ifaci

institut français de l'audit et du contrôle internes

Actes du colloque

Dispositifs de lutte contre la corruption, le blanchiment de capitaux et le financement du terrorisme

Comment concilier sécurité des organisations et liberté des personnes ?

mardi 19 juin 2012

Les Salons de l'Aéro-Club de France

Sommaire

Discours d'ouverture **4**
Paul-Olivier GIBERT
Directeur Associé R2M Partners – Président de l'AFCDP 4

Panorama des réglementations et pratiques européennes et internationales **5**
Manon ROY 5
Vice-Présidente, Accuracy Canada 5

Les diverses manifestations de criminalité financière et l'impact des nouvelles technologies **9**
Manon ROY 9
Vice-Présidente, Accuracy Canada 9

La protection des données personnelles – Les textes réglementaires – Le projet de règlement communautaire **15**
Cyril PIERRE-BEAUSSE 15
Avocat, Global Data Protection Leader, Allen & Overy 15

Mettre en place des dispositifs de protection des droits et libertés des personnes **25**
Paul-Olivier GIBERT 25
Directeur associé R2M-Partners, CIL, Président de l'Association Française des Correspondants aux Données Personnelles 25

La lutte contre la corruption : quelles perspectives ? **28**
Dominique LAMOUREUX 28
Directeur Ethique et Responsabilité d'Entreprise, Thales 28

Ouverture de l'après-midi **34**
Christiane LEGAT 34
Directrice de l'Audit interne, Corporate Finance Bank, Groupe General Electric 34

Développer ou optimiser ses systèmes de lutte contre la corruption, contre le blanchiment et le financement du terrorisme **35**
Manon ROY 35
Vice-Présidente, Accuracy Canada 35
Nicolas DARBO 35
Associé, responsable de l'expertise dédiée aux institutions financières, Accuracy France 35

Lutte anti-blanchiment : quelles évolutions ? **43**
Marie-Agnès NICOLET 43
Présidente du Cabinet Regulation Partners 43

Comment développer une approche proportionnelle et équilibrée de la lutte contre la corruption, le blanchiment et le financement du terrorisme **47**
Table ronde animée par Blandine CORDIER-PALASSE 47
Fondateur de Cordier Conseil Executive Search 47

La conformité : entre loi et éthique **54**
Philippe MONTIGNY 54
Président d'Ethic Intelligence 54

Discours d'ouverture

Paul-Olivier GIBERT
Directeur Associé R2M Partners – Président de l'AFCDP

Il m'a été demandé d'introduire cette journée consacrée aux dispositifs de lutte contre la corruption, le blanchiment et le financement du terrorisme. Nos échanges auront pour questionnement sous-jacent : « Comment concilier sécurité des organisations et liberté des personnes ? »

Le sujet nous est apparu tout à fait d'actualité. En effet, nous avons assisté, au cours de la dernière décennie, à un renforcement des dispositifs de surveillance destinés à lutter contre le financement du terrorisme, la corruption et le blanchiment de capitaux. Ces dispositifs se traduisent par une mise en responsabilité des entreprises et des organisations. Cette mise en responsabilité implique la possibilité d'être sanctionné, si le dispositif est considéré comme insuffisant par le régulateur. L'entreprise doit dès lors s'interroger sur la conduite à tenir pour assurer sa sécurité juridique. Une première série d'interventions portera sur ce thème.

En parallèle, nous avons constaté le développement ou le renforcement de dispositions et réglementations destinées à assurer la protection des droits et libertés des personnes. C'est le cas de toute la réglementation Informatique et Libertés, sur laquelle j'aurai l'occasion de revenir en compagnie d'un avocat-expert. Néanmoins, il existe aussi d'autres réglementations, que nous pouvons considérer comme protectrices des droits et libertés des personnes, en matière de droit du travail, autour des thèmes de la non-discrimination. L'entreprise se trouve donc en tension entre, d'une part, des obligations de surveillance, qui vont plutôt dans le sens de la transparence la plus poussée, et d'autre part, des réglementations qui ont pour but d'assurer le droit à une certaine opacité.

Cette journée nous permettra, à travers les différentes interventions, d'examiner de quelle manière les différentes réglementations s'appliquent et comment l'entreprise construit un mode de fonctionnement tendant à équilibrer ces contraintes quelque peu contradictoires.

J'invite à présent Manon Roy à nous apporter son expertise sur le recyclage des produits de la criminalité, en tant que praticienne et professionnelle de la lutte contre ce type de phénomènes. Elle nous apportera aussi un point de vue, que je qualifierais, de manière provocante, d'anglo-saxon, mais francophone.

Panorama des réglementations et pratiques européennes et internationales

Manon ROY
Vice-Présidente, Accuracy Canada

C'est avec la plus grande humilité que j'introduirai la première partie de cette séquence, puisqu'elle devait être animée par Madame CUTAJAR, qui a finalement dû s'absenter. La première partie de ma présentation sera donc la sienne. Je vous exposerai ensuite ma propre présentation.

Les dispositifs actuels de lutte contre le blanchiment sont issus des travaux réalisés par le Groupe d'Action financière (GAFI). Ce dernier a été créé en 1989, à la suite d'une réunion des membres du G7 à Paris. Le GAFI a pour mandat d'aider le système financier à se prémunir contre les différentes menaces susceptibles de nuire au système financier international. Le GAFI a élaboré un programme de lutte contre le blanchiment de capitaux tandis que les membres du G7 ont chacun mis en place des dispositifs de lutte contre ces pratiques. Par la suite, d'autres membres se sont ajoutés au groupe. Finalement, le GAFI a mis en place tout un ensemble de règles, notamment le système des évaluations mutuelles. Une évaluation mutuelle du programme de lutte contre le blanchiment de capitaux a, par exemple, été menée par la France.

Le GAFI contribue également à la lutte contre la corruption. Il n'est pas doté de prérogatives normatives, mais s'efforce plutôt de susciter une volonté politique. Actuellement, la plupart des pays suivent ses recommandations. Initialement, 40 recommandations sur la lutte anti-blanchiment ont été émises. S'en sont suivies neuf autres recommandations relatives au financement du terrorisme. Tout récemment, le groupe a émis des recommandations sur la lutte contre la corruption.

Le GAFI préconise d'identifier des risques et de développer des politiques permettant de lutter contre le blanchiment de capitaux, le financement du terrorisme et plus tard, contre la corruption. Il souligne l'importance d'accorder les pouvoirs nécessaires à chacune des entités et pays qui devront mettre en œuvre ces politiques. Il recommande également la mise en place de mesures facilitant la coopération internationale. De même, les échanges d'information visent à mieux lutter contre le blanchiment de capitaux et à partager les typologies des différents pays pour renforcer les programmes de lutte.

