCO, au-delà de la valeur symbolique du rattachement, d'apporter une vision et une approche indépendante par rapport au management de l'entreprise dans son ensemble. Ici, il s'agit de permettre au CCO de dire non, pour autant, bien sûr que sa position soit argumentée. Et dans ce groupe, ce principe est répliqué au niveau de chaque division : le *Complicance Officer* (CO) de division a un double rattachement *solid line*, au dirigeant de la division et au CCO du groupe. Cette pratique est intéressante dans la mesure où elle donne plus d'autorité au CCO et d'indépendance au CO qu'un modèle plus courant dans lequel le CO n'a qu'un rattachement matriciel (*dotted line*) par rapport au CCO. Le CCO, qui est à l'origine de cette organisation, nous explique qu'il a tout de même voulu conserver le rattachement au directeur de la division pour que l'organisation *compliance* ne soit pas isolée au sein de la division.

De manière plus générale, l'une des clefs de la réussite semble être la capacité du CCO et de son équipe à être consultés très en amont d'un certain nombre de projets ou décisions stratégiques ; qu'il s'agisse d'investissements dans un pays, de développement d'une solution technique/opérationnelle, d'une acquisition ou d'un partenariat. La participation des *Compliance Officers* aux comités concernés est essentielle.

En l'absence de rattachement ou de lien direct avec le Conseil d'administration ou équivalent et ou à l'un de ses comités, le rapport périodique du CCO à ce conseil ou comité prend une grande importance. Son contenu peut être variable, et les CCO devraient à notre avis utiliser la latitude dont ils disposent pour adopter une conception ambitieuse de ce rapport. « Je rapporte [au Conseil deux fois par an], explique l'un d'entre eux :

– sur ce qui marche bien
– sur les motifs d'inquiétude
– sur la stratégie de compliance »

Cette approche stratégique et cette dimension de rapport d'activité sont importantes. Elles n'excluent pas une synthèse sur les incidents majeurs et les cas d'alerte traités, mais se concentrent surtout sur les actions en matière de prévention (formations, procédures,…) et les résultats des tests d'efficacité du programme

Cependant, ce qui reste décisif, au-delà de la place du CCO dans l'organigramme, ce sont sa légitimité professionnelle et le soutien que lui accorde le management au plus haut niveau.

V – BONNE PRATIQUE N° 5 : LE PROGRAMME DE *COMPLIANCE* AU CŒUR DE LA POLITIQUE DE CENTRALISATION DE L'ENTREPRISE

Nos interlocuteurs ont presque tous fait le lien entre programme de *compliance* et centralisation de l'entreprise. Dans le contexte d'organisations décentrali-

sées et d'une diversité de métiers et de localisations, l'enjeu du contrôle par le groupe ne concerne pas que la *compliance*. Mais la nécessité de renforcer le système de *compliance* peut constituer une incitation supplémentaire à mettre en place une culture, des procédures ou un environnement informatique communs :

> Le programme de *compliance*, nous dit-on dans ce groupe très décentralisé, est aussi un moyen de renforcer de manière plus générale le contrôle sur la manière dont l'activité est exercée de par le monde.

Mais le responsable de ce groupe est avant tout pragmatique, soulignant l'importance du risque de standardisation face à la valeur apportée par la diversité et l'autonomie des différentes filiales ou divisions et le risque de « braquer toute l'organisation » par un programme insuffisamment « proportionné » et inadapté aux « différentes spécificités ».

Pour faire face à ce risque, le CCO du groupe a mis en place un réseau de quatre *Compliance Officers* (un par branche d'activité du groupe), qui ont ensuite nommé eux-mêmes un réseau dans leur branche. Les thèmes à couvrir par le programme de *compliance* ont été décidés en central et un contenu a été formalisé également en central. Mais les *Compliance Officers* des branches ont été chargés de signaler, lors de la conception du programme, les modalités d'aménagement nécessaires, tant sur les thèmes que sur le contenu. Par ailleurs, une fois les grandes lignes décidées, ils ont été chargés de la mise en place effective du programme en tenant compte des métiers et des modes d'organisation locaux. « On pense ainsi être en train de mettre en place un cadre programme adapté à chaque branche, mais dans un cadre homogénéisé. », nous dit le responsable *compliance* au niveau groupe.

