TABLE RONDE

Gestion des risques & Compliance

Dans les locaux de Linklaters LLP **Le 01 Mars 2018**

La compliance, une stratégie de gestion des risques transformante pour les entreprises

Soumises à un feu interrompu de réglementations reflétant les nouvelles préoccupations sociétales, les entreprises se sont lancées dans des démarches de mise en conformité répondant au concept protéiforme de ''compliance''. Mais la mise en œuvre de cette stratégie de gestion des risques n'est pas sans conséquences pour leurs activités opérationnelles, comme en ont brillamment débattu les experts réunis par le Magazine des Affaires.

Photographie : Philippe Castano

Xavier Leloup, Le Magazine des Affaires : J'aimerais qu'on essaie de délimiter, à supposer que ça puisse l'être, le concept de compliance. Je me suis aperçu — vous devez le savoir encore mieux que moi —, que lorsque vous parlez à des gens qui ne sont pas de cette filière, la première question qu'ils posent, c'est : « la compliance, c'est quoi ? » On ne sait pas très bien ce que ça recouvre. Est-ce que c'est juste un autre mot savant pour parler de «réglementation » ?

Pierre-Antoine Badoz, Orange : Pour moi, la compliance c'est plus que cela. C'est une démarche, qui est encore assez récente en France, et qui consiste à déployer un programme, c'est-à-dire d'un ensemble d'actions, de procédures et de contrôles, afin de s'assurer que l'entreprise va se conformer dans sa globalité, c'est-à-dire dans l'ensemble de ses métiers, dans tous les pays où elle est présente et dans tous ses processus, à un certain nombre de lois et de règlements. Cela permet aussi à l'entreprise de démontrer qu'elle a mis en œuvre le programme adéquat qui assure cette conformité.

Xavier Leloup, le Magazine des Affaires : C'est une démarche pour montrer qu'à priori l'entreprise fait tous les efforts nécessaires pour se conformer à… ?

Pierre-Antoine Badoz, Orange : Oui, à des lois, à des règlements, avec des périmètres qui peuvent varier, parce que ce n'est bien évidemment pas l'ensemble des lois et des règlements qui sont inclus dans cette démarche dans la mesure où celle-ci est relativement lourde à déployer puisqu'elle doit l'être dans l'ensemble de l'entreprise.

Xavier Leloup, le Magazine des Affaires : Surtout pour des entreprises internationales.

Eléonore Hannezo

➤ Avocate chez Linklaters LLP, au sein de l'équipe Dispute Resolution.

➤ Eléonore est spécialisée en droit pénal des affaires, en contentieux financiers et en compliance. Elle intervient notamment dans le cadre de litiges post-M&A ou encore dans des procédures devant les autorités de régulation françaises telles que l'Autorité des marchés financiers (AMF) et l'Autorité de contrôle prudentiel et de résolution (ACPR). Elle a par ailleurs été co-auteur du Rapport sur l'avenir de la profession d'avocat remis au Ministre de la Justice, Garde des Sceaux, en 2017.

➤ À Paris, Linklaters LLP a réuni, au sein d'une équipe pluridisciplinaire, une dizaine d'avocats aux expertises complémentaires afin de répondre aux besoins de ses clients français et étrangers en matière de compliance. Cette équipe intervient aussi bien au stade de l'élaboration et de l'actualisation des programmes de compliance que dans le traitement des non-conformités devant les autorités administratives et judiciaires compétentes.

Pierre-Antoine Badoz, Orange : Oui, pour les entreprises internationales mais cela concerne maintenant aussi les entreprises de taille intermédiaire. Le champ de la compliance couvre généralement la prévention de la corruption, le respect des programmes de sanctions économiques internationales (les embargos), et parfois le respect du droit de la concurrence.

Xavier Leloup, le Magazine des Affaires : Il me semble, Catherine, que vous englobez la concurrence. C'est dans votre périmètre, mais pas chez Orange, n'est-ce pas ?

Catherine Delhaye, Valeo : Oui, le périmètre chez Valeo recouvre l'anti-trust — *anti-bribery* —, *export control and economic sanctions*, bientôt RGPD, donc *data privacy*. Avec la loi Sapin, voire la loi sur le devoir de vigilance, la compliance s'impose en France, et rend la démarche dont parlait Pierre-Antoine incontournable dans de nombreux domaines désormais. La compliance est en fait une démarche.

> ''A travers la conformité, l'entreprise est placée dans quelque chose de schizophrène : elle est à la fois la police et en même temps elle est potentiellement l'auteur, par le fait de ses dirigeants, voire ses employés''
>
> *Eléonore Hannezo*

C'est une méthodologie, une technique de gestion des risques. L'entreprise choisit le ou les risques qu'elle veut spécifiquement mettre sous contrôle. En effet, les risques varient en fonction des métiers. Les entreprises nucléaires ou pharmaceutiques ne traiteront pas le risque de la même façon qu'une entreprise comme Orange ou comme Valeo. Donc elle identifie son risque et l'adresse par anticipation selon la méthodologie décrite par Pierre-Antoine. Chacun a sa définition mais pour moi, c'est une technique de gestion des risques. C'est une nouvelle approche de management du risque juridique.

Jean-Jacques Quang, Duff & Phelps : Je peux voir une distinction entre la conformité et compliance : la conformité, c'est se conformer à toutes les réglementations qui existent, françaises et internationales. Dans la compliance, il y a une notion très

anglo-saxonne ou américaine, qui va un peu au-delà. On a l'ambition de faire vivre toutes les valeurs de l'entreprise, pas uniquement de se conformer à la réglementation, mais faire en sorte qu'en interne, l'ensemble du personnel y adhère, les vive au quotidien et fasse en sorte d'être proactif vis-à-vis de ces réglementations, et qu'on ne soit pas uniquement garant de la conformité.

Xavier Leloup, le Magazine des Affaires : Cela veut-il dire aussi qu'une entreprise peut être plus stricte sur certains points que ne l'impose la législation ?

Jean-Jacques Quang, Duff & Phelps : Elle peut être plus stricte, mais surtout bien faire comprendre l'intérêt des valeurs, de l'éthique : valeurs morales, valeurs de l'entreprise, qu'elles soient effectivement vécues par tout un chacun et pas uniquement avec un aspect contrainte. Les Américains appellent ça *live the value*. C'est cette notion que j'ai pu rencontrer dans de nombreux groupes anglo-saxons à travers le monde.

Xavier Leloup, le Magazine des Affaires : Les juristes que vous êtes ?

Valentin Autret, Skadden Arps : S'obliger à respecter les différentes règles qui s'appliquent à son activité et celles que l'on se fixe n'est pas nouveau. La nouveauté de la compliance serait plus la méthode que l'on emploie pour y parvenir et prévenir une éventuelle défaillance. C'est aussi un excellent moyen de se préparer aux contentieux qui naîtraient d'une défaillance. La création ou le renforcement de la fonction ou de l'organe en charge de la compliance dans l'entreprise apporte en effet beaucoup à son éventuelle défense. Le responsable de la conformité, s'il est impliqué dans la prise de décision grâce au lien qu'il représente entre les juristes et les opérationnels, entre la contrainte juridique et les objectifs business, permet la constitution d'un dossier démontrant que les décisions ont été prises en encadrant raisonnablement des risques identifiés. Avec les contraintes qui s'accumulent (loi Sapin II, loi sur le devoir de vigilance, le RGDP), le quantum des sanctions qui grimpent et la judiciarisation des activités de l'entreprise, l'attelage entre le responsable de la conformité et l'avocat contentieux devrait devenir central.

Xavier Leloup, le Magazine des Affaires : On a l'impression que le champ réglementaire des obligations qui pèsent sur les entreprises, notamment pour les plus grandes d'entre elles, a été démultiplié en l'espace de deux, trois ans. On a un devoir de vigilance qui est différent encore de la fameuse loi Sapin II dont on a beaucoup parlé sur les pratiques de corruption. Ce sont deux législations complémentaires, mais distinctes. Il y a le RGDP dont on va parler sur la gestion des données personnelles. Tout d'un coup, il y a comme une accélération de l'histoire pour les entreprises.

Eléonore Hannezo, Linklaters : La compliance est un concept protéiforme, une "auberge espagnole" selon le Professeur Frison-Roche. Le terme est assez bon parce qu'il est vrai que la compliance recouvre énormément de concepts distincts. Je pense que pour bien comprendre la notion, il faut distinguer la compliance volontaire de la compliance subie et conserver à l'esprit qu'il y a plusieurs degrés d'exigence dans la compliance subie. Ainsi, la compliance peut être volontaire et mise en place par une entreprise dans un souci d'éthique ou en guise de moyen de défense : elle pourra utiliser son programme de compliance pour dire qu'elle a pris toutes les mesures pour s'organiser et prévenir le risque à l'avenir. La compliance peut aussi être imposée, mais imposée sous des formes différentes. La compliance dans sa version la plus légère, c'est le fait de simplement obliger l'entreprise à décrire les procédures de conformité qu'elle a mises en oeuvre, et ça, c'est par exemple l'obligation de reporting extra-financier, devant figurer dans le rapport de gestion. On explique comment la société prend en compte les conséquences sociales et environnementales de son activité. Ça, c'est la compliance imposée dans sa version la plus légère. Après, il y a une obligation de mettre en place un certain nombre de procédures, avec le risque d'engager seulement sa responsabilité civile. C'est le devoir issu de la Loi de vigilance. Et dans la version la plus exigeante, la plus dure de la compliance, il y a des obligations de mettre en place des programmes

Jean-Jacques Quang

- Director, Duff & Phelps
- Au sein de Duff & Phelps, Jean-Jacques fait partie de l'équipe européenne d'experts en Disputes & Investigations et Compliance & Regulatory Consulting, en charge des solutions anti-corruption et anti-fraude.
- Jean-Jacques est un investigateur expérimenté dans la lutte contre la corruption et la fraude, avec plus de 20 ans d'expérience conjuguant responsabilité opérationnelle en industries et conseil en risk management, contrôle interne et dispositif anti-corruption.
- Avant de rejoindre Duff & Phelps, Jean-Jacques était Directeur Fraude & Corporate Investigations chez CMA-CGM, couvrant les sujets de fraude interne, collusion, corruption. Auparavant, Jean-Jacques a démarré sa carrière en Asie, à des fonctions de Direction Financière puis Audit Interne pour plusieurs industries. De retour en France, Jean-Jacques a développé l'activité Business Risk Services chez Grant Thornton, avant de se spécialiser dans la lutte anti-fraude.
- Jean-Jacques est titulaire d'un Master en Management et possède la certification « Certified Fraud Examiner - CFE ».

aux contours très délimités par le législateur et le pouvoir règlementaire, avec un contrôle des autorités qui vont regarder les diligences qui ont été mises en place par l'entreprise, et là, je cite encore le Professeur Frison-Roche parce que ses travaux sur la compliance sont vraiment très intéressants.

Xavier Leloup, le Magazine des Affaires : Et qui vient de sortir un livre avec vous.

Eléonore Hannezo, Linklaters : Oui, avec Arnaud de La Cotardière. Elle a des mots très forts : l'entreprise devient un "agent de la légalité", participant à "un service public mondial" pendant que les autorités, les régulateurs, sont "des spectateurs des diligences mondiales" mises en place par l'entreprise. Il y a une sorte de transfert de pouvoir régalien de l'Etat vers l'entreprise,

> "Dans les acquisitions, l'exposition en matière de pratiques non-conformes n'est pas forcément prise en compte dans la valeur de l'entreprise et peut avoir des répercussions dramatiques. Donc il faut pouvoir aborder les due diligences sur les aspects compliance"
>
> *Jean-Jacques Quang*

compte tenu des difficultés pour l'Etat d'exécuter son pouvoir de police dans un monde sans frontières.

Xavier Leloup, le Magazine des Affaires : C'est le mot, « police ». Quand on voit les règlements internes, il va y avoir des sanctions. On est presque dans un pouvoir de police interne ?

Eléonore Hannezo, Linklaters : Mais l'entreprise est placée à travers la conformité dans quelque chose de schizophrène : elle est à la police en même temps que d'être potentiellement l'auteur, par le fait de ses dirigeants, voire de ses employés. Et de ce point de vue, la compliance peut l'amener, j'ai vu que vous aviez rajouté une question là-dessus, on pourra en parler, à se dénoncer

Xavier Leloup, le Magazine des Affaires : Le sentiment dans les entreprises aujourd'hui est-il de se demander ce qui va prochainement leur arriver ? Car finalement, tout cela est-il sous contrôle ?

Catherine Delhaye, Valeo : J'ai le sentiment que les choses évoluent très vite. Il y a sept ans, quand on parlait de *compliance*, le concept paraissait exotique. Effectivement, on arrivait avec une nouvelle méthodologie, totalement inconnue, qui passait par des procédures, par des formations, par des formulaires, par la documentation des actions, par la preuve, la justification. Pourtant, il s'agissait simplement de mettre en place, pour des raisons juridiques, des méthodes nouvelles pour les Directions juridiques mais que les départements Qualité avaient implémentées depuis des années. C'était la qualité appliquée au droit. Et comme vous le disiez, il y avait déjà des domaines réglementés, la banque, la pharmacie, l'assurance, qui ne pouvaient pas échapper à la conformité, c'est-à-dire à des obligations réglementaires extrêmement strictes. La *compliance* dont nous commencions à parler s'entendait en l'occurrence d'une démarche volontaire adoptée par des entreprises désireuses de se protéger d'un certain nombre de risques, par la mise en oeuvre d'un cadre établi. On sait très bien ce qu'est la *compliance*. C'est une méthodologie qui s'appuie sur six, sept ou huit piliers en fonction des lois. Dans la loi Sapin, on a huit piliers. Les Américains ont parlé pendant des années des *seven standards*, qui regroupent à peu près tous, ces mêmes étapes, cette même démarche. Aujourd'hui, ce qui est nouveau et différent, c'est que le règlement sur la protection des données nominatives, comme la loi Sapin, comme d'une certaine façon la loi sur le devoir de vigilance, imposent aux entreprises ce cadre. Non seulement on est comptable des manquements, des violations de la loi, mais on est également comptable de ne pas avoir mis en place des systèmes de prévention. Les entreprises comprennent rapidement que ça peut être extrêmement vertueux. L'éducation, la formation, la sensibilisation et le fait d'avoir un cadre précis qui permet aux gens de savoir où se positionner, comment agir, est très réconfortant. Bien sûr, il faut du *change management*. Et le *compliance officer* est avant tout un *change manager*, quelqu'un capable d'accompagner le choc, l'électrochoc, et la conduite du changement. Mais passée la phase d'adaptation, les entreprises comme les collaborateurs s'y retrouvent…

Xavier Leloup, le Magazine des Affaires : Avant d'arriver à la distinction entre directeur juridique et directeur de la conformité, j'aimerais m'arrêter un instant sur une initiative d'Orange. Il me semble que vous êtes à l'origine du droit de "débrancher". C'est une politique propre à votre entreprise, c'est-à-dire que les salariés ont le droit de se déconnecter, le droit à la déconnexion.