Le processus d'évaluation mutuelle constitue un volet fondamental de ce système. Il permet d'évaluer l'efficacité des dispositifs mis en place. En particulier, l'évaluation mutuelle de la France s'est avérée globalement satisfaisante. A l'inverse, pour le Canada, les conclusions de l'évaluation menée il y a quelques années, se sont révélées plutôt décevantes. Le programme canadien présentait différentes lacunes. Le Canada n'avait notamment pas encore mis en place un programme évaluant les différents risques de blanchiment de capitaux. Il convient de rappeler que cette évaluation avait eu lieu plusieurs années avant celle de la France. Toutefois, il se peut également que la France soit beaucoup plus proactive en la matière.

Le rapport ayant trait à la France souligne plusieurs marges d'amélioration. Sur le fond, les mesures mises en œuvre en France sont très efficaces. Sur les 49 commentaires émis par le GAFI, la plupart font état d'un programme tout à fait conforme aux attentes. Les problématiques sont surtout liées à l'unité française de lutte contre le blanchiment de capitaux, Tracfin, qui ne posséderait pas suffisamment de ressources humaines et financières pour lutter contre le blanchiment de capitaux. Toutefois, le pays disposerait de suffisamment d'outils pour lutter contre le blanchiment de capitaux, notamment le pouvoir de réaliser des inspections auprès des entités visées, en particulier les institutions financières, ainsi que le pouvoir d'imposer des sanctions.

I) La lutte contre le blanchiment de capitaux

Les mesures mises en œuvre par la France sont donc plutôt satisfaisantes. Toutefois, la Commission Européenne a annoncé récemment qu'elle allait adopter une proposition de quatrième directive à l'automne 2012, pour améliorer le système de lutte contre le blanchiment de capitaux en Europe. Les moyens et les stratagèmes mis en œuvre en matière de blanchiment étant de plus en plus sophistiqués, ils requièrent une adaptation et une optimisation des règles.

Les pistes de réforme de la Commission Européenne en matière de lutte contre le blanchiment sont les suivantes.

1) Amélioration de l'approche fondée sur les risques

Il est actuellement demandé aux différentes entités visées par les exigences relatives à la lutte contre le blanchiment de capitaux d'évaluer les risques de blanchiment existant en leur sein. Cette évaluation porte sur les produits susceptibles d'être utilisés par les criminels cherchant à blanchir des capitaux, mais aussi les services et les clientèles à risque, les canaux de communication et de distribution. Ainsi, les services offerts en ligne présentent davantage de risques, dans la mesure où ils sont plus anonymes que les services offerts en succursales. Il est donc demandé aux entités de mettre en place des programmes dans ce sens. Ces approches ne sont toutefois pas clairement définies. Chaque entité doit adapter son approche en fonction de sa taille et de ses activités commerciales. Ce manque d'uniformité engendre des difficultés. La révision de la Commission Européenne vise donc à rendre ces évaluations plus concrètes, par une approche plus commune et supranationale. Il convient également de fournir des orientations sectorielles, puisque l'approche diffèrera entre une institution financière et une compagnie d'assurance. L'adaptation des orientations à la taille et à la nature des entités permettra de régler certaines divergences et de faciliter la vérification de l'identité des clients.

Lorsque les criminels mettent en place des stratagèmes de blanchiment, ils font souvent appel à des prête-noms ou des hommes de paille, qui réaliseront pour eux des transactions au sein de différentes entités, dont les institutions financières. L'obligation de vérifier l'identité des clients permet justement de déceler si les personnes effectuant les transactions ont partie liée avec le crime.

On parle également de détermination quant au tiers. Il s'agit d'une approche similaire, par laquelle on s'assure que la personne effectuant une transaction au sein de l'entité agit pour le compte d'un tiers. Il pourrait s'agir, par exemple, d'un expert-comptable, avocat effectuant différentes transactions au nom d'une autre personne. Il convient de faciliter l'identification des transactions relatives au blanchiment et de faciliter les opérations subséquentes. L'approche fondée sur les risques permettra d'améliorer toutes ces mesures et de renforcer les obligations de vigilance. Pour les clientèles jugées moins à risque, la surveillance sera moindre. Pour les produits, services ou clientèles jugés à risque moyen, les contrôles devront être renforcés. Enfin, pour les produits, services ou clientèles jugés très à risque, un contrôle extrêmement renforcé devra être mis en œuvre. Il s'agira, par exemple, de suivre régulièrement les activités de clients effectuant des transactions fréquentes susceptibles de soulever des soupçons.

Le projet de la Commission Européenne vise à intégrer l'approche par les risques dans le traitement des personnes politiquement exposées (PPE). Les PPE renvoient à des personnes ayant exercé des responsabilités au sein de différents pays, qui ont eu la possibilité de blanchir certains fonds en provenance de différents pays, via la corruption.

2) Adoption d'une directive pénale permettant d'incriminer plus facilement le blanchiment de capitaux et le financement du terrorisme

Il existe actuellement des disparités entre les différents dispositifs mis en place dans différents pays.

3) *Extension du champ d'application des obligations de la lutte contre le blanchiment et le financement du terrorisme*

Le GAFI recommande de considérer comme infractions sous-jacentes les infractions fiscales et pénales. Les transactions suspectes sont souvent liées à l'évasion fiscale. Il est très difficile de faire la distinction. En juxtaposant les deux infractions, la lutte contre le blanchiment est facilitée. L'extension du champ d'application passe également par un élargissement des entités visées par les règles actuelles. Ainsi, la directive s'étendrait au secteur des jeux de hasard, aux opérations de location effectuées par les agents immobiliers, ainsi qu'aux négociants en métaux et pierres précieuses.

4) *Amélioration de l'identification du bénéficiaire effectif*

Cette identification porte sur les clients utilisant les entités visées pour effectuer différentes transactions via leurs entreprises. Il existe actuellement une obligation d'identifier tout bénéficiaire effectif d'une entreprise, détenant au moins 25 % des actions ou droits de vote de l'entreprise. Il est envisagé d'abaisser ce taux à 20 %. Toutefois, la plupart des observateurs s'opposent à ce projet, estimant qu'il constitue le talon d'Achille de la lutte contre le blanchiment, et qu'il conviendrait plutôt de le renforcer et de mieux identifier les bénéficiaires effectifs.

5) *Amélioration du dispositif de déclaration des soupçons*

Actuellement, les entités assujetties doivent identifier et déclarer toute transaction effectuée, susceptible d'être liée à une activité de blanchiment de capitaux ou de financement de terrorisme. L'objectif est de renforcer ce programme, notamment au niveau des cellules de renseignement financier, comme Tracfin.

6) *Amélioration du dispositif au sein des groupes de sociétés*

Il existe des lacunes au regard des succursales ou filiales des entités assujetties. Il s'agit de renforcer les règles, de définir ce qu'est un groupe de sociétés, et d'autoriser une communication des cas en interne.