Le risque de cette approche très respectueuse de la nature décentralisée de l'organisation est qu'une certaine résistance au changement et au contrôle se cache derrière l'invocation des « spécificités » du métier ou du pays et que le programme de *compliance* ne reste au final qu'à la surface des choses. Ainsi le CCO de cette autre entreprise, bien avancée dans le déploiement d'une organisation *compliance* dans les différentes divisions et géographies du groupe, identifie la résistance à la centralisation comme l'un des « enjeux de moment » pour l'organisation *compliance* :

> Il faut faire accepter que les choses se fassent de manière centralisée, alors qu'on est décentralisé par pays et par métiers. Il y a à ce sujet des luttes internes, des résistances, il y a une dimension "défense".

Dans cette autre entreprise, le CCO identifie dès le début de l'entretien l'unification de la culture d'entreprise comme l'un de ses principaux défis : « La culture d'entreprise est encore assez souple. Il est important de travailler sur le *tone at the top* et de faire le tour de toutes les entités (…) On a une apparence de centralisation, mais… ».

Il nous semble donc indispensable de faire avancer d'un même mouvement le programme de *compliance* et les sujets pour lesquels l'entreprise décide d'une

approche centralisée. Ainsi, par exemple, l'investissement important que représente l'unification de l'ERP au sein du groupe peut également permettre au dispositif de *compliance* de franchir une étape décisive. Mais cet investissement ne sera décidé qu'au regard du bénéfice qu'une telle unification représente pour l'ensemble des fonctions de contrôle du groupe.

Parfois la *compliance* joue dans la centralisation le rôle d'un véritable déclencheur. Il en va ainsi, par exemple, des entreprises qui ont mis en place, pour des raisons de *compliance*, un registre centralisé de leurs parties tierces (voir ci-dessous, bonne pratique n° 7). Le surcroît de visibilité que procure ce registre en central peut servir bien au-delà de la *compliance* pour contrôler toutes sortes d'autres risques tenant aux parties tierces. On peut alors véritablement parler d'une « centralisation par la *compliance* » : la *compliance* a contribué au changement de l'organisation dans son ensemble. C'est un succès pour la *compliance* et c'est un succès pour l'entreprise, à condition bien sûr, que cela ne nuise pas à la capacité d'innovation, à la culture du groupe… Tout réside dans l'habileté et le management du changement : éviter l'uniformisation tout en permettant une organisation constante, cohérente, fluide et homogène.

Certains interlocuteurs ont expliqué, dans cet esprit, comment leur programme de *compliance*, bien qu'il n'en soit qu'à ses débuts, était lié à une volonté de changement d'organisation de l'entreprise. Ainsi, dans ce groupe multinational historiquement très décentralisé, c'est un plan de réorganisation visant à redéfinir les modes de prise de décisions qui a fait émerger une fonction *compliance* exercée conjointement par la direction des risques et la direction juridique. Ce tandem s'est vu donner comme première feuille de route de remettre à plat toutes les normes internes du groupe pertinentes au regard du contrôle des risques, nous explique-t-on :

> « On veut créer un document avec un langage commun, une base documentaire accessible à tous. Ensuite, il s'agit de créer, pour chaque grand domaine, un corpus contenant dix règles d'or. Par exemple : comment achète-t-on dans notre entreprise ? Ce sera moins opérationnel que basé sur les valeurs. Les projets seront validés par le COMEX et déclinés dans les différentes divisions (…) C'est vraiment un projet d'entreprise que nous sommes en train de lancer ».

Par ailleurs, un outil de rationalisation tel que le recours à des centres de services partagés pourrait être optimisé en introduisant certains contrôles de détection des cas de non-*compliance*, ces centres gérant notamment les paiements, les relations avec les banques, un certain nombre de fonctions juridiques, fiscales et ressources humaines. La *compliance* n'a pas été, dans l'un des groupes interrogés, la raison première de la mise en place de ces centres de services partagés, mais la *compliance* en bénéficie néanmoins, par exemple à travers les contrôles qui peuvent être opérés systématiquement et de manière harmonisée au moment de la création des fournisseurs.