Pierre-Antoine Badoz, Orange : Effectivement, notre précédent DRH a été l'auteur d'un rapport passionnant sur la transformation numérique et son impact sur la vie au travail qui comprend différentes propositions, dont le fameux droit à la déconnexion.

Xavier Leloup, le Magazine des Affaires : Qui a été mis en œuvre chez Orange. Je me souviens qu'aux États-Unis, ils avaient trouvé cela très étrange. C'était intéressant à observer, parce qu'eux comme nous d'ailleurs sont complètement connectés. D'autres entreprises pourraient s'en inspirer. Vous êtes quasiment à l'origine d'un nouveau droit.

Pierre-Antoine Badoz, Orange : Un nouveau droit, peut-être pas, mais je pense que la réflexion sur l'impact du digital dans le travail et sur la façon dont on met en musique, justement, l'interaction entre la dimension professionnelle et la dimension personnelle afin que l'ensemble des salariés bénéficie d'une vie qui reste équilibrée, c'est un vrai sujet : d'ailleurs, nous le vivons tous à titre personnel. Il est donc important de fixer quelques règles qui pour le moment relèvent encore de la *soft law*.

Xavier Leloup, le Magazine des Affaires : On pourrait tout de même imaginer que fort de votre pratique le législateur mette sur pied une réglementation allant dans ce sens.

"Avec la transformation digitale, toutes les activités de base peuvent conduire à vérifier le critère de surveillance systématique et à grande échelle des individus, rendant ainsi le Délégué à la Protection des Données obligatoire"

Denise Lebeau-Marianna

Pierre-Antoine Badoz, Orange : L'avenir nous le dira.

Xavier Leloup, le Magazine des Affaires : Quelle est la différence entre directeur juridique et directeur de la conformité ? On parlait de police, je crois que le directeur de la conformité doit être indépendant de manière à pouvoir le cas échéant dénoncer une pratique. Peut-on délimiter les champs juridique et compliance à l'intérieur de l'entreprise ?

Pierre-Antoine Badoz, Orange : Effectivement, comme l'a bien expliqué Catherine, la compliance est un sujet de changement dans l'entreprise, de nouvelles procédures à mettre en œuvre et donc, le choix qui a été fait chez Orange, c'est d'avoir quelqu'un qui vient de l'opérationnel et qui connaît bien les différents métiers de l'entreprise. Je suis pour ma

Denise Lebeau-Marianna

- Associée de DLA Piper
- Denise Lebeau-Marianna assiste ses clients en matière de données personnelle dans la mise en œuvre de projets globaux de mise en conformité à la règlementation et mise en place d'une structure de gouvernance ainsi que sur des projets de traitements plus spécifiques tels que ceux mis en œuvre aux fins de lutte contre la corruption, le blanchiment et la lutte contre le financement du terrorisme ou encore les traitements de lutte contre la fraude aux paiements, lutte contre la contrefaçon ou les procédures de e-discovery.
- Elle conseille également ses clients dans le domaine des données de santé et les projets de télémédecine en relation avec les autorités (CNIL, ASIP).
- Denise dispose d'une solide expérience en Droit des Nouvelles Technologies : Droit de l'Informatique, de l'Internet, du E-commerce, et la réglementation des données personnelles dont elle traite les aspects contentieux et non contentieux. Elle est expert agréé EuroPriSe en données personnelles et certifiée CIPP/E.

part ingénieur de formation et mon enjeu c'est de transformer la manière d'agir de l'entreprise, afin que, dans nos processus et dans notre activité, le management du risque de corruption et de sanction économique, soit effectivement pris en compte et le plus en amont possible.

Xavier Leloup, le Magazine des Affaires : Ça veut dire que vous avez un lien ? N'étant pas directeur juridique, entretenez-vous un lien hiérarchique classique vis-à-vis de votre directeur général ? Ou vous êtes un électron libre ?

Pierre-Antoine Badoz, Orange : Non, je ne suis pas un électron libre.

Xavier Leloup, le Magazine des Affaires : Est-ce que vous passez dans les bureaux en disant : « non, ce n'est pas bien », avec votre règle ?

Pierre-Antoine Badoz, Orange : Je n'ai pas de pouvoir hiérarchique sur les patrons opérationnels et mon rôle est un mélange de pédagogie, de persuasion et d'incitations, diverses, au respect des règles et de la loi. Cela passe par le déploiement de notre programme de compliance, de différentes actions dans l'ensemble de nos activités, en France mais également à l'étranger, dans les activités opérationnelles comme dans les activités stratégiques, par exemple dans le M&A. C'est un enjeu majeur, quand vous rachetez une entreprise, vous rachetez potentiellement ses manquements à l'éthique passés. C'est d'ailleurs quelque chose qui aurait pu impacter directement Orange car en 2008, nous avons failli racheter Telia, l'opérateur historique suédois. Et en septembre 2017, Telia a été condamné à près d'un milliard de dollars d'amende pour corruption ! Or le schéma de corruption avait été mis en place à partir de 2007, donc avant notre tentative de rachat qui, heureusement, ne s'était pas concrétisée.

Xavier Leloup, le Magazine des Affaires : C'était un cauchemar pour vous, en tant que directeur compliance, ce n'est pas le scénario idéal.

Pierre-Antoine Badoz, Orange : Cela n'a pas été un cauchemar, puisqu'il n'a pas eu lieu...

Xavier Leloup, le Magazine des Affaires : Il n'a pas eu lieu, mais si ça avait eu lieu… ?

Eléonore Hannezo, Linklaters : Est-ce que ça n'a pas eu lieu pour cette raison-là ?

Xavier Leloup, le Magazine des Affaires : C'est ça, c'est ma question.

Pierre-Antoine Badoz, Orange : Je n'étais pas dans cette fonction qui d'ailleurs n'existait pas encore. L'actionnaire principal, qui était le gouvernement suédois, n'a pas souhaité donner suite, et donc l'affaire ne s'est pas faite.

Jean-Jacques Quang, Duff & Phelps : C'est vrai qu'aujourd'hui dans les opérations d'acquisition, on constate de plus en plus un volet due-diligence dédié à la compliance, pour pouvoir évaluer toute l'exposition que l'on pourrait avoir, et prévenir les incidents, les sinistres qui viendraient post-acquisition.

Xavier Leloup, le Magazine des Affaires : C'est quand même un enjeu majeur pour toutes les acquisitions étrangères qui sont aujourd'hui devenues monnaie courante. Lors d'une précédente table ronde, un dirigeant nous expliquait qu'après avoir réalisé une acquisition au Brésil, il avait découvert que le comptable opérait quelques petits voyages suspects…. Il est donc assez classique d'être confronté à des irrégularités quand vous achetez une entreprise.

Jean-Jacques Quang, Duff & Phelps : Oui, il peut y avoir des petites irrégularités, et puis il y en a des plus sérieuses, organisées, systématiques ou qui sont peut-être orchestrées au plus haut niveau de la hiérarchie. Donc il y a vraiment deux poids, deux mesures, et ce sont ces derniers éléments-là qui sont les plus délétères, parce que quand on achète une entreprise, il peut y avoir des différences financières, juridiques, opérationnelles, celles-ci sont plus ou moins reflétées dans le prix d'acquisition ; mais l'exposition en matière de pratiques non-conformes, n'est pas forcément prise en compte dans la valeur de l'entreprise et peut avoir des répercussions dramatiques. Donc il faut pouvoir effectivement aborder les due diligences sur les aspects compliance, et je pense qu'il y a une

Catherine Delhaye

➤ Catherine Delhaye est la Directrice de l'Ethique et de la Conformité de Valeo qu'elle a rejoint en mars 2012. Elle est membre du Comité Opérationnel du Groupe Valeo. Elle préside également le Comité d'Alerte du Groupe.

➤ Catherine Delhaye a débuté sa carrière en tant qu'Avocate au barreau, au sein du cabinet d'Avocats Alain Bensoussan, durant six années.

➤ Catherine Delhaye a ensuite rejoint Accenture pendant seize ans où elle a occupé différentes fonctions telles que Directeur Juridique pour l'Europe, le Moyen-Orient, l'Afrique et l'Amérique Latine. Elle est devenue, au sein d'Accenture, Deputy General Counsel en 2007 et Regulatory Ethics and Compliance Global Managing Director.

tendance à ce que les grands groupes, quand ils font des grosses opérations internationales fusion-acquisition, intègrent de plus en plus ce volet conformité aux réglementations, pour s'assurer qu'on a la bonne organisation en place, qu'on ait à peu près une assurance raisonnable que les risques soient sous contrôle, maîtrisés.

Xavier Leloup, le Magazine des Affaires : Ça veut dire que quand on regarde les comptes de l'entreprise cible, on les regarde pour la génération d'EBITDA et sa rentabilité, mais on les regarde peut-être aussi pour les mouvements suspects ou sans contrepartie ?

Valentin Autret, Skadden Arps : Il y a effectivement des contrôles qui relèvent de l'enquête interne, mais qu'il peut être difficile d'approfondir en amont d'une acquisition. Il faudra cependant le faire après l'acquisition si elle est réalisée. Dans les procédures de due diligences, il est plus fréquemment demandé de s'intéresser aux mesures de compliance mises en place dans l'entreprise cible. Un programme de conformité est-il en place ? Est-il conforme à ses standards nationaux ? Conforme aux standards de l'investisseur ? etc. Cette demande d'un audit compliance est très forte de la part d'investisseurs étrangers et incite d'ailleurs beaucoup d'entreprises à mettre en place des programmes solides. L'entrée en vigueur du RGDP, dont les sanctions sont importantes, devrait augmenter ce type d'audit.

> ''Il est clair que nos missions contribuent largement à faire avancer la cause du développement durable et à donner une belle image de l'entreprise, soit en la protégeant, soit en montrant combien elle est vertueuse et combien elle a investi''
>
> *Catherine Delhaye*

Eléonore Hannezo, Linklaters : C'est extrêmement difficile de déceler la corruption sur la base des documents qu'on a dans une due diligence classique. Il y a beau y avoir une façade de conformité avec toutes les bonnes cases cochées, des contrats par exemple avec les intermédiaires prévoyant des clauses anti-corruption, on ne peut pas être totalement sûrs, sur la base de seuls documents, de ce qui se passe.

On sait bien que ce n'est pas parce qu'il y a une clause anti-corruption dans un contrat que ça n'existe pas. Ce qui est intéressant, ce sont les flux financiers vers les intermédiaires, leurs véritables missions, etc., et ça, savoir si c'est problématique, on ne le voit pas simplement sur le papier.

Xavier Leloup, le Magazine des Affaires : Ça veut dire qu'il faut se déplacer, regarder ? Dans une acquisition, il faut voir aussi sur le terrain comment les choses se déroulent ?

Jean-Jacques Quang, Duff & Phelps : Comme disait Catherine, si l'on constate qu'il y a un programme avec un certain nombre de dispositifs pour pouvoir se contrôler en interne, on peut se dire qu'effectivement, il y a déjà eu un balayage sur les risques potentiels dans certains pays. En fonction des dossiers avec certaines zones d'ombre, on peut être amené dans les due diligences, à demander des investigations complémentaires, à aller sur le terrain et vérifier qu'il n'y a pas de zones grises, au-delà des documents audités.

Catherine Delhaye, Valeo : C'est pour ça que le DOJ et le *Serious Fraud Office*, les régulateurs américains et anglais sont extrêmement pratiques et pragmatiques. Ils vous disent : "lorsque vous faites une due diligence pré-acquisition, vous voyez ce qu'on veut bien vous donner à voir, ce que vous avez la possibilité, le temps de voir au départ".

Xavier Leloup, le Magazine des Affaires : Oui, le temps de voir.

Catherine Delhaye, Valeo : Mais de toute façon, dès lors que vous prenez possession de l'entité, vous avez accès aux données, et ces régulateurs considèrent qu'il vous incombe d'aller creuser de nouveau pour vous assurer que les due diligence d'origine étaient suffisantes. Vous avez littéralement six mois pour le faire, six mois pour aller voir les autorités et dire : « voilà ce que j'ai trouvé ». Passé ce délai de six mois, on considère que soit vous n'avez pas été suffisamment diligent, soit vous n'avez pas d'intérêt pour la chose, soit vous avez accepté d'endosser ce que vous avez trouvé ou ce que vous n'avez même pas cherché à trouver, et c'est donc vous qui assumerez. C'est une démarche très pragmatique.

Xavier Leloup, le Magazine des Affaires : Pour résumer, sur une fusion-acquisition, les due diligence compliance ou conformité sont aujourd'hui aussi importantes qu'une due-diligence financière.