7) *Renforcement du dispositif applicable aux avocats*

La Commission Européenne estime qu'il n'est pas nécessaire de revoir fondamentalement le traitement actuel de la profession juridique, mais que les règles nationales doivent être suffisamment détaillées et précises pour permettre aux avocats de distinguer les situations dans lesquelles ils sont soumis à des obligations en matière de déclaration. L'objectif est que les professions juridiques déclarent davantage de transactions suspectes. Les systèmes les plus efficaces de lutte contre le blanchiment font, en effet, intervenir des avocats et des comptables.

8) *Autres modifications*

Il est envisagé d'harmoniser les sanctions administratives et de rechercher un équilibre entre la protection des données personnelles et l'efficacité du programme.

II) La lutte contre la corruption

Comme je vous le disais tout à l'heure, le GAFI lutte aussi contre la corruption. Il a émis récemment un rapport pour identifier les vulnérabilités du cadre actuel. Les recommandations initiales du GAFI ont été conçues pour lutter contre le blanchiment de capitaux et le financement du terrorisme, mais lorsqu'elles sont effectivement mises en œuvre, elles peuvent aussi aider à lutter contre la corruption. Le rapport identifie les éléments qui devront être améliorés.

Dans une communication sur la lutte contre la corruption, la Commission européenne constate que, « *bien qu'au cours des dernières décennies, l'Union européenne ait fortement contribué à ouvrir l'Europe et à la rendre plus transparente, il est évident qu'il reste beaucoup à faire. La corruption représente 120 milliards d'euros par an, soit 1 % du PIB de l'Union européenne* ».

Dans une résolution adoptée le 15 septembre 2011, les eurodéputés demandent des sanctions européennes contre la corruption et invitent les États membres à prendre un engagement politique clair pour mettre en œuvre les règles permettant de l'enrayer.

S'agissant du cadre juridique européen, il convient de rappeler que le traité sur le fonctionnement de l'Union européenne reconnaît que la corruption est une infraction grave revêtant une dimension transfrontière et que les États membres ne sont pas toujours armés pour y faire face seuls. La mise en œuvre du cadre juridique de lutte contre la corruption demeure inégale d'un État membre à l'autre et globalement peu satisfaisante. Même là où des institutions et une législation anticorruption sont en place, leur mise en application est souvent insuffisante dans la pratique.

La Commission juge donc nécessaire de stimuler la volonté politique sur cette question. Elle le fera au moyen de la mise en place d'un mécanisme, le rapport anticorruption de l'Union Européenne. Actuellement, des évaluations régulières sont effectuées au sujet de la lutte contre le blanchiment. La même démarche sera mise en œuvre pour la lutte contre la corruption. Ce mécanisme de rapports permettra de suivre et d'évaluer les efforts des Etats membres dans la lutte contre la corruption.

Les diverses manifestations de criminalité financière et l'impact des nouvelles technologies

Manon ROY
Vice-Présidente, Accuracy Canada

Les organisations criminelles doivent trouver un moyen de disperser et d'intégrer les fonds récoltés à travers des activités criminelles. Le blanchiment de capitaux est certes ancien comme le monde, mais récemment, l'émergence de nouveaux outils a aidé les criminels à créer des stratagèmes de blanchiment de capitaux. Par exemple, au Canada, mais également en France, le trafic de stupéfiants a pris beaucoup d'essor au cours des trente ou quarante dernières années, ce qui a nécessité une sophistication de ses moyens.

Or, à l'époque, il n'existait pas, ni en France ni au Canada, d'équipe d'investigateurs en mesure de lutter contre ce genre de fléau. Rapidement, la création d'équipes de policiers a permis de lutter contre cette problématique. A l'origine, lorsque les criminels importaient des stupéfiants, en France notamment, ils consommaient tout simplement leurs bénéfices, en acquérant différents biens et actifs grâce à l'argent issu du crime. Tout ceci a attiré l'attention, à la fois de leur entourage, mais également des investigateurs. Il s'agissait de comprendre comment certains individus ne semblant pas travailler de manière régulière ou recevoir un salaire important pouvaient acquérir un patrimoine de plusieurs centaines de milliers ou millions de dollars. Les policiers ont alors fait appel à des « juricomptables », pour les aider à mener des investigations, consistant notamment à comparer les revenus déclarés au fisc et l'accroissement du patrimoine, pour déceler d'éventuelles incohérences.

Dès lors, les criminels ont dû s'adapter et créer de nouvelles façons de blanchir les capitaux pour faire disparaître la trace de l'origine de leurs fonds. Ils ont d'abord dû déposer ces fonds auprès des institutions financières. Ces dernières avaient l'avantage de sécuriser leurs fonds et de leur apporter une certaine crédibilité. Pour déposer les espèces sans attirer l'attention, ils ont fait appel à différents individus de leur entourage, à l'abri de tout soupçon car dépourvus de tout passé criminel. Ces derniers ont été nommés les « *schtroumpfs* », en référence aux personnages de la célèbre bande dessinée, qui passent inaperçus. Ils ont déposé des espèces dans les institutions pour des montants inférieurs au seuil de déclaration. La seconde étape consistait ensuite à créer une dispersion, en transférant les fonds entre plusieurs comptes de différentes institutions financières, dans plusieurs succursales et dans différents pays pour faire perdre la trace de l'argent. Il en résultait un enchevêtrement complexe de multiples transactions. La dernière étape consistait à réintégrer les fonds dans l'économie avec une apparence légitime. Dans les premières années, l'entreprise a été considérée comme une opportunité intéressante pour blanchir les capitaux. A l'époque, la plupart des transactions se faisaient en espèce, contrairement à aujourd'hui. Plusieurs types de commerces favorisaient, par conséquent, le blanchiment de capitaux, notamment la restauration.

L'immobilier constitue également un moyen de blanchir des capitaux. Ainsi, un individu issu de la criminalité identifie un immeuble locatif à vendre sur le marché. Il rencontre le vendeur en lui proposant de payer une partie de la valeur du bien en espèces. Si l'immeuble vaut 100 000 dollars, il propose de payer 75 000 dollars en apparence et de glisser sous la table 25 000 dollars en espèces. Vu de l'extérieur, l'immeuble locatif a été acquis au prix de 75 000 dollars. Quelques mois plus tard, le groupe criminalisé revend cet immeuble 100 000 dollars sur le marché, réalisant ainsi un gain apparent. Dès lors, le montant de 25 000 dollars qui avait été glissé sous la table aura une apparence légitime. Le criminel et son organisation pourront justifier l'accroissement de richesse. Lorsque cet individu se rendra auprès d'une entité financière pour procéder à un dépôt ou pour acquérir

différents biens, comme des valeurs mobilières ou des produits d'assurance, il gagnera en crédibilité.