VI – BONNE PRATIQUE N° 6 : UNE CARTOGRAPHIE FINE DES RISQUES, ADAPTÉE AUX ENJEUX LOCAUX

L'analyse des risques est le point de départ permettant de dimensionner les efforts en matière de *compliance*. On ne dira sans doute jamais assez l'importance de l'analyse des risques et de combien de manières diverses elle devrait irriguer le programme de *compliance,* et plus généralement la vie de l'entreprise. Lors de la conception initiale du programme, c'est l'analyse des risques qui permet de définir les principaux domaines qui seront inclus dans le périmètre de l'organisation *compliance*. Périodiquement, les mises à jour de cette cartographie au regard des évolutions de la régulation ou des incidents observés dans l'entreprise permettront d'adapter le périmètre. C'est encore la cartographie des risques qui permettra au CCO de défendre son budget et de l'utiliser de la manière la plus effective. À un niveau plus « micro », une entreprise suffisamment mature en matière de *compliance* sera capable d'intégrer de manière opérationnelle des critères de « risque *compliance* » dans ses choix stratégiques et son modèle d'affaires, dans le cycle de vie de ses offres commerciales et projets, dans l'évaluation de ses cibles en matière de croissance externe, ou encore dans le choix et le suivi de ses partenaires, fournisseurs et autres parties tierces. Enfin, un bon programme d'audit est, lui aussi, nécessairement fondé sur une analyse des risques que présentent les diverses entités et géographies du groupe.

C'est en outre dans une assez large mesure la qualité de l'analyse des risques, et la rationalité des conséquences qui en sont tirées, qui donnent une chance, dans certains systèmes juridiques, à l'entreprise mise en cause sur le plan pénal de faire état de sa bonne foi et de faire la différence entre la responsabilité de l'entreprise et celle des individus mis en cause. En effet, seule l'utilisation argumentée de manière convaincante de la notion de risque peut permettre à l'entreprise de tenter de démontrer qu'elle a consacré à la prévention des moyens adéquats et qu'elle les a répartis de la manière la plus efficace possible.

Particulièrement difficiles à réaliser sur les risques de corruption, de fraude et de cybercriminalité, pour n'en citer que trois, ces cartographies doivent être assez fines pour permettre la mise en évidence des *scenarii* spécifiques et des moyens à développer pour prévenir et pour détecter les cas. Bien évidemment, cette analyse doit être effectuée tant au niveau « corporate » qu'au niveau des filiales.

Or, au fil de nos observations, nous constatons trop souvent que l'analyse des risques *compliance* reste limitée à une entrée unique de type « fraude et corruption » dans la matrice générale des risques de l'entreprise, ou à une simple entrée « éthique » dans une fiche d'évaluation des fournisseurs ou des projets.

Cependant, nous avons noté, au titre des bonnes pratiques, qu'un des groupes rencontrés avait développé une matrice mettant en évidence une vingtaine de schémas potentiels de corruption, pour laquelle était demandée aux filiales leur analyse des risques et des moyens de contrôles et de détection. L'objectif est double : d'une part, permettre à la filiale de mieux appréhender les risques majeurs qui la concernent sur ce domaine et renforcer ses moyens de prévention

et, d'autre part, au niveau du groupe, chercher à bâtir une vision « consolidée » afin de mieux évaluer le risque global. Dans cette entreprise, la remontée et la consolidation des informations au niveau groupe constituent ainsi un défi pour l'année en cours. Le CCO projette par ailleurs de transposer cette approche au risque sanctions/embargos.

C'est ce type de travail qui doit être au cœur des missions du département *compliance*. Son coût et sa difficulté ne doivent pas être sous-estimés : il suppose en effet une remontée régulière d'informations variées et de qualité suffisante. C'est à ce prix que l'outil d'évaluation des risques *compliance* peut asseoir sa crédibilité en interne et pousser l'entreprise dans son ensemble à prendre au sérieux les signaux qu'il produit. À défaut, l'analyse des risques pourrait devenir un simple exercice administratif et routinier.