Catherine Delhaye, Valeo : Bien sûr, on a des questionnaires spécifiques, pour aller évaluer, 1) l'existence, 2) la solidité du programme de *compliance*.

Pierre-Antoine Badoz, Orange : Et ça a un impact sur la décision qui sera prise et un certain nombre d'affaires ne se font pas parce qu'en termes de compliance, on estime que…

Xavier Leloup, le Magazine des Affaires : C'est ça, ça peut mettre fin à…

Pierre-Antoine Badoz, Orange : C'est aujourd'hui clairement un "*deal-breaker*".

Xavier Leloup, le Magazine des Affaires : Oui, ce n'est pas juste théorique.

Pierre-Antoine Badoz, Orange : Absolument, ce n'est pas du tout théorique, c'est très concret, cela conduit parfois à l'arrêt des discussions.

Olivier Bénureau, le Magazine des Affaires : Mais a-t-on vraiment le temps de faire des due-diligences fouillées en compliance, quand on voit que les process sont accélérés, que tout s'accélère ? Est-ce qu'on peut vraiment le faire sérieusement ?

Xavier Leloup, le Magazine des Affaires : Surtout en compétitif, s'il y a plusieurs candidats pour une même cible.

Denise Lebeau-Marianna, DLA Piper : Sur le volet "protection des données à caractère personnel", le résultat des audits est souvent négatif car rien n'est documenté. Dans le meilleur des cas, quelques déclarations nous sont fournies mais les obligations réglementaires ne sont généralement pas respectées, notamment quant à l'information des personnes, à la mise

Pierre-Antoine Badoz

➤ Pierre-Antoine Badoz est directeur de la conformité - Chief Compliance Officer du Groupe Orange depuis octobre 2014.

➤ Il était précédemment « Directeur Orange Est », en charge des activités opérationnelles d'Orange en Alsace, Bourgogne, Franche-Comté et Lorraine depuis mars 2011.

➤ Diplômé de l'école Polytechnique, de Télécom Paris Tech et Docteur en Physique de l'Université Joseph Fourier de Grenoble, Pierre-Antoine Badoz a commencé sa carrière en R&D. Il a été conseiller technique au Cabinet du Ministre de l'Industrie avant de rejoindre le groupe France Télécom ou il a été directeur de la Stratégie et des Finances de la Division Opérateurs, directeur de l'Agence Entreprise « Paris la Défense », directeur du Centre de R&D « technologie », directeur des affaires publiques du groupe FT-Orange.

en place de mesures de sécurité, de conservation des données, lesquelles sont souvent conservées de manière indéfinie… Le résultat de l'audit se réduit donc à quelque chose de très court pour conclure que la société n'est pas conforme à la réglementation des données personnelles.

Olivier Bénureau, le Magazine des Affaires : Est-ce qu'on voit une vraie différence entre les acquéreurs anglo-saxons qui ont cette culture compliance et les acquéreurs français ? Est-ce que justement ils sont plus attentifs, parce qu'ils n'hésitent pas à allonger la durée des due diligence pour pouvoir justement se mettre à l'abri d'un enjeu réputationnel, donc d'irrégularité ? Est-ce que vous le voyez ?

Jean-Jacques Quang, Duff & Phelps : L'expérience que j'ai pu avoir, c'est surtout avec des fonds d'investissement anglo-saxons et américains, qui quand ils acquièrent une société font leur due diligence et peuvent effectivement prendre du temps supplémentaire d'analyse, d'investigations complémentaires avant de se positionner, donc d'investir. J'imagine que dans les grands groupes aujourd'hui, il y a également un tendance à se ménager un peu plus de temps, s'il y a besoin, pour aller un peu plus loin dans des investigations poussées sur tel sujet ou domaine, que ce soit de conformité ou de zones géographiques. C'est que j'ai pu faire dans mon expérience passée en industrie.

> "La compliance est un enjeu majeur dans le M&A, car quand vous rachetez une entreprise, vous rachetez potentiellement ses manquements passés à l'éthique"
>
> *Pierre-Antoine Badoz*

Xavier Leloup, le Magazine des Affaires : On parle de l'accès à l'information. Valentine, quand on a préparé cette table ronde, vous m'avez parlé d'un concept que je n'avais pas du tout en tête, à savoir le sondage, autrement dit le contrôle par échantillons. Qu'en est-il exactement, en particulier dans le monde de la banque que vous connaissez bien ?

Valentine Baudouin, Kramer Levin : J'ai en effet occupé différents postes en banque et société de gestion d'être avocate. La conformité était une notion quasi inconnue en banque il y a trente ans et elle est dorénavant prééminente dans tout le secteur financier. La conformité est issue à l'origine de la déontologie, c'est-à-dire le « gardien » de l'interprétation des textes les plus structurants pour l'établissement. La notion a connu une transformation entre 1995 et 2000 : la fonction « déontologie » disparaît peu à peu pour être absorbé par la notion plus large (et distincte) de « conformité ». L'évolution des textes réglementaires français le prouve par exemple avec l'apparition de la notion dans le Règlement CRBF 90-08 qui introduit la notion de « responsable du contrôle interne ». La notion est par la suite en croissance régulière jusqu'en 1997, date de son explosion à travers le Règlement CRBF n°97-02. Ce règlement met en place le système actuel de conformité, repris à l'identique en matière financière au sein du Règlement général de l'AMF. Pour comprendre la conformité, il faut comprendre sa *ratio legis*, c'est-à-dire ses soubassements idéologiques. La conformité a deux parents. Tout d'abord, la philosophie de l'aversion au risque, c'est-à-dire de l'idée que le risque est une matière scientifiquement déterminable et contrôlable. Elle est également le fruit de l'opposition qui a existé entre l'approche latine dite des « principes » (*based principles approach*) et l'approche anglo-saxonne de l'ultra-réglementation (« *regulation based approach* »). Ainsi, quand vous regardez dans le domaine de la banque, dans le domaine des services d'investissement ou dans le domaine de la gestion d'actifs, la conformité est née de la croyance que le système bancaire et financier ne peut se développer qu'en procédant à une suppression méthodique des risques ce qui impose de les définir, un par un, de les identifier puis de les soumettre à un corpus de règles étatiques dupliquées à travers des procédures internes destinées à proscrire toute survenance du risque, ces règles étant soumises à une superposition de niveaux de contrôles exercées par des personnes protégées par l'indépendance de leur statut. Vous arrivez maintenant en 2018, dans le domaine financier, à ce que Thierry Bonneau, professeur de droit financier appelle la « mort par overdose ». On a ainsi vraiment une conformité qui est assez établie.

Xavier Leloup, le Magazine des Affaires : C'est charmant comme expression !

Valentine Baudouin, Kramer Levin : Elle a été utilisée en 2005 qui a vu son lot de réformes. Mais quand vous regardez ce qui s'est passé en réglementation post-crise, il y a eu également un amoncellement de réglementations sectorielles dans le domaine financier, auxquelles s'ajoutent toutes les réglementations dont on vient de parler depuis le début de la table ronde. La mise en place de ces réglementations dans des délais très réduits entre la parution des textes et leur mise en application (imposant un travail important d'interprétation en vue de leur exploitation) auquel s'ajoute un télescopage de différentes réglementations entrant toute en application au même moment put créer ce sentiment d'overdose. Une fois la mise en place des procédures, restent également à les contrôler. Dans mon expérience opérationnelle, c'était impossible de contrôler l'intégralité par exemple des dossiers d'entrées en relations d'affaires que faisait la banque avec ses clients. Une des façons de le faire, était de réaliser ce qu'on appelle des contrôles par sondage, c'est-à-dire de prendre un échantillon raisonnable de dossiers, selon un certain nombre de critères, et de les contrôler. C'est d'ailleurs également une méthode utilisée par les régulateurs lors de leurs contrôles.

Xavier Leloup, le Magazine des Affaires : Est-ce ce que vous faites aussi en entreprise ? Un matin, vous vous dites : « ce bureau, je vais le contrôler aujourd'hui » ? C'est de l'aléatoire ?

Pierre-Antoine Badoz, Orange : On a effectivement les audits qui vont cibler telle ou telle entité et faire effectivement ce type de contrôle par sondage, mais l'essentiel du travail, c'est le déploiement du programme de conformité, c'est à dire des différentes

Valentin Autret

➤ Valentin Autret est avocat au sein de l'équipe International Litigation & Arbitration de Skadden. Il co-anime l'activité contentieux du cabinet à Paris. Depuis 15 ans, Valentin traite des dossiers à forts enjeux financiers et industriels mobilisant des domaines variés du droit des affaires.

➤ Valentin intervient avec l'équipe M&A de Skadden pour accompagner des opérations stratégiques ou résoudre des situations conflictuelles sensibles (en 2017, Skadden a été le cabinet le plus actif en M&A en volume au niveau mondial).

➤ Valentin travaille également avec l'équipe Cross-border Investigations de Skadden (droit pénal, compliance, anti-corruption, sanctions internationales et règlementation des institutions financières). L'équipe est reconnue par la Global Investigation Review comme l'une des 5 meilleures dans le monde.

actions et des procédures qui doivent être mises en oeuvre dans l'ensemble de l'entreprise, parce que le risque de corruption existe absolument partout : il peut-être plus ou moins important parce qu'il dépend du pays, il dépend de l'activité spécifique de l'entité, mais il existe et s'il y a un problème de corruption dans une filiale au bout du monde, c'est toute l'entreprise qui sera concernée. Et donc, notre programme, nous le déployons de manière systématique dans l'ensemble de l'entreprise, de nos pays et de nos activités. Et c'est ça l'enjeu, pour une grande entreprise, d'avoir un déploiement qui soit homogène et le plus cohérent possible.

Xavier Leloup, le Magazine des Affaires : Ce qu'a dit Valentine a dû vous parler, parce que chez Orange, vous faites aussi de la banque maintenant.

Pierre-Antoine Badoz, Orange : Tout à fait, nous avons lancé Orange Bank en France en novembre dernier.

Xavier Leloup, le Magazine des Affaires : Donc vous avez la double casquette.

> "Avec les contraintes qui s'accumulent (loi Sapin II, loi sur le devoir de vigilance, le RGDP), le quantum des sanctions qui grimpe et la judiciarisation des activités de l'entreprise, l'attelage entre le responsable de la conformité et l'avocat contentieux devrait devenir central"
>
> ***Valentin Autret***

Pierre-Antoine Badoz, Orange : Nous sommes en effet maintenant une banque : Orange Bank est encore une petite banque mais elle croît rapidement et a des ambitions importantes. De ce fait, nous partageons tous les enjeux de la compliance bancaire, c'est-à-dire le respect de l'ensemble des règles et des procédures de conformité bancaire. A cela s'ajoute la conformité dont nous parlions jusqu'à maintenant, la prévention de la corruption et le respect des programmes de sanctions économiques. Nous avons de plus des éléments spécifiques et relatifs à la lutte contre le financement du terrorisme et le blanchiment d'argent, notamment en Afrique où nous opérons "Orange Money", notre service d'argent électronique : c'est un service disponible sur tous les portables qui se déploie de manière extrêmement dynamique. Nous offrons à l'ensemble de la population des services financiers auxquels elle n'avait pas accès précédemment, car les taux de bancarisation y sont faibles et sont parfois inférieurs à 10 %. A

contrario, les taux de pénétration du mobile dans la population adulte étant maintenant peu éloignés de ceux que l'on observe en Europe, Orange Money s'adresse potentiellement à l'ensemble de la population des pays où nous sommes présents.

Valentin Autret, Skadden Arps : Ce qui pose des questions intéressantes d'exportation de nos règles de compliance en raison de leur extraterritorialité. Une entreprise française avec une activité à l'étranger, par exemple en Afrique, l'exercera en respectant les règles françaises de compliance et en les imposant localement, y compris si l'activité est strictement localisée à l'étranger Si une défaillance apparaît à l'étranger, le risque juridique serait en effet aussi un risque français, voire uniquement français si le pays concerné n'a pas une réglementation identique…

Pierre-Antoine Badoz, Orange : Les banques centrales locales ont en fait adopté et adapté des règles de droit international, la réglementation de la BCEAO ou de la BEAC n'ont réellement rien à envier à celle de l'ACPR…

Pierre-Antoine Badoz, Orange : On trouve la réglementation sur place, on n'a pas besoin de l'apporter !

Valentin Autret, Skadden Arps : On doit néanmoins également respecter notre réglementation. Certains pays n'ont pas notre façon d'aborder les risques de corruption et de blanchiment ou les embargos. Dans une filiale très loin dans l'organigramme, chez un sous-traitant ou un partenaire commercial implantés dans un pays ignorant nos contraintes, ces sujets pourraient être ignorés, mal maîtrisés ou envisagés très différemment. Cet effet de l'extraterritorialité qui conduit à exporter des règles nationales et à en sanctionner la violation dans le monde entier a d'ailleurs douloureusement affecté des entreprises européennes en raison d'embargos inconnus chez nous. Le terme d'auberge espagnole qui a été utilisé traduit bien que la compliance conduit à ce que l'on importe et impose nos contraintes dans des pays ou des marché qui ne les connaissaient pas. C'est un vrai défi pour les directions de la conformité et leurs conseils d'expliquer et de faire accepter cette exportation juridique.

Pierre-Antoine Badoz, Orange : C'est le côté passionnant du métier !

Catherine Delhaye, Valeo : Le premier pilier d'un programme de conformité, c'est *the tone at the top*, c'est-à-dire l'engagement de la direction générale et du conseil d'administration à lutter contre le blanchiment d'argent, la corruption, les pratiques anticoncurrentielles, etc. Une fois que l'impulsion est formellement et fermement donnée, l'entreprise s'exécute, même si l'ensemble des contraintes qui se déversent alors sur les opérations suscitent de nombreuses réticences, voire résistances au début. C'est pour ça le *change management* s'impose.