Les criminels ont dû rechercher une sophistication accrue pour blanchir des capitaux. Des stratagèmes nettement plus spécialisés se sont ainsi mis en place. Dans ce contexte, les entreprises offraient de nombreuses opportunités de faire transiter des fonds vers l'extérieur du pays ou de les rapatrier. Alors que le criminel peut, à tout moment, être arrêté et se voir confisquer les biens issus de la criminalité, le transfert de fonds à l'extérieur du pays permet de les positionner hors juridiction, donc hors d'atteinte des investigateurs. Ainsi, une entreprise française pourrait ouvrir des filiales dans des pays qui offrent le secret bancaire, ou un taux de fiscalité moindre, et divers autres avantages, dont un bon système de communication et un système politique stable pour éviter les risques de pertes de patrimoine. Le criminel simule la vente de biens aux filiales à l'étranger et joue sur le prix de transfert. Si le criminel est supposé avoir vendu un bien à l'étranger, pour un montant de 20 dollars pièce, il pourra soit réduire ce prix à 10 dollars, soit l'augmenter à 30 dollars, en fonction de ce qu'il souhaite, à savoir transférer des fonds à l'étranger ou les rapatrier. Ainsi, les criminels acquièrent une multitude d'entreprises, en concurrence avec les entreprises présentes loyalement sur le marché.

Au cours des nombreuses formations que je dispense au Canada à ce sujet, les participants soulignent que le blanchiment de capitaux est bon pour notre organisation, parce qu'il fait tourner l'économie. Je souligne que ce point de vue relève uniquement du court terme. Les clients avec qui nous faisons affaire sont avec nous pour plusieurs années, pour du financement, pour l'acquisition de différents investissements. Au contraire, les criminels ne font affaire avec nous que pour quelques jours, quelques mois tout au plus. En outre, très souvent, les revenus initialement prévus ne sont pas générés, une grande dispersion a lieu. Il importe que les collaborateurs des entités financières comprennent bien cet élément.

Les organisations ont progressivement affiné leurs stratagèmes. Ainsi, elles ont eu l'idée de créer du faux financement. Un cas est notamment survenu au Canada. Un groupe de criminels implantés en Floride importait de la marijuana de la Jamaïque. La drogue était ensuite vendue aux Etats-Unis. Tout l'argent issu de cette vente était déposé sur différents comptes de sociétés anonymes, puis transféré à l'extérieur du pays vers des fiducies en Suisse. Plus tard, les criminels sont revenus au Canada et ont acquis un centre de ski en grave difficulté financière, pour huit millions de dollars. La fiducie suisse avait accepté de financer le centre de ski à hauteur de six millions de dollars parce que des dépôts servaient de garantie. Le centre de ski a ensuite permis de blanchir encore davantage de capitaux. En effet, différents produits de la criminalité étaient déposés dans les comptes bancaires du centre de ski, en simulant que l'argent provenait des activités du centre. Les employés du centre de ski étaient au courant mais n'avaient pas intérêt à dévoiler la situation. Quant à l'institution financière, elle n'a pas pu mettre la situation à jour, puisque l'entreprise concernée n'était pas locale.

Pour une institution financière, il est très difficile de détecter que la transaction d'un client est reliée à des fonds issus de la criminalité. Lorsque nous formons les personnels à la détection de ces situations, nous soulignons la fréquence des transactions et d'autres indicateurs complémentaires.

Pour complexifier le sujet, après le financement adossé à des actifs, il existe également de faux litiges. Ainsi, dans le cas d'une entreprise implantée en France, et d'une autre entreprise à l'étranger, un contrat est créé entre les deux entités. Par la suite, une rupture de ce contrat est simulée. Dès lors, l'entreprise située en France va ester en justice, faire appel à un conseiller juridique, se présenter devant les tribunaux pour pouvoir récupérer les dommages subséquents à cette rupture de contrat. Dans les faits, cela ne pose pas de problème puisque tout ceci a été monté de toutes pièces. Au lieu d'un procès, un règlement à l'amiable va survenir.

Plaçons-nous à présent du point de vue d'un employé dans une entité financière, une banque par exemple. Les indicateurs suivants sont susceptibles d'éveiller des soupçons.

Un conseiller reçoit un client nouvellement établi, qui vient créer une entreprise. Cette dernière enregistre une croissance importante et rapide. L'entrepreneur, rencontré régulièrement dans le cadre du financement de ses activités, annonce qu'il décide de s'ouvrir sur le monde et de faire affaire à l'étranger. Peu de temps après, il explique qu'il rencontre des difficultés puisqu'il a dû poursuivre en justice une entreprise avec laquelle il avait établi un contrat, et qu'il tente de récupérer des fonds sur lesquels il a été lésé. De manière inattendue, l'affaire sera rapidement réglée à l'amiable, les fonds récupérés permettant de rembourser de manière anticipée le prêt souscrit auprès de l'institution financière. En règle générale, les employés situés en première ligne ont une difficulté à détecter les problématiques relatives au blanchiment de capitaux derrière ces procédés. L'un des éléments importants à surveiller tient au fait qu'une entreprise a eu beaucoup de chance, a prospéré rapidement, a fait affaire à l'étranger, a dû ester en justice mais, par chance, a pu récupérer rapidement les fonds dans un règlement à l'amiable survenu très rapidement. Tous ces éléments sont de nature à illustrer une problématique de blanchiment de capitaux.

Les faux litiges peuvent aussi porter sur des factures impayées. Ils peuvent également être plus complexes. Ainsi, une entreprise acquiert une entreprise de recherche et développement à un prix officiel, assorti d'un montant en espèce versé sous la table. Par la suite, l'entreprise acquise met un nouveau produit sur le marché, obtient un brevet. Le criminel demande à une autre entreprise créée à l'étranger de copier le produit. Il pourra ester en justice pour violation de la propriété intellectuelle. Un procès aura lieu, suivi d'un règlement à l'amiable. Cet exemple démontre le degré de sophistication des stratagèmes mis en place, et la difficulté pour les employés des institutions financières de détecter ces derniers.

Avec le temps, les criminels ont identifié les multiples opportunités offertes par les entités financières. Leur problème initial consiste à pouvoir déposer des espèces. Ils ont donc fait appel à plusieurs types d'entités pour déposer ces espèces. Rapidement, le marché financier s'est ajusté. Les entités de valeurs mobilières ont refusé de recevoir des dépôts. Les criminels ont dû se tourner vers les banques pour déposer des espèces. Les banques ont raffiné leurs outils de détection des problématiques.