VII – BONNE PRATIQUE N°7 : UN REGISTRE INFORMATIQUE DES PARTIES TIERCES

Si l'identification des risques pertinents est une priorité, le suivi et la documentation d'une telle approche le sont tout autant. Pour les zones de risques élevés, telles que par exemple celles qui sont liées à l'utilisation d'intermédiaires, une bonne pratique consiste à mettre en place un système de suivi et de documentation de l'analyse effectuée, qu'il s'agisse du processus de *due diligence* sur les tiers (*integrity check*) ou des différentes étapes de décisions internes de l'entreprise. La traçabilité de l'analyse, la conservation des documents qui permettent de justifier des décisions prises, dans leur contexte d'origine, sont clés.

Chacun a en tête, à cet égard, les recommandations générales concernant la gestion des parties tierces au regard du risque *compliance*. Ainsi, par exemple, de cet extrait de recommandations formulées en la matière par l'ICC : « Pour établir un protocole de *due diligence* qui soit à la fois complet, efficace et efficient, la première étape consiste à dresser un inventaire complet et précis des types de parties tierces (et des activités qu'elles mènent pour le compte de l'entreprise) et de leurs relations (avec des agents publics ou privés), à identifier leurs niveaux de risque, les signaux d'alerte et l'exposition de l'entreprise et, sur ces bases, à définir des degrés appropriés de vigilance ».[6]

Pourtant, on est surpris, à évoquer le sujet avec les divers responsables de la *compliance* rencontrés, du caractère souvent peu formalisé et peu centralisé des processus de catégorisation, d'analyse de risques et de contrôle des parties tierces. Le sujet reste très souvent traité au niveau des filiales par les commer-

6. ICC Guidelines on Agents, Intermediaries and Other Third Parties, ICC, 2010, p. 1 : « The first step in creating a due diligence protocol that is comprehensive as well as efficient and cost-effective is to create a complete and accurate inventory of the types of Third parties (and activities performed on behalf of the enterprise by such Third parties) and their relations (with public officials or private to private), to identify levels of risk, red flags and exposure for the enterprise and, finally, to define appropriate degrees of reviews. »

ciaux et opérationnels, sans procédure ni vision d'ensemble et sans véritable contrôle du département *compliance*. Beaucoup des entreprises interrogées admettent sans difficulté que leur entreprise a des progrès à faire de ce côté.

Exception notable, les entreprises qui ont recours à des agents commerciaux, consultants et autres intermédiaires sur une base régulière ont conscience du risque particulier que pose cette catégorie et tendent à centraliser au siège la signature de ces contrats et des autorisations de paiement correspondantes. À partir de là, on peut observer deux types d'évolutions. Certaines entreprises, ayant fait le bilan des coûts, risques et avantages de l'usage des agents et consultants, décident de cesser purement et simplement d'y avoir recours. Une nouvelle politique interne est alors rédigée, un plan de transition et des instruments de contrôle spécifiques sont mis en place. D'autres entreprises suivent une voie différente : ayant fait fonctionner pendant quelques temps un système strict, et jugé satisfaisant, de contrôle centralisé du risque *compliance* des agents, elles élargissent ensuite progressivement le champ d'application de ce système.

Illustrant cette deuxième approche, le responsable de la *compliance* de cette entreprise industrielle qui utilise un réseau d'intermédiaires à l'étranger nous explique que le département *compliance* est « risk owner » sur le risque de corruption posé par l'usage des intermédiaires et ceux-ci sont approuvés en central. Le projet du département *compliance* consiste aujourd'hui à élargir le périmètre de la notion d'intermédiaire à celle d'« associated person » au sens du UK Bribery Act[7] et à transposer progressivement des modes de contrôles initialement prévus pour les seuls agents aux sous-traitants, dont le niveau de risque *compliance* a été réévalué. Dans un premier temps, une catégorie intermédiaire a été mise en place, celle des « third parties at risk », qui va au-delà de celle des intermédiaires, pour inclure certains sous-traitants. Sur ces « third parties at risk », la *compliance* dispose aujourd'hui d'un droit de véto. À terme, l'objectif est que toute la *supply chain* puisse faire l'objet d'une approche cohérente en matière de *compliance*.