Pierre-Antoine Badoz, Orange : Et c'est vrai que le rôle de la compliance est un rôle d'animation, d'organisation, je dirais même "d'évangélisation" de toutes ces bonnes pratiques qui doivent se disséminer à tous les niveaux de l'organisation et dans toutes les filiales, même - voire surtout - les plus lointaines. On parle de programme, et c'est réellement toute une organisation : ce sont des ressources, des femmes et des hommes, des moyens, des procédures. Il faut que celles-ci soient connues afin que les salariés, quel que soit leur métier et leur pays, sachent qu'il y a un cadre, et que ce cadre est la pour les aider.

Xavier Leloup, le Magazine des Affaires : Il y a une obligation de moyens, vous n'êtes pas tout seul. Vous avez des conseils, de très bons conseils aussi, le cas échéant. Je crois que c'est aux États-Unis que des ratios de contrôleurs internes sont imposés aux entreprises.

Valentin Autret, Skadden Arps : Chiffrer, mesurer, évaluer est effectivement une méthode permettant de s'assurer que les moyens adéquats sont mis en œuvre et que les procédures sont effectivement appliquées.

Valentine Baudouin, Kramer Levin : Le régulateur français a cette approche aussi. Très souvent, c'est l'insuffisance des moyens humains et techniques qui conduit à une sanction : « vous avez une insuffisance de moyens humains et techniques, donc vous ne pouvez pas avoir de bon programme de

Valentine Baudouin

➤ Collaboratrice senior au sein de Kramer Levin, Valentine Baudouin intervient en matière de structuration juridique des véhicules d'investissement. Disposant d'une forte expertise métier en matière de fonds d'investissement et de gestion d'actifs, elle intervient également en matière d'agrément des sociétés de gestion et des prestataires de services d'investissement, en relation avec l'AMF, et des conditions de commercialisation des produits financiers.

➤ Valentine Baudouin dispose d'une expertise spécifique en conformité dans les secteurs des marchés de capitaux, de la gestion d'actifs et de la banque et porte un intérêt particulier pour la finance alternative et les modes de financement alternatifs au financement bancaire conventionnel (financement participatif, places de marché et financement islamique). Elle collabore régulièrement aux groupes de travail de place sur ces sujets (AFG, Europlace, OCDE).

➤ Avant de rejoindre Kramer Levin, Valentine exerçait en qualité de conseil juridique et conformité de sociétés de gestion et banques privées.

conformité ». S'il n'y a pas de ratios, il y a néanmoins des attentes qu'on peut relativement bien calculer en termes de moyens humains et techniques. L'une des réactions suite à une sanction est d'ailleurs de renforcer la fonction conformité en ajoutant des moyens humains et techniques.

Xavier Leloup, le Magazine des Affaires : C'est ça. Il y a une injonction de faire. On peut demander aux entreprises de mettre un effectif : « vous faites x milliards de chiffre d'affaires, donc vous devez avoir une équipe d'au moins 100, 150, 350 »…

Pierre-Antoine Badoz, Orange : C'est effectivement le cas dans la banque mais ça ne l'est pas aujourd'hui, à ma connaissance, dans le domaine de la compliance, au sens prévention de la corruption et respect des programmes de sanctions.

> "Si le challenge « macro » est bien passé après la crise, reste encore à mon sens le challenge « micro », c'est-à-dire de s'assurer que l'accumulation de formalisme et de contrôle ne va pas entraîner une déresponsabilisation des acteurs"
>
> *Valentine Baudouin*

Xavier Leloup, le Magazine des Affaires : Là, en gestion des risques, on pourrait se dire : « je couvre l'organisation de mon propre contrôle de conformité ».

Valentin Autret, Skadden Arps : Statistiquement, plus on fait de contrôles, plus on trouve d'erreurs. Si on contrôle 100 % des opérations, on a *a priori* l'opportunité de repérer 100 % des erreurs. Plus on consacre de ressources humaines et financières à la compliance plus la probabilité qu'un événement défavorable intervienne devrait diminuer. Aborder la compliance avec ce prisme uniquement quantitatif présente cependant le risque de se satisfaire d'un ratio théorique ou de centaines de cases cochées. Envisager la gestion des risques avec pragmatisme, c'est-à-dire en acceptant de ne pas cocher toutes les cases, mais de cocher efficacement les bonnes semble plus




efficace. Pour allouer les ressources là où elles seront utiles le directeur de la conformité est alors essentiel. Il connaît la réglementation applicable, il connaît l'activité de l'entreprise et les opérationnels, il est impliqué dans les réflexions et les prises de décisions du top management. Il est bien qu'il implique aussi les ressources humaines afin de concrétiser le message sur papier glacé du rapport annuel disant : « *pas de ça chez nous* ». En lien avec les ressources humaines, le directeur de la conformité peut ainsi intégrer la dimension compliance dans l'évaluation et la rémunération de la performance des collaborateurs. Un exemple : il pourrait être rétrospectivement reproché à une entreprise d'avoir incité à conquérir des parts de marché là où l'on sait que le risque de corruption est important ; pour que l'entreprise ne soit pas tenue comptable d'errements individuels qu'elle aurait involontairement incités, le responsable de la conformité peut proposer que soit récompensé le respect de règles exigeantes même si elles rendent plus difficile le développement commercial.

On peut se demander ensuite si la gestion des risques c'est occuper le rôle de la police dans son organisation. Il semble en effet qu'il y ait une incitation à la coopération et à la dénonciation des brebis galeuses. Sans doute l'entreprise qui veut être reconnue comme victime doit-elle se comporter comme une victime et agir à l'encontre de ceux qui ont commis des actes répréhensibles lui portant préjudice. Les entreprises sont cependant soumises à des règles (protection des correspondances, des données personnelles, des droits des salariés, etc.) qui ne sont pas moins importantes que les objectifs poursuivis par les autorités de poursuite. Il ne faut donc pas que le respect de ces règles nuise à leurs relations avec ces autorités.

Jean-Jacques Quang, Duff & Phelps : Elle va aussi et d'abord dénoncer en interne, pas forcément auprès du législateur. Mais c'est vrai que ce dont je m'aperçois, c'est qu'un bon programme de compliance, avec tout le volet qualitatif d'accompagnement, permet effectivement de détecter et de traiter en interne. S'il y a des brebis galeuses, il faut les traiter déjà en amont pour que ça ne se reproduise plus et pour qu'on ne soit pas effectivement confronté à un incident qui se trouvera en place publique.

Catherine Delhaye, Valeo : Je rebondis sur ce qu'on disait tout à l'heure, c'est du management de risque, c'est à dire d'abord et avant tout, de la prévention. Et la prévention, ça passe par la sensibilisation. Parce *que you don't know what you don't know*. Tant que vous ne savez pas que vous êtes confronté à un risque, ou qu'une pratique est interdite, vous la pratiquez allégrement. Par exemple, vous payez en dollars des transactions avec des pays sous embargo américain etc. Donc, il faut 1) de la sensibilisation et 2) du contrôle interne permettant de vérifier au moyen de campagnes planifiées l'effectivité de votre programme et qu'il ne reste pas un programme sur étagère. Ensuite il faut des audits, et c'est le troisième point. L'audit cible des opérations particulières pour vérifier non pas l'effectivité, mais l'efficacité du dispositif. C'est à l'occasion d'un audit ciblé, que vous pouvez identifier un certain nombre de mauvaises pratiques. C'est aussi parfois par hasard, parce que vous auditez une activité ou une pratique, qu'une anomalie peut vous sauter aux yeux. Il y a une dernière dimension de prévention que sont les lignes d'alerte. Il est absolument fondamental de promouvoir les lignes d'alerte parce qu'elles permettent d'identifier au plus tôt les anomalies, lorsqu'il y en a, et d'y remédier. C'est tout ce dispositif qui se transforme en culture d'entreprise, qui s'infuse au plus profond de l'entreprise depuis le top management et le middle management, jusqu'aux employés. Là, vous avez raison une fois encore, c'est à travers les objectifs annuels, ou à travers cette culture qu'on diffuse, que se construit cet écosystème de *compliance*.

Xavier Leloup, le Magazine des Affaires : Mais finalement, le respect du formalisme suffit-il à se prémunir d'un risque ? Aujourd'hui, lors d'une transaction sur Internet, on vous impose souvent des conditions générales de vente que finalement personne ne prend le temps de lire. Un trop grand nombre de cases à cocher ne va-t-il pas finir par tuer le concept ?

Pierre-Antoine Badoz, Orange : Je pense, comme le soulignait Catherine, que la compliance, c'est un enjeu de changement et de culture et à ce titre, ce n'est pas du formalisme. Mais "en même temps", si je puis me permettre l'expression, un minimum de formalisme est nécessaire afin de pouvoir démontrer que l'entreprise a mis en œuvre les programmes, les actions et les procédures nécessaires, et qu'effectivement cette prévention est bien mise en œuvre, que ce n'est pas juste écrit sur le tableau à l'entrée de l'entreprise.

Valentin Autret, Skadden Arps : Avec la cartographie des risques la loi oblige à distinguer son degré d'exposition selon les marchés, les produits, les pays, les services de l'entreprise… Les mesures mises en place peuvent alors être spécifiques, c'est-à-dire pragmatiques et non théoriques. Parce qu'elles sont en phase avec les réalités opérationnelles elles seront plus efficaces. En cas de réalisation d'un risque, les autorités regarderont néanmoins dans le rétroviseur. Il faut donc disposer d'un dossier de travail sérieux expliquant les choix raisonnablement faits en fonction des risques raisonnablement anticipés.

Eléonore Hannezo, Linklaters : Je voudrais nuancer sur la cartographie des risques. Il faut formaliser pour pouvoir prouver qu'on a fait les diligences requises par la loi, mais il faut faire attention à ne pas trop formaliser, et surtout à savoir exactement ce qu'on écrit. La cartographie des risques, c'est un document central qui sera accessible aux contrôleurs de l'AFA, mais aussi à tout enquêteur à leur demande. D'ailleurs dans les recommandations de Sapin II publiées par l'AFA fin décembre dernier, il y a un élément qui me choque beaucoup. L'équipe crosspractice de Linklaters a d'ailleurs répondu à la consultation publique de l'AFA en soulevant ce point, mais il n'a pas été exclu des recommandations définitives de l'AFA malheureusement. Il est ainsi recommandé par l'AFA, dans la cartographie des risques, de donner les informations les plus complètes sur les incidents passés qui ont eu lieu dans l'entreprise. Or, qu'est-ce que cela signifie ? Cela équivaut à devoir raconter tous les incidents passés découverts dans l'entreprise, alors qu'on sait que l'autorité administrative a un devoir, c'est l'article 40 du Code de procédure pénale, d'alerter, de dénoncer au parquet les faits délictueux dont elle a connaissance.

Xavier Leloup, le Magazine des Affaires : C'est de l'auto-dénonciation.

Eléonore Hannezo, Linklaters : Oui, on avait dit que cela allait trop loin. On glisse vers l'auto-dénonciation. Il faut construire la cartographie des risques et le programme sur la base des événements passés, parce qu'évidemment c'est de l'expérience, et comme les programmes doivent être adaptés à l'organisation et à la culture de l'entreprise, c'est surtout grâce à cette expérience qu'on peut construire un programme efficace. Il n'en reste pas moins qu'il n'y a pas d'exigence de révélation exhaustive des faits passés, une telle exigence n'étant pas justifiée et, à tout le moins, pas conforme aux textes.

Jean-Jacques Quang, Duff & Phelps : Je vais apporter une petite nuance, parce que je pense que c'est une transposition de la méthodologie risk

management appliquée à Sapin 2. J'étais risk manager dans une autre vie auparavant, et c'est vrai que quand on fait une cartographie des risques, on répertorie tous les risques, tout en prenant en compte la sinistralité et la base d'incidents.

> "En tant que société de gestion, l'important est d'être capable de mettre un contexte sur les pièces contrôlées par l'AMF. Car c'est souvent l'absence d'explication qui laisse l'incompréhension s'installer"
>
> *Hannah Rossiter, Duff & Phelps*

Xavier Leloup, le Magazine des Affaires : Comme un assureur fait.

Jean-Jacques Quang, Duff & Phelps : Tout à fait. Pour pouvoir mieux circonstancier les risques que l'on apprécie. Bien évidemment, dans le cas spécifique de la corruption, on ne va pas jusqu'à dénoncer tout ce qu'il y a eu lieu auparavant. Encore faut-il qu'il y ait eu une traçabilité des incidents en interne avant la loi Sapin 2, ce qui n'est pas toujours le cas.

Valentine Baudouin, Kramer Levin : La cartographie des risques dans certains secteurs a pour but d'identifier les risques, les mesures correctrices puis d'évaluer le risque résiduel. Vous avez néanmoins certains grands risques où malgré la mesure préventive, malgré les mesures de contrôle, il y a ce risque résiduel. Connaître ce risque résiduel est une bonne façon aussi de le gérer.

Xavier Leloup, le Magazine des Affaires : Oui, il ne faut pas perdre de vue son intérêt en tant qu'entreprise, pour résumer.

Denise Lebeau-Marianna, DLA Piper : En matière de protection des données, le risque s'évalue de manière différente dans la mesure où avec le RGPD, l'entreprise est tenue de dresser un inventaire de ses traitements (une cartographie des traitements), et d'identifier les non-conformités pour mettre en place un plan de conformité. Or, documenter ces différentes étapes peut être problématique si les autorités y ont accès. Le recours à des avocats pour procéder à cet inventaire permet de protéger les résultats obtenus, par la "confidentialité avocat".

Xavier Leloup, le Magazine des Affaires : Denise, il y a ce sujet de la digitalisation. Vous allez nous en dire un mot, la gestion des données personnelles, c'est vraiment nouveau d'après ce que je comprends.