La deuxième étape, à savoir la dispersion, ne fait pas appel à de l'argent comptant, mais seulement au transfert d'argent en différents comptes, différentes institutions ou entités financières. Dès lors, toutes les compagnies d'assurance, de valeurs mobilières ou institutions financières peuvent servir, à travers de multiples transactions, à créer un enchevêtrement complexe. Le criminel s'est ainsi demandé quelles opportunités lui offrent les compagnies d'assurance de personnes. Ces sociétés ont développé des produits, par exemple en approchant certains clients qui venaient réclamer des produits d'assurance-vie. Ainsi, si j'apprends soudainement que j'ai un cancer, je contacte mon conseiller en assurance de personne. Ce dernier m'indique que je suis couverte pour un million de dollars. Il propose de me remettre 100 000 dollars immédiatement en espèce, en échange d'un changement de bénéficiaire effectif de ma police d'assurance. Dans mon désarroi, et par ignorance, je peux accepter de toucher 100 000 dollars pour profiter du peu de temps qui me reste à vivre. Or ces dispositifs ont été créés pour blanchir des capitaux, de même qu'au niveau des valeurs mobilières.

Au niveau des institutions financières, l'international est devenu très intéressant pour les criminels. En effet, ils doivent trouver des manières d'apparence légale pour transférer des fonds vers l'étranger et protéger ces fonds de toute saisie. Rapidement, les personnes spécialisées dans ce domaine ont su détecter les télévirements internationaux trop fréquents ou trop importants. Ils ont mené des investigations. Les criminels ont dû affiner leurs méthodes. Ainsi, le crédit documentaire sert à couvrir des opérations de blanchiment à l'international. Une nouvelle entreprise souhaitant faire affaire à l'étranger va obtenir tout un crédit documentaire pour supporter les transactions. Tout ceci apporte une crédibilité et une apparence de légitimité. Il est également recouru à l'affacturage, à savoir le fait, pour une entreprise, de vendre à une institution financière, à escompte, des comptes à recevoir d'une entreprise étrangère. L'affacturage donnera une grande légitimité à ces transactions.

Les criminels travaillent à déceler les opportunités dans chacun des secteurs des entités financières, mais aussi pour chacune des entités financières distinctes. Ainsi, au Canada, il existe le mouvement Desjardins, groupe financier coopératif très décentralisé. Ses multiples entités décentralisées permettent difficilement d'avoir une vision globale, d'autant plus pour les transactions effectuées par un client auprès de ces différentes entités. Les criminels font affaire, soit avec des personnes en interne en collusion, soit avec des anciens employés, qui fournissent des informations.

Croire qu'il n'existe pas de blanchiment de capitaux dans les différentes entités pour lesquelles nous travaillons n'est donc pas la bonne approche. Il convient de penser différemment. C'est la raison pour laquelle l'approche fondée sur les risques s'avère si utile.

Je terminerai en évoquant l'utilisation des nouvelles technologies. L'un des problèmes actuels tient au fait de devoir disposer d'espèces une fois intervenue la vente de stupéfiants sur le marché. Si cet élément pouvait disparaître, les clients pourraient payer la drogue dans la rue autrement qu'avec des espèces. Les cartes prépayées permettent au client de payer avec une carte préchargée, par exemple pour acheter de l'essence dans un commerce. L'organisation criminelle se retrouve alors avec un grand nombre de cartes prépayées, qu'elle utilise au sein d'un commerce. Elle va acquérir une entreprise de transport de marchandises. Les cartes prépayées serviront aux camionneurs. Ainsi, l'argent sera intégré au sein du système financier sans attirer l'attention. Différents services en ligne permettront d'effectuer des virements sur différents comptes ou des investissements à court terme auprès d'entités qui vendent des valeurs immobilières. Avec l'apparition des guichets automatiques, les « schtroumpfs » n'ont plus à se rendre dans les institutions financières pour procéder à différentes transactions. Il existe au Canada des guichets automatiques privés, détenus par des particuliers ou des entreprises spécialisées. Les criminels peuvent mettre la main sur ces guichets et les alimenter, avec des fonds provenant, non pas d'institutions financières, mais de la criminalité. Les clients réguliers vont procéder à des retraits dans ces guichets et placer malgré eux l'argent du crime dans l'économie financière.

Enfin, récemment, j'ai été informée du cas des jeux virtuels, dans lesquels le joueur se crée un avatar. Les criminels recrutent des jeunes performants dans ces jeux, mettent à leur disposition beaucoup d'argent issu de la criminalité. Ces jeunes prodiges font passer l'argent par différents comptes jusqu'à ce que l'on en perde la trace. Lorsque l'on rencontre de tels obstacles pour retracer la piste de l'argent, pour déterminer d'où il provient et vers où va l'argent, la situation est évidemment très complexe.

En conclusion, il importe de convaincre les employés de première ligne que le blanchiment de capitaux va désormais bien au-delà du simple dépôt d'espèces. La plupart des employés croient fermement que lorsque l'argent comptant n'intervient pas dans une transaction, cette dernière ne comporte pas de risque de blanchiment de capitaux. En réalité, il convient de les amener à penser différemment et de les sensibiliser aux nouveaux risques induits par la sophistication des créations d'entreprises ou d'organisations, localement ou à l'international, et des stratégies mises en place pour disperser l'argent du crime et lui donner une apparence légitime. En raison du *turnover* important dans les entités financières, il est difficile de maintenir une conscience de ces sujets parmi les employés.

Paul-Olivier GIBERT

Je vous remercie pour ce tableau très précis, qui nous rappelle la justification de l'existence de réglementations anti-blanchiment.

De la salle

J'ai eu la chance d'assister hier à une conférence de Thomson Reuters, en présence d'une intervenante de Tracfin. Au début de votre intervention, vous avez signalé un manque de ressources humaines chez Tracfin. En effet, Tracfin compte aujourd'hui 33

personnes, principalement issues de l'administration des douanes. Depuis cinq ou six ans, les enquêtes et saisines affichent une croissance d'environ 20 %, ce qui confirme le manque de ressources. 2 945 informations ont été mises en enquête en 2011, et 2 874 ont été mises en pré-enquête, c'est-à-dire soumises à un système d'investigation allégée. Tracfin a enfin la possibilité d'exercer un droit d'opposition sur des transactions, notamment dans le cas de transactions immobilières. Elle a usé de ce droit à huit reprises.

Par ailleurs, vous avez évoqué un manque de clarté des dispositions en matière de lutte contre le blanchiment. Je vous signale la création d'une institution appelée la *Global Organization of Parliamentarians against Corruption* (GOPAC), qui vise à informer et sensibiliser les parlementaires. La GOPAC a publié un remarquable rapport au mois de mars 2012, dédié à la lutte contre le blanchiment.

Paul-Olivier GIBERT

Merci pour ces compléments d'information très enrichissants.

De la salle

Pourriez-vous expliquer plus concrètement l'utilisation des crédits documentaires comme moyen de blanchiment ?