Une bonne pratique plus nette encore est observable dans une autre entreprise industrielle qui, ayant fait le choix de cesser d'avoir recours à des agents et consultants, a été conduite à mettre en place, sous l'égide de son département *compliance*, un registre informatique complet de l'ensemble de ses parties tierces, permettant de centraliser les informations et décisions relatives au niveau du risque *compliance*, des *due diligence*, aux approbations et au suivi de la relation. À l'origine de cette évolution se trouvait la nécessité de vérifier que les anciens agents et consultants ne cherchaient pas à contourner l'interdiction en se faisant réemployer par ailleurs en capacité, par exemple, de distributeurs ou de fournisseurs. L'entreprise devait donc mettre en place un outil commun lui permettant de contrôler de manière harmonisée et rigoureuse la totalité de

7. La « personne associée » (*associated person*) est, aux termes de l'article 8 du UK Bribery Act de 2010, toute personne qui effectue des services pour l'entreprise ou pour son compte. Dans certaines conditions, les actes de corruption active d'une personne associée peuvent entraîner la responsabilité pénale au regard du UK Bribery Act de l'entreprise donneuse d'ordres.

ses parties tierces alors même que, selon leur typologie, elles étaient gérées de manière distincte dans l'entreprise. En particulier, un effort important a été fait dans ce cadre pour soumettre plusieurs dizaines de milliers de fournisseurs à des procédures *compliance* communes à toutes les parties tierces de l'entreprise et inclure ces fournisseurs dans le registre informatique commun. Le département *procurement* s'est pour ce faire doté d'une sous-division chargée spécifiquement de faire le lien entre les procédures « procurement » et les procédures « compliance ».

On le voit, ces deux expériences supposent un investissement significatif. Mais, celui-ci une fois réalisé, l'entreprise fait un véritable saut qualitatif : elle dispose d'un outil de contrôle unique de ses relations avec toutes ses parties tierces, outil auquel elle peut progressivement ajouter des fonctionnalités, au-delà même du champ de la *compliance*.

VIII – BONNE PRATIQUE N°8 : UN OUTIL D'AUTO-ÉVALUATION DES PRATIQUES

La formation est centrale, dans tout programme de *compliance*. Elle constitue l'une des transitions indispensables entre l'énoncé des valeurs et procédures, d'une part, et les différentes formes de contrôle et de sanction, d'autre part. Elle est cependant très consommatrice en temps, surtout pour les entreprises dispersées sur le plan géographique, et tend de plus en plus à prendre la forme d'un *e-learning* qui, entre autres avantages, présente celui d'une parfaite traçabilité. Au risque toutefois de ne pas marquer les esprits autant qu'une formation traditionnelle et de ne pas ouvrir la possibilité d'un véritable dialogue.

C'est pourquoi une expérience liant *e-learning* et auto-évaluation nous a semblé innovante et susceptible d'être relevée au titre des bonnes pratiques. Dans ce groupe où coexistent une direction éthique et une direction de la *compliance*, cette dernière concentre son effort sur l'opérationnalisation des principes de la charte éthique. « Nous voulons donner des outils opérationnels, pragmatiques, des aides, pour passer de l'énoncé de la loi en général à la mise en pratique », nous explique le responsable de la *compliance*. L'approche de la *compliance*, ainsi définie, est distinguée de celle de l'audit par son caractère « amical », et donc essentiellement pédagogique : « Notre discours c'est : " ne mettez pas les pieds là, vous allez vous faire mal " ».

Un travail assez classique, mais indispensable, a d'abord été fait par l'entreprise sur la documentation, avec une déclinaison et explication des valeurs et procédures de l'entreprise en fiches et documents accessibles et attractifs, par thèmes et par fonctions.