Denise Lebeau-Marianna, DLA Piper : Pas du tout !

Xavier Leloup, le Magazine des Affaires : Cette réglementation est nouvelle.

Denise Lebeau-Marianna, DLA Piper : Comme le rappelait très justement Isabelle Falque-Pierrotin dans son article dans *Les Échos*, 80 % du RGPD existe déjà dans la réglementation actuelle. Le RGPD ne fait que rafraîchir une réglementation qui date de 1978 pour la France qui a été précurseur dans ce domaine. La protection des données personnelles est loin d'être nouvelle. Elle n'a juste pas été prise assez au sérieux. Lorsque les entreprises étaient un minimum sensibilisées, elles procédaient à une déclaration souvent simplifiée mais sans véritablement se conformer aux obligations qui en découler, c'est à dire l'obligation d'informer les personnes concernées des conditions de traitement de leurs données, l'obligation de mettre en place des mesures de sécurité appropriées et une durée de conservation limitée, etc. Le RGPD apporte un véritable changement, en faisant disparaître (du moins en partie) les formalités déclaratives et en obligeant l'entreprise à se responsabiliser et à documenter sa conformité (connu sous le principe d'*accountability*). Le RGPD hérite de ce qui a été construit par la compliance pour instaurer de manière très prescriptive, les mesures à prendre pour se conformer à la règlementation. Comme le disait Catherine, le RGPD est extrêmement prescriptif sur ce qu'il faut mettre en place pour documenter la conformité. En témoigne, la référence aux outils qu'il faut mettre en place pour attester de la conformité. Tel est le cas notamment, des études d'évaluation d'impacts, de la nécessité de documenter les politiques qui seront mises en place pour informer les individus et assurer la transparence, des procédures pour faire appliquer ces politiques au sein de l'entreprise, les mesures techniques et organisationnelles qu'il faut mettre en place. Or dans le cadre de la compliance, ces mesures étaient au départ mises en place sur une base volontaire et sont devenues par la suite de plus en plus prescriptives avec la loi Sapin. Le RGPD s'inscrit dans une démarche très prescriptive en prévoyant : « les disposition contractuelles à insérer dans les contrats avec les prestataires, les mentions obligatoires à faire figurer dans les notices d'information etc. »

Xavier Leloup, le Magazine des Affaires : Mais il y a vingt ans, on ne manipulait pas autant de données personnelles.

Denise Lebeau-Marianna, DLA Piper : C'est effectivement le développement des technologies donnant lieu à un traitement de plus en plus important des données, de manière parfois intrusive et à l'insu des individus, qui a été à l'initiative du RGPD. Il est donc nécessaire de changer de culture et de commencer à documenter et surtout à structurer les process internes à l'entreprise, pour mieux appréhender la protection des données dès la conception. Le *privacy by design* est un concept qui existait depuis un certain temps, mais qui n'a jamais été véritablement appliqué et qui n'était pas prévu par les textes. Le RGPD consacre ce principe de manière expresse. Ce qui signifie qu'à chaque fois qu'un traitement est mis en oeuvre, la protection des données doit être envisagée dès la conception du traitement. Il est important de noter que tous les principes de licéité du traitement, transparence, loyauté, proportionnalité et minimisation de la donnée qui caractérisent le "*privacy by design*" existent déjà dans la réglementation actuelle. Ce constat devrait logiquement conduire à considérer que normalement, les entreprises situées dans les pays européens ont une petite longueur d'avance et devraient donc être prêtes au 25 mai 2018 contrairement à celles situées dans des pays non-européens qui du fait de l'extraterritorialité de l'application du RGPD se verront également appliquer le RGPD lorsqu'elles ont pour cible des personnes situées sur le territoire européen. Les autorités sont consciente que le RGPD implique une charge de travail colossale et qu'un nombre important d'entreprises en seront pas prêtes au 25 mai 2018. Les déclarations récentes des autorités européennes de protection des données ont été moins alarmantes que prévu. La CNIL a clairement indiqué que les contrôles sur les nouvelles obligations du RGPD (telle que l'étude d'impact, le droit à la portabilité, etc.) ne commenceraient pas immédiatement et que la CNIL serait plutôt dans une démarche d'accompagnement. En revanche, la CNIL maintiendra son pouvoir de contrôle et de sanction en cas de non-conformité aux obligations existantes qui existent depuis la loi du 6 janvier 1978 telle que modifiée.

Xavier Leloup, le Magazine des Affaires : Le changement, ce n'est peut-être pas de ce point de vue le contenu de la réglementation, mais plutôt leur champ de par les changements intervenus dans l'activité des entreprises.

Denise Lebeau-Marianna, DLA Piper : Vous voulez parler de la transformation digitale des entreprises ?

Xavier Leloup, le Magazine des Affaires : Oui, c'est cela.

Denise Lebeau-Marianna, DLA Piper : Cette transformation renforce l'obligation des entreprises à se mettre en conformité puisqu'elles traitent plus de données et doivent donc se conformer à des principes qui existent depuis un certain temps. Cela suppose un réel changement de culture avec une réelle sensibilisation à tous les niveaux du traitement. C'est ce changement de culture qui fera la différence lorsque l'autorité devra sanctionner puisque le RGPD retient parmi les critères d'évaluation la négligence. Ainsi, que l'on soit un nouvel acteur sur le marché du digital ou pas, il est impératif d'être sensibilisé à ces principes qui datent de 1978.

Xavier Leloup, le Magazine des Affaires : Vous m'avez notamment expliqué qu'existerait bientôt un délégué à la transmission des données ?

Denise Lebeau-Marianna, DLA Piper : Un Délégué à la Protection des Données, connu sous le nom de DPO ou DPD en français.






Xavier Leloup, le Magazine des Affaires : Donc le DPD va être dans l'équipe conformité, compliance ?

Denise Lebeau-Marianna, DLA Piper : Cela dépend de l'organisation interne du groupe.

Xavier Leloup, le Magazine des Affaires : Mais ce sera une autre fonction alors ?

Denise Lebeau-Marianna, DLA Piper : C'est effectivement une autre fonction qui se doit d'être indépendante puisque le DPO ne doit pas recevoir d'instruction sur la manière de conduire sa mission.

Catherine Delhaye, Valeo : C'est surtout une spécialité, c'est une expertise.

Xavier Leloup, le Magazine des Affaires : C'est une expertise, c'est très pointu.

Denise Lebeau-Marianna, DLA Piper : En effet, c'est une personne ayant des connaissances et une expertise très pointues.

Xavier Leloup, le Magazine des Affaires : Denise, vous m'aviez parlé aussi de mise en place de nouvelles structures de gouvernance.

Denise Lebeau-Marianna, DLA Piper : Oui, et le DPO va être au cœur de cette structure de gouvernance, pour les entreprises qui sont obligées d'en avoir un, sachant que les critères sont assez larges puisque seraient ainsi visées les entreprises dont les activités de base donnent lieu à des traitements qui impliquent une surveillance systématique et à grande échelle des individus. On pourrait ainsi penser que des entreprises qui ont une activité classique, a priori, ne seraient pas soumises à un DPO. Or avec la transformation digitale, toutes les activités de base peuvent conduire à vérifier ce critère rendant ainsi le DPO assez facilement obligatoire. En effet, à partir du moment où les entreprises s'inscrivent dans une démarche de rapprochement de l'utilisateur final et qu'elles veulent contourner les circuits traditionnels de distribution pour être au plus proche de l'utilisateur final du produit, le risque de vérifier le critère de désignation d'un DPO paraît élevé. Par ailleurs, tous les organismes publics sont soumis de manière obligatoire à l'obligation de désigner un DPO, de même que les entreprises qui traitent des données sensibles (ou catégories spéciales de données), telles que les données de santé. Dans l'hypothèse où le DPO ne serait pas obligatoire, les autorités de protection des données recommandent sa désignation sur une base volontaire, car il s'agit d'un point de contact important pour les autorités et cela permet en termes de communication de donner également une bonne image de l'entreprise.

Pierre-Antoine Badoz, Orange : Je suis d'accord avec vous. Le GDPR est quelque chose de complexe à mettre en œuvre! Il y a deux enjeux différents et fondateurs pour le GDPR : le premier enjeu, c'est la protection et donc la cyber-sécurité. Je travaille dans un groupe où nous traitons beaucoup de données personnelles. Nous sommes régulièrement, comme toutes les entreprises de réseau, la cible d'attaques cyber et nous devons nous protéger toujours mieux afin de préserver les données de nos clients, de nos partenaires et aussi bien sûr celle de nos salariés. Le deuxième enjeu concerne le traitement et l'utilisation des données personnelles qui doit se faire dans le respect du droit. C'est une exigence croissante de nos clients, au moins en Europe, d'être rassurés et d'avoir confiance dans l'utilisation légitime de leurs données.

Denise Lebeau-Marianna, DLA Piper : Bien sûr, et même vis-à-vis des autorités, avoir un interlocuteur qui soit représentatif de cette problématique au sein de l'entreprise est extrêmement important.

Xavier Leloup, le Magazine des Affaires : Oui, parce que les bases de données sont aujourd'hui considérées comme des mines d'or digitales dont on peut faire beaucoup de choses. Certaines sociétés sont même rachetées sur la base de la valeur de leurs actifs digitaux.

Denise Lebeau-Marianna, DLA Piper : Exactement, les bases de données clients constituent un véritable enjeu, le "*fuel de l'économie numérique*".

Pierre-Antoine Badoz, Orange : Les États-Unis par exemple n'ont pas adopté l'équivalent du GDPR et de nombreux modèles économiques y reposent sur l'utilisation la plus large possible des données personnelles. On peut donc penser que, prochainement, si leurs données concernent également des citoyens européens, les sociétés américaines devront se conformer aux règles du GDPR.

Xavier Leloup, le Magazine des Affaires : Dans la banque, ce n'est peut-être pas aussi sensible que la santé, mais on n'en n'est pas loin, parce qu'il y a énormément de données personnelles.

Denise Lebeau-Marianna, DLA Piper : Non, elle n'est pas qualifiée comme telle, par le texte mais elle fait partie des données dont le traitement est effectivement soumis à des conditions strictes, notamment quant aux mesures de sécurité particulières qui doivent les entourer, les finalités pour lesquelles on les utilise, et leur durée de conservation.

Xavier Leloup, le Magazine des Affaires : Parce qu'avec votre relevé de banque, vous suivez toutes vos dépenses, on peut suivre tout ce que vous avez fait pendant 48 heures.

Denise Lebeau-Marianna, DLA Piper : La réglementation donne une liste extrêmement claire des données sensibles. Ce sont notamment les données de santé, les opinions politiques, religieuses, les orientations sexuelles, les opinions syndicales, etc... Les données bancaires n'en font pas partie. En revanche, il y a des données soumises à un régime très strict, comme les données de condamnation, mesures de sûreté, infractions et certaines données très particulières comme le numéro de sécurité sociale. Ce sont des données soumises à un régime strict de la part des autorités, du fait de leur caractère "sensible". Sans être catégorisée de "sensibles", les données RH font partie des données présentant un risque.

Xavier Leloup, le Magazine des Affaires : La donnée RH ?

Denise Lebeau-Marianna, DLA Piper : Le RGPD a une approche basée sur les risques. Ainsi dans le cadre de la cartographie des risques établie lors de l'inventaire, les traitements des données des salariés sont généralement considérés comme étant des traitements à risque. En effet, il s'agit de données relatives à la paie, à la performance, à la gestion des carrières professionnelles et des talents, qui constituent à cet égard un actif important de l'entreprise.

Xavier Leloup, le Magazine des Affaires : Vous parliez de gestion des risques. Ce que vous nous dites entre les lignes, c'est que la plupart des entreprises ne sont pas encore prêtes.

Denise Lebeau-Marianna, DLA Piper : Les entreprises sont effectivement dans une démarche où elles ne peuvent couvrir de manière exhaustive tous leurs traitements. Elles doivent donc établir une cartographie des traitements avec une identification des traitements à risque afin de prioriser les actions à conduire en termes de conformité. C'est en tout cas l'approche que nous adoptons pour accompagner nos clients.

Olivier Bénureau, le Magazine des Affaires : Surtout pour les entreprises, quelle que soit leur taille.

Denise Lebeau-Marianna, DLA Piper : La désignation obligatoire d'un DPO est indépendante de la taille, dès lors que l'entreprise vérifie les critères.

Xavier Leloup, le Magazine des Affaires : Quelle que soit la taille, donc une ETI, voire une PME doit avoir un DPO ?

Denise Lebeau-Marianna, DLA Piper : Oui, à partir du moment où elle vérifie les critères d'une désignation obligatoires du DPO (une activité de base donnant lieu à une surveillance systématique à grande échelle des individus ou un traitement de données sensibles à grande échelle). Si le traitement donnant lieu à une surveillance systématique à grande échelle, ne concerne qu'une activité accessoire, le critère de désignation obligatoire du DPO n'est alors pas vérifié. Il convient donc d'analyser au cas par cas si les critères de désignation sont vérifiés ou pas. La plupart des clients que j'assiste aujourd'hui, sont en pleine transformation digitale, et ont fait le choix de désigner un DPO.

Xavier Leloup, le Magazine des Affaires : Et jusqu'à 4 % du chiffre d'affaires en sanction ? Ça me semble énorme.

Denise Lebeau-Marianna, DLA Piper : Il y a en fait deux seuils : 2 % du chiffre d'affaires annuel ou 10 millions d'euros ou 4 % du chiffre d'affaires annuel et 20 millions d'euros, le plus élevé étant retenu !
Il s'agit de seuils maximums qui

peuvent être pondérés par de nombreux facteurs: la coopération avec les autorités, les relations passées avec les autorités, l'absence de récidive, les diligences pour se mettre en conformité, etc…

Valentin Autret, Skadden Arps : C'est une obligation de moyens qui est ainsi lourdement sanctionnée, non une obligation de résultat. Les entreprises qui respectent les exigences de la loi ne devraient pas être sanctionnées même si un risque se réalise.