Manon ROY

Le crédit documentaire permet à une organisation de traiter avec une institution financière. Par exemple, si une entreprise canadienne souhaite débourser un paiement auprès d'une entreprise étrangère, l'institution financière doit faciliter le transit de ce paiement en mettant en place différents contrôles documentés pour autoriser les paiements, notamment en investiguant la disponibilité des fonds. Ce dispositif donne une apparence légitime à la transaction. Il s'agit d'une documentation très complexe, basée sur de nombreux contrôles, qui apporte une grande crédibilité. Or, la plupart des personnes chargées de rédiger ces documents manquent de vigilance à l'égard de certains indicateurs révélateurs de blanchiment de capitaux.

De la salle

Avez-vous été témoin de cas avérés de blanchiment dans les organisations caritatives, en particulier avec des dons en provenance de l'étranger ?

Manon ROY

Ces cas ont été surtout constatés pour le financement des activités terroristes. Les terroristes ont une vision différente des blanchisseurs de capitaux. Ces derniers visent l'accroissement de leur patrimoine, alors que les terroristes sont avant tout mus par une idéologie. Pour réaliser leurs actes, terroristes et blanchisseurs doivent accumuler des fonds de différentes origines. Mais alors que les fonds relatifs au blanchiment de capitaux proviennent en général du crime, au niveau du financement du terrorisme, le mouvement est plutôt contraire : souvent les fonds proviennent d'origine légale, donc d'individus ou de sociétés qui ignorent participer au cumul de fonds pour commettre des actes terroristes.

Les organisations caritatives mettent en place des levées de fonds permettant d'accumuler d'importantes sommes d'argent. Il est difficile pour les institutions financières de déceler les organisations légitimes de celles qui ne le sont pas. Certains indicateurs peuvent toutefois y contribuer. Ainsi, une organisation caritative accumulant des fonds de façon disproportionnée en comparaison avec les autres organisations du même secteur, serait susceptible d'éveiller des soupçons. Par ailleurs, les fonds restent immobilisés pendant un certain temps pour pouvoir servir le jour J de l'acte terroriste. Alors que dans le cas du blanchiment de capitaux, de très nombreux mouvements de fonds interviennent. Le nombre moindre de mouvements de fonds rassure souvent les personnes qui sont moins

familières avec le financement du terrorisme. Alors que le problème peut être tout aussi grave.

De la salle

Panama City comporte peut-être quatre fois le nombre de tours de la Défense. Ces immeubles sont appelés des « machines à laver ». Des investissements sont effectués dans l'immobilier, puis les loyers sont blanchis, puisqu'en réalité les tours ne sont pas occupées. Or, il ne semble pas que quiconque intervienne pour mettre un terme à cette situation.

Manon ROY

Effectivement, Panama est considéré comme un centre international de transit des fonds issus de la criminalité. Les criminels cherchent des opportunités non seulement pour blanchir des fonds issus du crime, mais aussi pour faire fructifier l'argent. L'immobilier prend un essor important à cet égard.

De la salle

Avez-vous vu dans votre activité, des opérations mobilières montées par des *Anstalt*, qui sont des fiducies suisses totalement opaques, légales en Suisse ?

Manon ROY

Je n'ai pas rencontré de telles organisations. Pourtant, la réglementation suisse a été largement renforcée. A une époque, la Suisse était traitée de « poubelle » de l'argent sale mondial. Depuis, elle a mis en œuvre des mesures très exigeantes pour faciliter l'identification des réels ayants droit des comptes bancaires. Malheureusement, en Suisse comme dans d'autres pays, certaines organisations permettent de dissimuler cela. Parfois même, des institutions financières sont détenues par des criminels. Avant de transmettre ses soupçons à Tracfin, une entité financière doit procéder à une pré validation, et mettre en lumière qu'il est difficile d'identifier la source des fonds ou les mouvements de fonds réguliers. Une telle difficulté suffit à exercer une vigilance accrue, voire même à décider de faire cesser une relation avec un client.

Il importe de mettre en place des mesures suffisantes pour démontrer la rigueur avec laquelle l'institution a voulu lutter contre le blanchiment de capitaux, pour démontrer que la lutte contre le blanchiment de capitaux fait partie des valeurs de l'organisation. Il est impossible de mettre en place des contrôles massifs pour lutter contre le blanchiment de capitaux. Un scandale pourrait surgir à tout moment. Vous vous souvenez sans doute de l'affaire Bouton avec la Société Générale il y a quelques années. Monsieur Bouton a été poursuivi car il était soupçonné d'avoir été au courant de transactions menées par des groupes criminalisés sans agir. Il risquait une peine d'emprisonnement. Il a finalement été blanchi.

Paul-Olivier GIBERT

Je vous remercie de nouveau pour cet exposé passionnant. J'invite à présent Cyril PIERRE-BEAUSSE à intervenir. Je le remercie d'être venu de loin pour venir nous parler de protection des données à caractère personnel. Cyril PIERRE-BEAUSSE est avocat au Barreau de Luxembourg. Il est le responsable de la ligne mondiale *Privacy* au sein d'Allen & Overy, célèbre cabinet anglo-saxon. Cyril nous présentera, avec une approche européenne globale, la réglementation relative à la protection des données à caractère personnel, qui, je ne dévoilerai pas un grand secret, est un sujet amené à profondément évoluer dans les trois à cinq années qui viennent.

La protection des données personnelles – Les textes réglementaires – Le projet de règlement communautaire

Cyril PIERRE-BEAUSSE
Avocat, Global Data Protection Leader, Allen & Overy

Mon approche sera avant tout communautaire, tout en sachant qu'il existe, de pays en pays, des variations liées aux transpositions des directives dans la loi locale, mais aussi aux interprétations des autorités de protection des données, comme la CNIL en France. Il m'a été demandé de vous entretenir de l'aspect lié à la protection des données de tous les traitements rendus obligatoires par les lois.

Ma présentation porte sur les obligations pesant sur les entreprises en matière de lutte contre le blanchiment de capitaux, contre le financement du terrorisme, éventuellement contre la fraude fiscale et la corruption. Le corps de règles en la matière tend à se développer et à s'harmoniser. Elles vont plus ou moins imposer les mêmes obligations aux entreprises. La première obligation est la collecte d'information, soit directement auprès de la personne concernée, soit auprès de tiers, soit au fur et à mesure des transactions qui surviennent. Il s'agit ensuite de conserver cette information, éventuellement de la mettre sous une forme spécifique en vue d'un *reporting,* et ensuite de la communiquer à une autorité, qui peut être locale ou étrangère, régionale ou internationale. Ainsi, les Etats-Unis imposent la collecte et la transmission d'informations, par exemple récemment avec la loi FATCA, qui fait l'objet d'un certain nombre de discussions. Dans ce cas, il s'agit d'un traitement requis, c'est-à-dire un traitement à laquelle l'entreprise est contrainte de participer. Ce traitement lui-même n'est pas exempt de l'application des règles en matière de protection des données.