Une réalisation plus originale est par ailleurs en cours : mettre à la disposition des responsables sur le terrain un outil d'auto-évaluation. L'outil a été conçu en concertation avec le département de l'audit interne mais n'est pas un instrument d'audit. Il sera disponible en ligne et permettra, par l'auto-évaluation, de réviser les fondamentaux du programme de *compliance*. Le développement de

cet outil est décrit par le CCO comme l'un des 5 grands axes du programme de conformité. Cela pourra devenir, à notre avis, une forme originale d'*e-learning*, qui ne sera pas un simple exposé abstrait couplé à un test en ligne, mais un outil partant de l'expérience.

Si cette forme d'auto-évaluation présente l'avantage de dynamiser l'*e-learning*, elle n'est pas cependant sans une certaine ambiguïté, d'ailleurs bien perçue par nos interlocuteurs : les utilisateurs ne doivent pas percevoir l'auto-évaluation comme une « porte vers l'audit », sinon ils risquent de ne pas jouer le jeu de l'auto-évaluation et de se contenter de réponses de type « tick the box ». Mais, parallèlement, les responsables de la *compliance* ne pourront pas ignorer des signaux d'alerte résultant des réponses données dans le cadre de l'auto-évaluation.

IX – BONNE PRATIQUE N°9 : TESTER L'EFFICACITÉ DU DISPOSITIF DE *COMPLIANCE*

Lorsqu'un dispositif de *compliance* est jeune, la mesure de sa robustesse est rarement testée, notamment si les différentes procédures n'ont pas encore été totalement déployées. C'est le cas pour de nombreuses entreprises rencontrées, d'autant que les différentes initiatives en matière de *compliance* ont des niveaux de maturité différents (anti-concurrence, anti-corruption, sanctions, etc.).

Il est essentiel, au fur et à mesure du déploiement d'un dispositif de *compliance*, d'en tester d'une part la robustesse, et d'autre part l'efficacité par rapport au risque concerné. L'objectif est double :

- améliorer en permanence le dispositif en tenant compte des difficultés rencontrées sur le terrain et des nouveaux enjeux (investissements dans des pays émergents, nouveaux partenariats stratégiques….) ;
- démontrer la pertinence du dispositif.

En effet, le contrôle d'un programme de *compliance* constitue un axe de défense majeur pour l'entreprise en cas de poursuites par des autorités. Il lui permet de démontrer qu'elle a mis en place des moyens proportionnés aux risques identifiés et, qu'en cas d'incident, celui-ci est isolé. C'est ce *monitoring* qui peut permettre de distinguer les mesures efficaces des simples effets d'annonce ou d'habillage.

Lorsque des points faibles sont identifiés, il s'agit d'y remédier rapidement et de comprendre pourquoi, localement, cette procédure n'a pas été respectée. Il peut, en effet, s'agir d'un problème d'ordre culturel ou opérationnel rendant la procédure inadéquate (procédure jugée trop complexe ou trop contraignante par exemple) ou, tout simplement, d'une insuffisance de formation des équipes. Cela permet également de mettre sous contrôle les zones de risques les plus élevés. Ces tests peuvent être notamment réalisés par le département *compliance* ou l'audit interne. Dans ce cas, ils sont souvent ponctuels, rétroactifs et intégrés dans les procédures, lors de l'audit d'une filiale par exemple.

Cependant, ces véritables audits se différencient de ce l'on appelle le pilotage du dispositif de *compliance* (*monitoring*) que l'on peut observer dans des groupes plus matures. En effet, ce pilotage a pour objectif de mettre en place des indicateurs récurrents et fréquents pour détecter rapidement les principales opérations ou situations à risque.

Prenons comme exemple concret le risque de paiement d'un agent dans un autre pays que celui dans lequel il effectue sa prestation. Lors de la visite d'une filiale, l'audit peut se charger de vérifier que les agents ont bien été payés dans le pays prévu. Ce contrôle peut être effectué rétroactivement sur plusieurs années. Dans ce cas de figure, le pilotage consisterait à mettre en place et à surveiller, par exemple à l'aide d'un indicateur, tous les paiements d'agents réalisés dans un autre pays que leur lieu d'immatriculation, le lieu d'exécution du contrat, entre autres, et de réagir rapidement lors de la survenance d'une opération de ce type pour vérifier qu'elle est dûment justifiée.