DeniseLebeau-Marianna,DLAPiper: Il ne faut pas uniquement se focaliser sur les sanctions administratives, il y a également les dommages et intérêts aux victimes.

Xavier Leloup, le Magazine des Affaires : Si on vole, c'est ce que j'avais en tête quand vous disiez que c'était sécurisé dans votre cabinet d'avocats, on en a parlé. Je peux m'introduire chez vous.

Denise Lebeau-Marianna, DLA Piper : A priori non du fait des mesures de sécurités en place !

Xavier Leloup, le Magazine des Affaires : On peut faire des attaques ciblées sur un cabinet d'avocats comme sur des entreprises, et divulguer des informations, s'en servir à votre détriment, à votre préjudice. Dans ces cas-là, êtes-vous considéré comme responsable ?

Denise Lebeau-Marianna, DLA Piper : Si j'arrive à démontrer que j'ai mis toutes les mesures qui étaient nécessaires et requises et conformes aux règles de l'art, au regard de la règlementation des données personnelles, j'aurai satisfait mon obligation de "rendre compte" et mes obligations.

Xavier Leloup, le Magazine des Affaires : S'il y a une faute.

Valentin Autret, Skadden Arps : Si on a respecté la réglementation, il ne devrait pas, a priori, y avoir de faute.

Denise Lebeau-Marianna, DLA Piper : Un volet intéressant et nouveau du RGPD est celui des *class action*, qui est quand même très important puisqu'il permet d'engager des actions de groupe par les personnes qui seront victimes d'une violation de protection des données. De plus, le projet de loi qui va amender la loi informatique et liberté et compléter le RGPD prévoit également l'indemnisation des victimes dans le cadre des *class actions*. Il semble donc qu'un contentieux important et sensible pourrait se développer dans les années à venir.

Xavier Leloup, le Magazine des Affaires : C'est quand même un énorme paquebot qui se profile.

Denise Lebeau-Marianna, DLA Piper : mais largement inspiré de certaines réglementations précédentes, déjà très structurée et avec un fort impact, je pense en particulier au droit de la concurrence et à la compliance. Le RGPD, s'inscrit dans l'esprit de ces règlementations.

Xavier Leloup, le Magazine des Affaires : C'est du travail pour vous tous, n'est-ce pas ? C'est bien. Il faut se réjouir !

Valentin Autret, Skadden Arps : On peut se réjouir que les entreprises soient incitées à réduire leur exposition aux risques. Il aurait pu être clairement indiqué que leurs efforts, dont les coûts peuvent être très élevés, seront pris en compte si un risque se réalise néanmoins. L'entreprise est en effet souvent victime des errements de l'un de ses collaborateurs. Avoir mis en place toutes les mesures que la loi impose, ce qui évite la sanction administrative, devrait également réduire le risque de sanction pénale. Ce n'est pas encore clairement dit par les autorités de poursuite.

Catherine Delhaye, Valeo : Oui, ça, c'est le droit français. Si vous regardez l'affaire Morgan Stanley qui est le cas de référence dans le monde de la compliance, c'est très simple. Morgan Stanley avait un collaborateur indélicat qui, lors de sa mission en Chine a eu largement recours à la corruption pour développer le marché chinois; il a été attrapé. Le DoJ a étudié le programme de compliance de Morgan Stanley. Il a considéré que toutes les cases étaient cochées, que tout le travail avait été fait et que l'individu avait lui-même choisi de ne pas se soumettre aux règles de compliance de son entreprise; qu'il avait lui-même choisi de violer les règles qui lui avaient été expliquées, réexpliquées en détail et à maintes reprises, pour lesquelles il avait été formé. Morgan Stanley n'a pas été poursuivi. L'enquête ne s'est même pas ouverte formellement à l'encontre de Morgan Stanley.

Xavier Leloup, le Magazine des Affaires : Parce que formellement…

Catherine Delhaye, Valeo : C'est l'individu, en revanche, qui est en prison. Ce collaborateur a été très largement condamné, parce qu'il avait choisi de s'exonérer de ces règles. Je ne sais pas encore dans quelle mesure cela serait transposé dans le cadre de la loi Sapin, mais en l'occurrence, un vrai programme de Compliance a très bien fonctionné aux États-Unis.

Jean-Jacques Quang, Duff & Phelps : Il y a deux volets. Effectivement, si on n'a pas le dispositif adéquat, on s'expose à une sanction administrative du régulateur. Après, il y a le cas où un fait de corruption est poursuivi. Là, on entre dans une autre approche parce qu'on est face à la justice qui va instruire un dossier, sur lequel en fonction de la réalité, de la profondeur des faits de corruption, l'entreprise va être condamnée. Donc sur ce volet-là, même si on a un très bon dispositif, la justice, en France ou ailleurs, peut toujours en fonction de la gravité du fait de corruption, mener le dossier jusqu'au pénal, et obtenir des sanctions pénales et/ou civiles. Et c'est effectivement la double sanction : on peut faire l'objet d'une sanction administrative parce qu'on a eu un mauvais dispositif de compliance ; et en plus, on peut être condamné, s'il y a un incident majeur.

Xavier Leloup, le Magazine des Affaires : On parle de prévention des risques et de gestion des risques. Mais qu'en est-il lorsque ce risque survient ?

Valentine Baudouin, Kramer Levin : J'ai été juriste dans une société de gestion qui était fortement en termes d'encours à Bernard Madoff. Dans toutes les actions judiciaires ou les contrôles et enquêtes des régulateurs, la conformité a été clé. La question n'était pas de savoir si nous aurions pu « détecter » la fraude mais de démontrer que nous avions toutes les procédures en place qui auraient pu nous permettre de la détecter. Le fait d'avoir documenté ces points de contrôle a également été un facteur important. Et pourtant le niveau de due diligence sur un gestionnaire n'était pas le même dans les années 90 que dans les années 2005. Ce n'est pas parce que vous avez un doute sur l'occurrence d'un risque que vous allez être sanctionné. Il s'agit plutôt de pouvoir s'assurer que face à un doute, une mesure a été mise en place, et que cette dernière a été appliquée ou contrôlée. Dans des crises comme celle-ci, ce n'est pas que le droit finalement qui a été utile, c'est également la conformité.

Xavier Leloup, le Magazine des Affaires : Ça vous a sauvé finalement ?

Valentine Baudouin, Kramer Levin : Il est difficile de le dire. Cela a été en revanche des arguments qui ont été mis en avant par nos conseils externes. Avoir des contrôles, des programmes préventifs, de la documentation vous permet finalement de retracer comment l'entreprise avait appréhendé le risque, comment elle l'a vécu et comment c'est arrivé. C'est crucial si la crise survient.

Jean-Jacques Quang, Duff & Phelps : J'ai un autre exemple de vécu d'incidents de corruption sur un groupe pharmaceutique international : les diligences menées par les avocats, sur lesquelles nous avons collaboré, vont extrêmement loin parce qu'il faut démontrer avec des dossiers extrêmement lourds au DoJ, qu'on a tout le dispositif, et donc les contrôles, déployés au sein de l'organisation. Dans les investigations, on va regarder toutes les boîtes emails. On va regarder tous les échanges qu'il y a eu entre les opérationnels, pour identifier les schémas de corruption, les acteurs, mais également les échanges entre les opérationnels et la fonction Compliance, pour s'assurer que le cadre préventif existe, s'il a fonctionné et apprécier dans quelles circonstances les faits de corruption ont pu se dérouler.

Xavier Leloup, le Magazine des Affaires : Donc tous les emails, cela impacte également le quotidien, le contenu des échanges écrits qu'on reçoit ou qu'on envoie à son collègue de bureau. Il faut faire attention à ce qu'on écrit.

Eléonore Hannezo, Linklaters : Il faut faire attention à ce qu'on fait déjà !

Xavier Leloup, le Magazine des Affaires : Oui !

Eléonore Hannezo, Linklaters : Et après, à ce qu'on dit !

Jean-Jacques Quang, Duff & Phelps : Mais c'est impossible dans des sociétés de plusieurs dizaines de milliers de personnes, échangeant avec des collègues, des tiers à travers le monde, de se prémunir, de faire attention à ce qu'on va écrire ou ce qu'on pourrait potentiellement écrire. Et lorsque les investigations sont initiées, sous l'injonction du DoJ par exemple ; tout est balayé, c'est vraiment l'intégralité des échanges qui est prise en compte. On récupère tout sur les postes de travail, ce que l'on appelle des *images informatiques* des toutes les boîtes emails et autres documents, pour les analyses poussées : c'est la notion de eDiscovery.

Denise Lebeau-Marianna, DLA Piper : Ce qui n'est pas sans poser problème au regard de la protection des données, parce que…

Jean-Jacques Quang, Duff & Phelps : Les avocats en charge des investigations gèrent cet aspect...

Denise Lebeau-Marianna, DLA Piper : Oui, il faut en principe veiller à complètement isoler tous les messages identifiés comme personnels ou privés, etc.

Xavier Leloup, le Magazine des Affaires : Ce qui sous-entend de les lire d'abord pour dire : « non, ça, ça ne va pas ».

Jean-Jacques Quang, Duff & Phelps : Normalement, il faudrait écrire « private » ou « vie privée » sur les objets des échanges emails.

Denise Lebeau-Marianna, DLA Piper : C'est le résultat d'une construction jurisprudentielle en vertu de laquelle par défaut tous les emails reçus et émis, à partir d'une boîte mail de l'entreprise, sont professionnels. Ils peuvent donc être soumis à enquête, sauf s'ils ont été identifiés comme *"personnels" ou "privés"*. Or, dans le cadre des investigations massives menées (souvent sur demande d'autorités étrangères), tout est, comme vous le disiez, pris en "image" ("*imaging*"), mettant l'entreprise à risque. Il faut être extrêmement vigilant car elle peut être en infraction. Ce risque est accru, si les CE, syndicats ou autres parties intéressées sont informés des faits par des salariés et déclenchent eux-mêmes une action conduisant à vérifier la façon dont les investigations ont été conduites au sein de l'entreprise.

Eléonore Hannezo, Linklaters : Il faut se dire que les correspondances peuvent être examinées cinq ans plus tard. Or, cela peut être extrêmement difficile de reconstruire le contexte dans lequel ces propos s'inscrivent, surtout s'il ne s'agissait en réalité que d'une plaisanterie ou d'une fanfaronnerie. Tout le monde écrit dans l'instant présent mais personne ne pense à l'après.

Xavier Leloup, le Magazine des Affaires : Ce sont j'imagine des moments d'énormes tensions au moment du contrôle…

Valentine Baudouin, Kramer Levin : Et c'est la raison pour laquelle il est utile de s'y préparer en organisant des formations voire des « *serious games* ».

Eléonore Hannezo, Linklaters : C'est un vrai sujet. Devant l'ACPR, il n'est pas dressé de procès-verbal des échanges oraux ayant lieu avec les personnes physiques dans l'entreprise. Et pour l'Agence française anti-corruption, la loi prévoit que les entretiens doivent se dérouler dans des conditions assurant la confidentialité des échanges. Dans sa charte de contrôle, l'Agence dit : « l'entretien est confidentiel, ne peut ni être écouté ni enregistré, etc. » On verra comment cela se passera dans la pratique, mais à ce stade, on comprend que l'entreprise ne peut pas savoir, si elle n'insiste pas, ce qu'il s'est dit. Devant l'ACPR, on a soulevé un moyen de procédure sur ce point, en disant : « le défaut de procès-verbal est une atteinte au droit de la défense, puisqu'on n'est pas capable de voir ce qu'il s'est dit et de pouvoir y répondre ». À cela, il nous a été répondu : « oui, mais dès lors que de toute façon ce n'est pas dans le dossier et que les poursuites et la condamnation éventuelle ne vont pas se fonder sur ce qui a été dit, il n'y a pas de problème ». Sauf que je

trouve qu'il y a une vraie difficulté à ne pas savoir ce qu'il se dit parce qu'évidemment dans le stress devant des enquêteurs/contrôleurs, quelqu'un peut dire quelque chose d'inexact ou se tromper de bonne foi, ce qui devrait mériter un complément d'explication, une réponse.

Valentine Baudouin, Kramer Levin : D'où l'importance de la formation, parce que c'est vrai que les moyens de procédure sont difficiles à présenter.