Il convient d'abord de replacer la notion de protection des données dans son contexte. Historiquement, la protection des données constitue la première branche du droit de l'informatique. Dès que nous avons disposé d'un ordinateur, nous y avons placé des données personnelles. Après vingt ou trente ans, nous nous sommes aperçus que la possibilité donnée par les systèmes informatiques de traiter des données, de les interconnecter, de les transférer, de les manipuler, aboutissait à la remise en cause du principe de proportionnalité. En effet, lorsque nous étions dans le monde du papier, nous avions tendance à nous contenter du strict nécessaire pour procéder à des contrôles. Les systèmes informatiques rendant le contrôle plus facile, nous avons tendance à faire baisser le seuil de vigilance et à traiter les informations d'une manière beaucoup plus attentatoire aux droits et libertés fondamentaux des personnes concernées. Ainsi, dès les années 1970, une résolution du Conseil de l'Europe a recommandé à ses Etats membres de se doter d'une législation spécifique. La France a été le deuxième Etat dans le monde, en 1978, à se doter d'une législation spécifique, avec la Loi « informatique et libertés ». Cette législation existe toujours aujourd'hui, sous une forme profondément remaniée, après la directive 95/46/CE, qui est la directive fondamentale en matière de protection des données.

Cette directive a été transposée en droit français et a apporté une modification substantielle de la loi de 1978. Un projet de règlement communautaire est actuellement à l'étude. Il a été présenté publiquement en janvier 2012 et devrait aboutir d'ici trois ou quatre ans. La proposition est extraordinairement agressive et restrictive pour les entreprises consommatrices de données, et très protectrice des individus, ce qui annonce un lobbying intense au cours de sa procédure d'adoption. Nous allons assister, sans aucun doute, à une montée en puissance de la problématique des données personnelles au sein des entreprises.

Nous avons souvent tendance à considérer que la France est la seule à disposer d'une loi sur les données personnelles. Si elle est l'un des pionniers en la matière, les règles découlent d'une directive et s'appliquent dans l'ensemble des pays de l'Union européenne. Par ailleurs, un certain nombre d'Etats tiers se sont dotés d'une législation « *euro-compliant* », conforme aux standards communautaires, afin de protéger leurs propres ressortissants, mais aussi faciliter leur commerce avec l'Union Européenne, qui soumet le transfert de données hors de l'Union européenne à certaines restrictions.

De nombreux pays ne se sont pas encore dotés de législation. Certains se sont dotés de législations trop partielles pour permettre un flux libre de données, ce qui pose à la France un certain nombre de problèmes lorsqu'elle souhaite transférer des données à des autorités qui se situent dans ces pays.

La directive de 1995 et les lois existantes nous contraignent à opérer un changement de mentalité. Il est ainsi interdit, par principe, de traiter des données relatives à des personnes, car cela revient à empiéter sur leur vie privée, et est, par là-même, contraire à la convention de sauvegarde des droits de l'homme ainsi qu'à un certain nombre de dispositions nationales ou supranationales. Pour obtenir le droit de traiter les données personnelles, il convient de respecter les règles de la protection des données, et surtout savoir que ces règles s'imposent même si les traitements nous sont imposés par la loi ou demandés par les autorités. Les lois n'ont pas toujours été conçues pour fonctionner en cohérence les unes avec les autres. J'exerce à Luxembourg, et j'ai eu l'occasion de voir dans mon pays un certain nombre de cas dans lesquels une loi s'avère complètement contraire à une autre, par exemple la loi sur le secteur financier et la loi sur les données personnelles. Les autorités en charge de ces sujets au Luxembourg, l'équivalent de l'AMF et de la CNIL, non seulement ne s'entendent pas, mais se font des procès. Il ne faut donc attendre nulle tendresse et nulle compréhension du système. La loi sur la protection des données s'applique, en effet, même si l'entreprise se trouve dans l'obligation légale d'effectuer les traitements de données.

Dès lors, que doivent faire les entreprises par rapport aux règles sur la protection des données ?

Elles doivent d'abord respecter les grands principes de la protection des données. Ensuite, elles doivent respecter les droits des personnes concernées. Par ailleurs, elles doivent garantir la sécurité et la confidentialité des données. Enfin, elles doivent déclarer les traitements et obtenir des autorisations. La protection des données personnelles est souvent réduite à cette dernière étape. Si une entreprise ne respecte pas les trois premiers principes, elle peut aujourd'hui rencontrer des problèmes, et ces derniers n'iront que croissants dans l'optique du projet de règlement communautaire. Des amendes très importantes, atteignant jusqu'à 2 % du chiffre d'affaires mondial hors taxe, pourront en effet être prononcées, par exemple dans l'hypothèse d'une rupture de sécurité et de confidentialité des données.

I) Concepts

De nombreux concepts et acteurs entrent en jeu. Les entreprises doivent donc disposer d'une bonne grille de lecture pour analyser les obligations qui leur incombent. La loi sur les données personnelles définit un certain nombre de critères et porte sur tout traitement de données personnelles. Une donnée personnelle ne doit pas être confondue avec une donnée nominative. La directive et les lois qui en découlent s'intéressent également aux données relatives à une personne identifiable, directement ou indirectement par rapport à un numéro d'identification (numéro de sécurité sociale, plaque d'immatriculation, numéro de compte bancaire, adresse IP, etc.). Certaines autorités nationales de protection des données considèrent qu'une donnée personnelle existe, dès lors qu'il est possible de retrouver la trace d'un individu à partir d'une information collectée.

Lorsqu'une personne visite un site Internet, ce dernier peut collecter son adresse IP. Si le détenteur du site souhaite obtenir le nom de la personne détentrice de l'adresse IP, il va

se tourner vers le fournisseur d'accès Internet, qui lui, conformément à une autre directive, est tenu par une interdiction de fournir une information sur l'identité du détenteur de l'adresse IP. Certaines autorités de protection des données considèrent que la conservation de l'adresse IP relève déjà d'une collecte de données personnelles. La police peut venir saisir le fichier et remonter jusqu'à la personne concernée. Dès lors que quelqu'un est capable d'effectuer la traçabilité, la donnée n'est plus anonyme. La loi va donc très loin sur la définition de la donnée personnelle.

Enfin, la notion de traitement est extrêmement large. Elle est fixée par une liste non exhaustive de types d'opérations, comme collecte, enregistrement, conservation, adaptation. Le champ d'application de la loi est déjà très vaste.

Un traitement typique de données fait généralement intervenir deux à trois acteurs, en dehors de l'individu sur lequel portent les données. Le principal acteur est le responsable du traitement. C'est sur lui que pèse l'obligation de conformité à la loi. Il a pris l'initiative du traitement, il doit en déterminer les finalités et les moyens. Dès lors, il peut communiquer ces données à un sous-traitant, par exemple une entreprise qui édite les fiches de paie. L'entreprise effectue des traitements pour le compte de l'entreprise commanditaire, qui conserve la responsabilité du traitement. Ensuite, un destinataire peut intervenir. Ce dernier reçoit communication des données et les traite pour son propre compte. Il devient responsable d'un deuxième traitement, totalement distinct du premier traitement. La directive prévoit enfin qu'une autorité susceptible de recevoir communication de données personnelles dans le cadre d'une mission légale d'enquête ou de contrôle, n'est pas considérée comme destinataire.