L'analyse de données est cruciale pour la création d'un tel système d'indicateurs. Encore faut-il que l'entreprise ait développé des *scenarii* en réponse aux risques identifiés dans la cartographie afin de pouvoir détecter rapidement les transactions atypiques. La bonne pratique consiste donc à ce que, sur la base des risques identifiés lors de la préparation d'une cartographie fine, l'entreprise définisse et teste des *scenarii* de risques. L'objectif est de vérifier qu'aucune transaction anormale ne s'est produite. Pour cela, l'entreprise peut analyser simultanément les données au sein de plusieurs pays, dans différentes filiales, afin de détecter les transactions qui pourraient présenter un risque de non-conformité important. L'analyse de données rassure aussi en l'absence d'anomalies révélées.

Cette approche va donc bien au-delà d'un simple dispositif préventif, consistant à mettre en place des procédures pour éviter la survenance d'un cas.

X – BONNE PRATIQUE N°10 : UN DISPOSITIF DE RÉPONSE AUX ALERTES ET DE GESTION DES INVESTIGATIONS INTERNES

La mise en place d'une ligne d'alerte éthique est une bonne pratique et un bon nombre d'entreprises interrogées disposent d'une telle ligne. Elle permet en principe à tous de signaler des comportements déviants, tout en bénéficiant d'un cadre confidentiel approprié pour la protection de l'anonymat protégeant les lanceurs d'alerte.

Cependant, les CCO rencontrés ont mentionné de façon générale le peu de cas remontés par ce canal. Ils n'expliquent pas totalement cette situation. Un phénomène culturel propre à la France pourrait jouer sa part ainsi que le manque de communication, en interne, sur l'existence de la ligne d'alerte. La réticence des collaborateurs à utiliser la ligne d'alerte pourrait aussi provenir d'un sentiment d'insuffisance de protection de l'anonymat des lanceurs d'alerte. Un travail de communication paraît encore nécessaire, tant pour rassurer que pour promouvoir l'existence et l'utilité de cette ligne d'alerte.

Il doit également être noté que de nombreuses alertes ne remontent pas par le canal de la ligne d'alerte mais proviennent de sources très différentes : salariés utilisant différents canaux internes, fournisseurs, clients, etc. Le temps où ces alertes étaient disqualifiées sans analyse est révolu. Pour autant, toutes ne sont pas fondées et nombre d'entre elles manquent de sérieux.

Pour le savoir, une analyse et un triage de ces alertes est nécessaire afin de décider de manière documentée si elles nécessitent une investigation interne.

Ce triage comprend la prise de connaissance des faits allégués et la vérification sommaire de la vraisemblance des éléments qui y sont portés, incluant notamment la recherche de conflits d'intérêts éventuels (au travers d'une *due diligence* intégrité, notamment).

Si la vraisemblance est confirmée et le niveau de gravité suffisant, une investigation interne peut être conduite. Celle-ci a pour objectif de rechercher et documenter des faits qui confirment ou infirment l'allégation. Pour cela, les méthodes utilisées sont variées, de l'analyse des flux comptables et financiers à la revue des emails en passant par des entretiens et la compréhension des processus… Cette approche structurée, dite « forensic », doit être adaptée à chaque situation. Elle doit s'inscrire dans un cadre précis et respecter les lois et réglementations en vigueur dans chacun des pays où elle est effectuée. En ce sens, une bonne pratique relevée consiste à élaborer une charte d'investigation permettant de s'assurer que les principes clés d'intégrité, d'objectivité, d'impartialité, de confidentialité, de proportionnalité, de respect de la vie privée sont bien compris.

Les organisations rencontrées ont d'ailleurs mentionné un certain nombre d'écueils lors de la conduite des investigations. Parmi ceux-ci figurent notamment la protection insuffisante du lanceur d'alerte, de la réputation de la (ou des) personne(s) mise(s) en cause, le non-respect des lois et des réglementations en matière de données personnelles, la non-préservation des preuves, etc. Il incombe à l'organisation d'identifier ces difficultés en amont et de mettre en place les mesures concrètes pour y pallier.