Hannah Rossiter, Duff & Phelps : Pour rebondir sur ce point du contrôle et des enquêtes des autorités de tutelles dans le secteur financier, c'est vrai que côté ACPR on a moins de cadres appliqués par rapport au contrôle, et que l'AMF a un déroulement des missions de contrôle qui est bien plus précis que l'ACPR, mais néanmoins, ce n'est pas sans risque, parce que l'AMF, comme vous le savez, intervient très peu sur site aujourd'hui, contrairement à il y a quelques années, et donc sur pièces, et donc les documents qui sont téléchargés sur une base de données, qui sont récupérés par la mission de contrôle de l'autre côté, et ça crée un autre type de risque en fait. Ça rejoint le point de tout à l'heure. C'est l'incompréhension qu'on peut avoir face à des pièces qui remontent à il y a trois ans en général pour les contrôles AMF. L'important, c'est être capable en tant que société de gestion contrôlée de mettre un contexte sur ces pièces. Et très souvent, ce qu'on voit de notre côté quand on accompagne ces missions de contrôle, c'est l'incompréhension de la mission de contrôle qui s'installe relativement tôt, qui n'est pas aidée par l'absence d'explications et l'absence de contexte posée par la société de gestion. Ce que nous conseillons systématiquement, c'est de dire : « si vous passez ces documents à un tiers, que ce soit au sein de votre structure ou à l'extérieur et que la personne ne comprend pas ce qui est écrit soit dans le contrôle, soit dans la procédure, dans ce cas-là, vous rajoutez quelque chose pour expliquer le cadre ». Au vu de mon expérience, quand une mission de contrôle commence à déraper côté AMF, ce n'est pas que la mission de contrôle qui contrôle qui a des conséquences parfois sur certains domaines, et pas forcément sur le domaine d'activité critique de la société de gestion, il y a de la place pour que l'incompréhension s'installe. Et petit à petit, si on ne ferme pas les portes au fur et à mesure, on arrive à un constat en fin de contrôle, avec un rapport de contrôle qui n'est pas tout à fait faux, mais qui n'est pas non plus très pertinent compte tenu de l'activité. C'est là où ça dérape. On a des propositions administratives voire de fonction, certainement avec un certain nombre de points qui sont pertinents, mais la direction ne se sent pas comprise, l'activité de la société n'a pas été bien comprise et les griefs retenus ne sont pas pertinents compte tenu de l'activité exercée au sein de la société. Donc on peut effectivement avoir plus de risques quand les enquêteurs et contrôleurs se baladent autour de la machine à café ou de la fontaine d'eau, c'est clair, mais il y a aussi un risque assez important de traiter à distance des sujets qui sont relativement techniques et qui ont une durée assez longue, et sur la base de pièces qui remontent parfois à il y a trois ans. Là, il y a aussi de la place pour que l'incompréhension s'installe. On arrive à une issue de contrôle qui n'est pas tout à fait favorable pour la société de gestion.

Xavier Leloup, le Magazine des Affaires : Le danger peut donc provenir autant d'un contrôle formel ou informel ?

Hannah Rossiter, Duff & Phelps : Oui.

Xavier Leloup, le Magazine des Affaires : Dans votre esprit, la notion de "contexte" signifie-t-elle qu'il faut systématique contextualiser ses courriels ? Qu'en est-il concrètement ?

Hannah Rossiter, Duff & Phelps : Il faut faire attention à la manière dont on présente les pièces. Ce sont exactement les mêmes enjeux pour l'AFA au moment d'une visite. C'est de contextualiser et d'expliquer ce que sont ces documents, à quel moment ils ont été préparés, par qui. Est-ce que ça tient tout seul en fait ? Est-ce que moi en tant que tiers qui arrive avec plus ou moins d'expérience, parce que c'est ça, les individus qui vont intervenir, que ce soit ceux de l'AFA ou au niveau des autorités de tutelle AMF, est-ce qu'ils ont la possibilité d'arriver aux mêmes conclusions et de se mettre dans la situation telle qu'elle existait à l'époque ? C'est là où effectivement on a ce problème où il est très compliqué de se remettre à l'instant t dans le passé. Ça se ressent particulièrement quand on regarde les échanges de mails, parce qu'il n'y a pas de filtre. C'est ce que disait Valentine, il n'y a pas de filtre, on se livre, on est entre nous.

Xavier Leloup, le Magazine des Affaires : Ce qui est humain ! Quand on écrit, il faut donc se mettre dans la tête d'un tiers qui va lire son message cinq ans plus tard ? C'est un peu schizophrène.

Valentin Autret, Skadden Arps : Il faudrait se méfier de sa spontanéité. Il ne serait pas anormal de revenir à une façon de travailler où l'on fait attention à ce qu'on écrit. Il est bien de se rappeler que même sans papier à entête, la forme et le fond de ses messages pourront être analysés avec un regard rétrospectif qui ne sera pas forcément bienveillant. Il faut donc se méfier des emails qui ressemblent à des SMS parce qu'on les écrit depuis son téléphone portable. Il faudrait toujours se demander si l'on aimerait retrouver son message en première page de la presse ou dans le dossier d'un juge d'instruction. C'est difficile, mais les formations internes aident à y arriver.

Valentine Baudouin, Kramer Levin : Nous avons certains clients qui nous ont indiqué avoir des projets en interne pour remettre l'email dans un contexte un peu plus « formel » afin d'arrêter de systématiquement écrire et confondre email et texto.

Jean-Jacques Quang, Duff & Phelps : C'est vrai que le problème va se compliquer avec les moyens de communication aujourd'hui : emails, SMS, tchats, réseaux sociaux...

Valentin Autret, Skadden Arps : Récemment, les autorités américaines ont prévenu qu'elles considèreront défavorablement l'utilisation d'outils de communication qui ne gardent pas la mémoire des messages.

Jean-Jacques Quang, Duff & Phelps : Si vous allez en Chine aujourd'hui, la moitié des échanges business - relations d'affaires, cotations commerciales, prix, conditions,... - se fait par Wechat. C'est entré dans les moeurs et pratiques de travail en Chine, il n'y a quasiment plus de traçabilité dans ce contexte. C'est extrêmement difficile, lors d'investigations, de pouvoir récupérer ces informations parce qu'elles sont détenues chez un tiers, en l'occurrence Tencent - pour Wechat. Ce tiers ne collaborera pas, ne donnera aucune information. C'est une société proche de l'État chinois. C'est une complexité énorme dans les investigations pour matérialiser les faits de corruption par exemple. Dans l'entreprise dans laquelle j'ai travaillé auparavant, les emails, c'est pour les échanges avec le siège, en France, en Europe, aux États-Unis, quand il y a besoin formalisme. Mais le quotidien, le business en Chine, ça va aussi vite qu'un *chat* ; on fait affaire d'abord, et on formalisera le contrat après. Il faut désormais intégrer que cela va être plus difficile dans cette partie du monde. Ce n'est pas envisageable de dire : « revenons en arrière, posons-nous, faisons des emails formalisés ». Il n'y a pas de solution miracle.

Eléonore Hannezo, Linklaters : C'est de l'information et de la formation. On intervient à Sciences Po Paris en Master finance. Le Master finance prépare notamment ceux qui vont être dans les salles de marché. On leur dit — c'est un des points importants — : "faites attention à ce que vous faites", d'abord, et ensuite : "faites attention à ce que vous écrivez".

Xavier Leloup, le Magazine des Affaires : Globalement, pensez-vous que les droits de la défense sont respectés ?

Denise Lebeau-Marianna, DLA Piper : Je voulais juste ajouter un point sur les investigations, car il y a un volet données personnelles assez important, mais souvent négligé dans toutes les investigations qui sont menées. En effet, quand une entreprise en Europe ou en tous les cas en France reçoit du DoJ américain, une injonction de rendre disponible un certain nombre de documents ou de données, une telle mesure n'est en principe pas valable car elle ne respecte pas les règles procédurales françaises et internationales. Ce principe a été très clairement réaffirmé par le RGPD en son article 48. C'est aussi un moyen de défense. En pratique, souvent les entreprises ont tendance à coopérer très vite car la société US du groupe risque de fortes sanctions. L'évaluation du risque les conduisent donc à se mettre en infraction au regard de la réglementation française et européenne.

Xavier Leloup, le Magazine des Affaires : Il y a des différences de procédures d'un pays à un autre.

Denise Lebeau-Marianna, DLA Piper : Exactement. Le DoJ doit passer par le juge français qui vérifier la proportionnalité de la demande de l'autorité étrangère et des documents qui feront l'objet d'investigation. Ce contrôle permet d'éviter qu'une masse de documents ne transférée de manière injustifiée à une autorité étrangère. Cette approche est également préconisée dans le cadre du *blocking statute* en France qui a également vocation à s'appliquer à ce type d'investigations de la part des autorités étrangères. Il est donc très important de bien encadrer cette transmission d'informations et ce d'autant plus que le RGPD réaffirme à nouveau cette nécessité de respecter les conventions internationales applicables en cas de transmissions de données sur demande d'une autorité étrangère.

Xavier Leloup, le Magazine des Affaires : Et peut-on se conformer à un contrôle tout en se mettant en infraction avec une autre législation ?

Denise Lebeau-Marianna, DLA Piper : Il est préférable de ne pas le faire, mais comme je le disais précédemment c'est souvent le choix opéré par les entreprises après une évaluation du risque. Maintenant, on a une disposition très claire dans le RGPD qui indique qu'une telle communication doit se faire sur la base d'un traité international, en l'occurrence, la convention de La Haye.

Catherine Delhaye, Valeo : Le célèbre "Yates Memo" (*Individual Accountability for Corporate Wrongdoing*) va s'avérer plus difficile à mettre en oeuvre. Madame Sally Yates, *assistant attorney general* sous l'administration Obama, a en effet précisé en 2016 qu'elle attendait des entreprises qu'elles coopèrent, et que coopérer, signifiait non seulement fournir les éléments d'informations, mais fournir des noms, de sorte que la responsabilité personnelle puisse également être recherchée et que les personnes directement impliquées soient sanctionnées, voire licenciées.

Jean-Jacques Quang, Duff & Phelps : Effectivement, lorsque l'entité juridique est sanctionnée de plusieurs milliards, elle peut recommencer. En revanche, la personne au sein de l'entreprise qui est responsable, poursuivie et puni par des peines de prison, cela aura un vrai effet dissuasif. C'est l'esprit du Yates Memo de faire évoluer la réglementation américaine dans ce sens.

Xavier Leloup, le Magazine des Affaires : C'est une parfaite transition avec la question que je voulais poser : pensez-vous qu'existe aujourd'hui une régression des droits de la défense ?

Eléonore Hannezo, Linklaters : Il y a la question des droits de la défense devant les autorités administratives, assez satisfaisantes. Mais ce qui est remis en cause ici, c'est la question de l'auto-incrimination. Je trouve qu'il y a un glissement de la compliance à l'auto-dénonciation, les autorités s'attendant presque maintenant, pour qu'il y ait une bonne compliance, à ce que l'entreprise aille se dénoncer. Or, il n'y a pas d'obligation de se dénoncer en droit français, à part pour des crimes ou des infractions extrêmement spécifiques. En matière d'infractions économiques, cela n'existe pas. Or, on le voit bien, le fait de bien remplir son obligation de conformité, à la fin, cela peut vouloir dire de prendre toutes les mesures de remédiation adaptées, y compris se dénoncer et négocier, si possible. D'ailleurs, sur le traitement des alertes, on le voit aussi. Il y a cette obligation de mettre en place des procédures d'alerte, de les traiter, mais personne ne dit ce que cela veut dire, en pratique, de traiter une alerte. Il faut la recevoir, la "traiter", mais ensuite, qu'est-ce qu'on en fait ?

Jean-Jacques Quang, Duff & Phelps : Oui, on la traite en interne avec le dispositif et les actions adéquats, déterminé par le programme de compliance.

Eléonore Hannezo, Linklaters : Oui, mais quelle est la bonne réponse à donner ? J'ai eu un dossier où on a découvert un acte de corruption à l'étranger, mais on ne l'a pas traité au point d'aller se dénoncer, parce qu'on ne savait pas comment cela pouvait tourner. En pénal, ce n'est pas comme devant l'autorité de la concurrence, où, si on est le premier à dénoncer les faits, on peut espérer une exonération totale. En droit pénal français, il n'y a aucune récompense donnée aux personnes morales qui se dénoncent. Donc à la fin, dans mon dossier, l'entreprise n'a pas signalé. En soi, l'alerte a été traitée, mais l'alerte n'a pas été traitée jusqu'à une transmission aux autorités. Donc aujourd'hui, est-ce que l'Agence française anti-corruption face à un type de cas comme ça, elle ne va pas aller dire : « pour être en bonne conformité, vous auriez dû alerter les autorités » ? Je ne pense pas que cela soit possible : cela ne serait pas conforme aux textes. Mais on est dans une sorte de glissement où de plus en plus de conformité, c'est de plus en plus d'identification de faits problématiques qu'il faut ensuite traiter. L'aspect "prévention" est clef, mais ce qui est plus sensible c'est la révélation de faits et la remédiation subséquente, c'est à dire que fait-on des faits qu'on est seuls à voir identifier...

Xavier Leloup, le Magazine des Affaires : Peut-être que pour justement se prémunir de tout risque, elle va sanctionner systématiquement ou être proactive.

Eléonore Hannezo, Linklaters : Mais il y a quand même un problème de principe au regard des droits de la défense, et en particulier du droit à ne pas s'auto-incriminer. Les dispositifs de plaider coupable sont en soi constitutionnels et validés par la CEDH, mais il y a quand même cette question de fond qui se pose.

Jean-Jacques Quang, Duff & Phelps : Il y a peut-être aussi une gestion des risques. Par exemple Airbus : ce groupe a pris les devants et a dénoncé des faits de corruption au sein de son activité commerciale. C'est donc de se dire : « je prends les devants, la pénalité sera plus clémente que si les autorités tombent dessus ». Aujourd'hui tout est fait pour que les faits de corruption remontent à la surface par des dispositifs de lanceurs d'alerte, par la multiplication des parties prenantes avec la mondialisation des activités. C'est une question qu'il faut se poser : si on se dénonce aujourd'hui, on va peut-être payer 100 alors que si on se fait attraper demain, ce sera 1000.

Eléonore Hannezo, Linklaters : Ça, c'est la vision idéaliste. Je pense qu'il y a quand même beaucoup d'entreprises

qui, face au choix, préfèrent ne pas se dénoncer.

Xavier Leloup, le Magazine des Affaires : C'est un choix.

Jean-Jacques Quang, Duff & Phelps : Il faut évaluer effectivement la prise de risque que veut prendre l'entreprise. Ce risque doit être évalué, et finalement c'est la gouvernance et les valeurs et la posture de l'entreprise qui arbitreront.

Denise Lebeau-Marianna, DLA Piper : On a le même souci de la violation du droit à ne pas s'auto-incriminer avec l'obligation de notifier les failles de sécurité, la violation des données à caractère personnel qui impose à l'entreprise de notifier à l'autorité de protection des données qu'il y a eu une violation. Or, une telle notification peut être un élément déclencheur d'une enquête de la CNIL qui peut prendre une décision de condamnation mais en veillant à fonder sa décision non sur les éléments de la notification mais sur ceux de l'enquête résultant du contrôle. Cela soulève un véritable problème. L'absence de notification est sanctionnée mais la notification peut conduire à fournir "le bâton pour se faire battre".

Xavier Leloup, le Magazine des Affaires : Quand on développe une entreprise, c'est de la prise de risque. Le risque, d'ailleurs, en termes financiers, c'est une équation : plus vous prenez le risque, plus le rendement est élevé. Il s'agit de l'essence même de la création de valeur. Est-ce que tout ce dont on a parlé — et j'entends le rôle des responsables de la compliance dans la stratégie, etc. — ne va pas in fine influencer les choix stratégiques ? La compliance ne compromet-elle cette prise de risque indispensable à l'économie ?

Catherine Delhaye, Valeo : Je ne sais pas si ça l'empêche ; en tout cas, ça la manage. Ça oblige à y réfléchir, à la prendre en compte, à la pondérer. Ça permet une démarche beaucoup plus réfléchie en ce sens qu'au bout du compte, vous pouvez prendre un risque, mais vous savez que vous le prenez, et vous pouvez mettre autour tout un dispositif qui permette de le réduire. Je ne suis pas sûre que ça l'empêche totalement mais ça ne peut que réduire le risque.

Valentin Autret, Skadden Arps : Les entreprises se développent notamment grâce à la prise de risques raisonnables, ce que la compliance rend possible. Connaître, encadrer et prévenir un risque permettent plus facilement d'avoir envie de le prendre.

Pierre-Antoine Badoz, Orange : J'ai envie de dire qu'on va prendre des risques mais pour développer le business de manière durable. On ne va pas le faire de manière précipitée en disant « on va prendre des risques dans une optique de court terme, ne pas être regardant sur les pratiques pour gagner ce marché rapidement» et au bout de trois ans se faire sanctionner ! Non, il faut faire en sorte, même si c'est plus long, de respecter les règles afin de s'implanter de manière pérenne sur un nouveau marché. Ce sera fait en cohérence avec les valeurs de l'entreprise et surtout, on aura une croissance durable dans la région, le marché ou le pays.

Eléonore Hannezo, Linklaters : Mais là, on est dans une assemblée de juristes et de paranoïaques, par nature "risk adverse". On n'est pas avec des opérationnels de l'entreprise. J'ai fait des formations auprès d'eux, pas avec les équipes juridiques, et je trouve — vous le savez mieux que moi et j'imagine que c'est votre bataille quotidienne — que c'est difficile ; on trouve des réticences : « Pourquoi ? C'est trop de compliance. C'est pénible. On ne peut plus travailler. Vous nous empêchez de gagner des contrats. »

Catherine Delhaye, Valeo : Parlez-leur de ceux qui sont en prison.

Eléonore Hannezo, Linklaters : C'est ce qu'on fait, mais on sent une vraie réticence, comme si la compliance touchait à leur cœur de métier.

Pierre-Antoine Badoz, Orange : Oui, nous parlons ici de risque, nous faisons un peu peur, cela fait partie de la compliance. Mais je suis convaincu que la conformité sera pérenne lorsque l'on aura aussi réussi à faire passer des messages positifs. Et il y en a, il commence à y en avoir en termes d'image, en termes de réduction des risques, mais aussi en terme business. Sur le B2B, nos grands clients demandent maintenant à leurs fournisseurs de démontrer qu'ils ont mis en place un programme de conformité. En Europe, cela se généralise. Ce n'est pas encore tout à fait le cas dans d'autres régions du monde mais cela commence. Quand vous avez un réel programme de conformité — pas purement papier —, cela devient un avantage compétitif. J'ai l'exemple d'un appel d'offres que nous avons gagné car le client demandait de joindre à la réponse la preuve de l'existence du programme de prévention de la corruption. Il y a également un enjeu d'image : j'ai été frappé, il y a quelques semaines, par une publicité pour une crème au karité. Le message était, je cite de mémoire, « cette crème protège vos mains, mais elle protège également la communauté des femmes qui la produisent ». Dans ce cas de figure, on voit que la dimension éthique, la responsabilité sociale de l'entreprise, est devenue un argument pertinent, y compris à destination du marché grand public ! Et bien sûr, l'exigence, positive, pour l'entreprise, c'est un alignement de ses pratiques et de son discours.

Catherine Delhaye, Valeo : Il est vrai que l'éthique rejoint la compliance. Il y a quelques années l'éthique était plutôt un ensemble de valeurs. C'était moral, etc. À côté, la compliance, c'était les process, les méthodes, etc. Mais quand on s'intéresse aux aspirations des nouvelles générations, de tous les moins de 25 ans, même des moins de 30 ans, on s'aperçoit que ce sont des aspirations éthiques extrêmement fortes. Ils ne veulent pas entrer dans des compagnies qui n'ont pas mis en place ce qu'il fallait ou qui sont exposées à des pratiques absolument anormales. Vous avez aussi les agences de notation extra-financière qui regardent avec beaucoup d'intérêt tous les rapports annuels et qui cherchent en particulier tout ce qui a trait au *corporate social responsibility,* développement durable. Il est clair que nos missions contribuent largement à faire avancer cette cause et à donner une belle image de l'entreprise, soit en la protégeant, soit en montrant combien elle est vertueuse et combien elle a investi.

Xavier Leloup, le Magazine des Affaires : Vous leur faites gagner de l'argent.

Catherine Delhaye, Valeo : Je pense, oui.

Denise Lebeau-Marianna, DLA Piper : Oui, en instaurant la confiance.

Hannah Rossiter, Duff & Phelps : Je rejoins tout à fait ce qui a été dit tout à l'heure sur le fait que la compliance est perçue comme un empêchement de tourner en rond, un ensemble de coût. On aura peut-être l'adhésion totale de l'entreprise que ce soit de la direction ou des opérationnels. Il faut regarder ce qui s'est passé sur le secteur financier depuis vingt ans maintenant où on a des fonctions de compliance, de conformité aujourd'hui très bien développées, et où d'ailleurs, on a fait évoluer cette notion. Dans le temps on avait des déontologues, un concept un peu poussiéreux qui après avoir été oublié revient un peu maintenant avec la renaissance, le focus à nouveau sur l'aspect éthique. J'ai envie de dire que la crise de 2007, 2008 a un peu cristallisé les choses. Elle a permis aux fonctions de risque et de compliance d'être perçues comme permettant d'éviter une perte chiffrable. Effectivement, on n'a pas généré de chiffre d'affaires supplémentaire, mais au moins on n'a pas perdu ce qu'on avait. Et de plus en plus, ce sont des

Ils ont dit

➤ Valentin Autret

"Les entreprises qui respectent les exigences de la loi ne devraient pas être sanctionnées même si un risque se réalise".

➤Denise Lebeau-Marianna

"A chaque fois qu'un traitement est mis en oeuvre, la protection des données personnelles doit être envisagée dès sa conception. C'est le concept de privacy by design, que le RGPD consacre expressément".

➤ Catherine Delhaye

"Aujourd'hui, non seulement on est comptable des manquements, des violations de la loi, mais on est également comptable de ne pas avoir mis en place des systèmes de prévention"

➤Jean-Jacques Quang

"Aujourd'hui tout est fait pour que les faits de corruption remontent à la surface par des dispositifs de lanceurs d'alerte, par la multiplication des parties prenantes"

➤Eléonore Hannezo

"La cartographie des risques, c'est un document central qui sera utilisé dans le cadre d'une enquête, qui sera recherché par les enquêteurs pour dire justement que : "c'est la preuve que vous aviez connaissance du risque et que vous ne l'avez pas suffisamment prévenu"

fonctions qui participent à des lobbies institutionnels. Il y a des investisseurs qui arrivent. C'est tout à fait ce qui a été décrit tout à l'heure. Il y a un moment où on a regardé toute la partie opérationnelle. Ça va très bien, d'un point de vue pratique, ça marche. Regardons après si on a devant nous un partenaire qui fait envie et qui nous rassure dans la durée. Donc pour moi, les fonctions de compliance ont accompagné depuis la fin des années 2000 la croissance de la plupart des entreprises investissant des systèmes de gestion. Elles ont pu participer avec ce rôle de gage de qualité, de rassurer les institutionnels qui étaient en face, qui

pensaient investir. Je pense que c'est quelque chose qui va se généraliser.

Xavier Leloup, le Magazine des Affaires : Valentine, vous abondez dans le sens de Hannah ?

Valentine Baudouin, Kramer Levin : Oui, d'un point de vue « macro », totalement. Je pense que ce que vous disiez est beaucoup plus « micro ». Je pense qu'on est tous d'accord sur le fait de dire que la conformité au niveau macro, c'est de la création de valeur.

Ce qui est plus difficile — c'est comme ça que je le vivais en tout cas lorsque j'étais en interne —, c'est de faire passer le message au niveau micro pour convaincre qu'il y a une adéquation entre un formalisme exacerbé et création de valeur. Le challenge au niveau « micro » c'est l'adoption des procédures par les opérationnels sans voir justement le côté uniquement contraignant, terre à terre, *check-the-box* mais en véhiculant le message de création de valeur. Mon challenge était finalement de créer ce lien avec les opérationnels et leur faire comprendre que la conformité n'était pas un « empêcheur de tourner en rond », ni la personne qui dit « non ». Cela peut passer par plusieurs méthodes comme être au plus près des opérationnels avec des *hot desk*. Donc je vous rejoins tout à fait, c'est un vrai choix de l'entreprise de savoir s'il faut être un juriste ou s'il faut être un opérationnel pour être responsable de la conformité. Pour ma part, je venais justement de la fonction juridique et j'ai passé des examens de finance pour mieux comprendre le métier de la banque. Si le challenge « macro » est bien passé après la crise – plus personne ne doute de l'utilité de la conformité - reste encore à mon sens le challenge « micro », c'est-à-dire de s'assurer que l'accumulation de formalisme et de contrôle ne va pas entraîner une déresponsabilisation des acteurs. Parce qu'à force de vous dire qu'avec le *tick the box*, on n'a finalement plus besoin d'expliquer au client son produit, parce que de toute façon je vais lui remettre 90 pages en prospectus et il va signer en bas. Il ne faudrait pas qu'on arrive à l'effet inverse de la déresponsabilisation des acteurs au niveau « micro ».

Xavier Leloup, le Magazine des Affaires : Pour finir, pensez-vous que ces nouvelles règles de compliance mettent-elles les entreprises européennes en situation de faiblesse face à leurs concurrents américains ou chinois ?

Pierre-Antoine Badoz, Orange : Je pense que c'est mondialisé aujourd'hui. Toutes les réglementations…

Xavier Leloup, le Magazine des Affaires : Oui, mais ce ne sont pas les mêmes. En Chine, ce n'est pas pareil.

Pierre-Antoine Badoz, Orange : La Chine commence à adopter les mêmes dispositions, tout à fait.

Catherine Delhaye, Valeo : Bien sûr. Si vous regardez, c'est près d'un million de personnes en Chine qui ont été attrapées pour fait de corruption en trois, quatre ans, l'entité…

Xavier Leloup, le Magazine des Affaires : Et qui sont en prison.

Catherine Delhaye, Valeo : L'autorité antitrust chinoise est extrêmement forte. Il y a des *dawn raids* à répétition. En matière de cybersécurité et de protection des données nominatives en Chine, ils sont en train d'évoluer. Si vous regardez l'Inde, la politique anti-corruption, la réglementation de protection des données personnelles sont très strictes. Si vous faites le tour, le Brésil, la Corée; tout le monde s'y met.

Jean-Jacques Quang, Duff & Phelps: Je pense qu'il y a un nivellement par le haut. Ils savent que les Européens et les Américains ont mis un certain nombre de réglementations fortes, extraterritoriales, donc les pays émergents vont faire la même chose, se doter des mêmes armes réglementaires pour pouvoir lutter sur un pied d'égalité.

Eléonore Hannezo, Linklaters : Il y a là surtout un enjeu de politique pénale et, plus largement, de diplomatie. Avoir une arme réglementaire, c'est une chose ; décider de la façon dont on l'utilise et envers qui en est une autre. Aux États-Unis, par exemple, sur les quinze plus importantes condamnations ces dernières années en matière de sanctions internationales, il n'y a que deux entreprises américaines. Ce chiffre est évocateur.

Catherine Delhaye, Valeo : Mais si vous suivez le flux d'informations venant des Etats-Unis, vous constaterez que les sanctions tombent tous les jours. Le nombre d'Américains emprisonnés est très important…

Jean-Jacques Quang, Duff & Phelps: Vous avez raison, il y a une notion de guerre économique, et c'est pour cela qu'on se dote des mêmes armes, parce que les Américains attrapent étrangement plus de sociétés européennes. Il faudrait que l'Europe arrive à faire la même chose…

Catherine Delhaye, Valeo : Sapin va nous protéger !

Xavier Leloup, le Magazine des Affaires : Merci à tous. Merci Hannah d'avoir participé à distance. Merci à tous. ■

Ils ont dit

➤ Valentine Baudouin

''Très souvent, c'est l'insuffisance des moyens humains et techniques qui conduit à une sanction. S'il n'y a pas de ratios, il y a néanmoins des attentes qu'on peut relativement bien calculer en termes de moyens humains et techniques. L'une des réactions suite à une sanction est d'ailleurs de renforcer la fonction conformité''.

➤ Pierre-Antoine Badoz

''Notre programme, nous le déployons de manière systématique dans l'ensemble de l'entreprise, de nos pays et de nos activités. Et c'est ça l'enjeu, pour une grande entreprise, d'avoir un déploiement qui soit homogène et le plus cohérent possible''.