Que les investigations soient menées en interne ou externalisées auprès d'un prestataire, celles-ci doivent être pilotées avec rigueur. La *Compliance*, l'Audit interne, le Juridique ou d'autres départements peuvent y contribuer. À ce titre, il convient de mentionner l'émergence d'une nouvelle fonction, celle de responsable d'investigation. Mais parmi les entreprises rencontrées, encore peu d'entre elles ont une équipe spécialisée en interne (*forensic auditors*).

*
* *

Que retenir de cette étude sur les bonnes pratiques de *compliance* dans les entreprises françaises ? Elle révèle tout d'abord une tendance, celle d'entreprises en mouvement : des entreprises qui ont, en grande majorité, pris le virage de la *compliance* et qui, sans renoncer à une approche en termes d'éthique ou de responsabilité sociale, voire sociétale, adoptent progressivement une démarche

fondée sur la formalisation croissante des règles et processus internes et une politique de prévention du risque juridique dans son ensemble. Aujourd'hui, en matière de *compliance*, les entreprises françaises sont à l'écoute et nombreuses à développer des solutions innovantes pour mettre à jour leurs divers organigrammes (au niveau *corporate* ou à celui des filiales, etc.) apprécier leurs risques, harmoniser leurs procédures et y former leurs équipes.

L'obligation de prévention de la corruption dans les entreprises introduite en droit français par la loi Sapin II de lutte contre la corruption, interviendra en terrain favorable et devrait permettre d'accélérer un mouvement déjà bien engagé.

L'image est plus nuancée en ce qui concerne la mise en œuvre des programmes de *compliance*, et leur robustesse. La présente étude n'a pas permis de savoir si les moyens dont dispose le département *compliance* sont correctement dimensionnés par rapport aux missions qui lui sont assignées. Pour ce faire, il serait utile que de futures recherches soient menées, permettant ainsi de fournir aux entreprises un référentiel commun en matière de périmètre et de moyens des départements *compliance*. Par ailleurs, la mise en œuvre au sein de l'entreprise de moyens de détection et d'investigation des cas de non-*compliance* soupçonnés ou confirmés est aussi primordiale que les initiatives en matière de prévention. Et les efforts investis dans les actions de prévention ne se substituent pas à ceux qui doivent être dédiés aux moyens dits de « réaction ». Cela est d'autant plus vrai que les risques et cas de *non-compliance*, en particulier la fraude et la corruption, ne sont pas toujours simples à identifier, l'entreprise pouvant mettre jusqu'à 18 mois avant de s'apercevoir des faits. Elle peut d'ailleurs ne pas s'en apercevoir du tout. En particulier, il peut s'avérer particulièrement compliqué d'identifier l'origine des faits et de mesurer les impacts exacts – financiers et opérationnels – pour l'entreprise. Cette étape est cependant obligatoire pour mettre en place les actions de remédiation sur le court, moyen et long terme. Maîtriser les risques est l'affaire de tous, c'est bien pour cela que la collaboration entre les différents départements est nécessaire, voire indispensable, et constitue de ce fait une bonne pratique.

Plus généralement, apparaissent notamment au terme de cette étude des axes de progrès : la maîtrise effective du risque lié aux parties tierces, l'audit de l'efficacité du programme ou la gestion rigoureuse de la *hotline* et des investigations. Autant de questions cruciales pour apprécier la crédibilité d'un programme de *compliance*.

Développer une réelle culture de la *compliance* commune au sein de l'entreprise n'est pas une tâche facile. Il s'agit désormais d'accompagner l'entreprise dans un changement profond des mentalités et des principes d'actions. Le *Compliance Officer*, seul, ne peut y parvenir et l'un des chantiers d'envergure, avec le soutien de l'ensemble de la direction, sera de montrer aux différents acteurs de l'entreprise qu'il s'agit d'une démarche commune dont il est l'un des principaux coordinateurs. La force de la *compliance* réside avant tout dans sa capacité à convaincre les opérationnels qu'ils en sont les premiers acteurs pour assurer le développement pérenne de l'entreprise.