Ainsi, si une banque communique des informations à l'AMF, qui est en train de mener une enquête, cette dernière n'est pas considérée comme destinataire. Toutes les règles applicables au fait de communiquer les données à un tiers ne s'appliquent donc pas. Cette exception légale relève en quelque sorte de la notion de force majeure. L'entreprise n'a pas le choix, elle doit fournir les informations à l'autorité. Or, ni la directive ni les lois nationales n'expliquent ce qu'est une autorité, et quelle est la limite, si les autorités locales sont les seules concernées, ou si la notion inclut d'autres autorités étrangères, de l'Union Européenne ou des Etats-Unis. De manière générale, les autorités de protection des données retiennent une approche relativement restrictive.

Il est donc très important de bien identifier le responsable. Il convient de se poser certaines questions pour déterminer si l'entité est responsable du traitement.

La première question a trait à l'acteur qui prend l'initiative du traitement, et les décisions correspondantes. Ainsi, si une société mère impose un traitement à une filiale, on pourrait considérer que la société mère est responsable du traitement. Ensuite, il est intéressant d'examiner à qui incombe l'obligation légale d'effectuer le traitement. Dès lors qu'une entreprise a une obligation légale de collecter des données, par exemple pour identifier un client ou effectuer un *reporting* en matière de lutte contre le blanchiment de capitaux, elle est responsable de sa mise en application.

Enfin, il convient de se demander qui est en relation contractuelle avec la personne concernée. Il s'agit d'autres critères de responsabilité du traitement.

Concernant l'application territoriale, la loi d'un Etat membre s'applique lorsque le responsable du traitement est situé dans cet Etat membre. Mais les situations peuvent être très complexes, dans des scénarios de groupes, présents dans différents Etats membres, avec des scénarios de coresponsabilité.

II) Traitement

Tout traitement de données, qu'il soit requis par la loi ou non, doit respecter un certain nombre de principes. L'un des principes importants est le principe de la qualité des données. Selon ce principe, la collecte des données doit respecter le principe d'une finalité particulière. Il s'agit donc de traiter des données pertinentes par rapport à un besoin.

Ensuite, il convient de collecter des données nécessaires pour permettre d'atteindre une finalité. Les données doivent être exactes, et si nécessaires, mises à jour. Enfin, elles ne doivent pas être conservées pour un délai plus long que la raison pour laquelle elles ont été collectées.

Le principe de légitimité est très important. Un traitement est légitime s'il correspond à l'un des cas d'ouverture suivants, prévus par la loi :

- Prouver que l'on a obtenu le consentement de la personne concernée ;
- Prouver que le traitement est nécessaire pour l'exécution d'un contrat ou de mesures précontractuelles prises à la demande de la personne concernée ;
- Prouver que le responsable du traitement est soumis à une obligation légale ;
- Prouver un intérêt public important ;
- Enfin, prouver l'intérêt légitime du responsable. Ce cas d'ouverture revient à établir une balance entre cet intérêt et les droits fondamentaux de la personne concernée.

Un certain nombre de traitements sont soumis à restrictions, comme le traitement du casier judiciaire. Dans un certain nombre de pays, il n'est pas possible de traiter des données judiciaires, sauf si la loi le prévoit expressément.

Paul-Olivier GIBERT

La loi de 1978 modifiée pose le principe d'une interdiction de tout traitement relatif aux infractions. Une interprétation du Conseil constitutionnel indique que cette formulation ne fait pas obstacle à la possibilité que détient toute personne morale de mettre en œuvre les traitements nécessaires à son propre contentieux.

Cyril PIERRE-BEAUSSE

Parmi les cas de légitimité, l'obligation légale s'applique à nos traitements requis de manière évidente. L'intérêt public important concerne davantage les autorités. Enfin, l'intérêt légitime du responsable pose autant de questions qu'il n'apporte de solutions.

L'obligation légale soulève la question de la loi recevable ou éligible pour créer une obligation légale d'exercer un traitement. Une loi étrangère d'application directe, comme la loi FATCA, peut-elle justifier qu'une entreprise française traite des données aux fins de satisfaire aux exigences du fisc américain ? A mon sens, il ne peut s'agir que d'une obligation légale nationale. Un certain nombre d'indices concourent à le démontrer.

Paul-Olivier GIBERT

Pouvez-vous préciser quelle est la loi FATCA ?

Cyril PIERRE-BEAUSSE

Il s'agit d'une loi américaine faisant obligation aux ressortissants américains de déclarer leurs avoirs à l'étranger, et, de la même manière, faisant obligation aux banques étrangères, de faire une déclaration aux autorités fiscales américaines au sujet des avoirs de citoyens américains qu'elles détiennent. Il s'agit d'une loi assez agressive. Un certain nombre de banques européennes ont cessé de servir des clients américains à cause de cette obligation. Il s'agit d'un cas typique de traitement requis, dans lequel des entreprises vont devoir traiter des données et en organiser le transfert vers les Etats-Unis.

Nous retenons, encore une fois, une interprétation restrictive de l'obligation légale : seule une loi française ou une loi qui aurait une application légale en France, peut justifier un traitement sur la base de l'obligation légale.

Le projet de règlement communautaire prévoyait un régime d'autorisation préalable, ici en France, de la CNIL, avant l'envoi de données à une autorité étrangère. Ce débat a eu lieu en réaction à la loi FATCA. L'idée est de bloquer tout transfert jusqu'à ce que les

autorités nationales aient pu, au cas par cas, donner une autorisation. Cette situation plaçait les entreprises entre le marteau et l'enclume. Ainsi, il m'est arrivé d'agir pour des banques ayant des litiges aux Etats-Unis. Le juge américain applique sa loi et se moque de savoir s'il existe une restriction empêchant une entreprise européenne de communiquer les informations. Les entreprises sont devenues l'enjeu de la guerre que se livrent les Etats-Unis et l'Union Européenne en termes d'impérialisme juridique. Beaucoup interprètent le retrait de cette disposition comme un recul de l'Union Européenne. Je parlerais plutôt de pragmatisme, parce que les entreprises se seraient retrouvées dans des situations impossibles.

Un autre principe essentiel du traitement des données a trait à la finalité. Le traitement des données doit être effectué pour une finalité, c'est-à-dire un but qui justifie le traitement. Toutes les finalités doivent être déterminées à l'avance et être légitimes, c'est-à-dire entrer dans les cas de figure listés précédemment. Un traitement de données personnelles ne doit pas être assimilé à une base de données ou à une application. Une base de données peut poursuivre plusieurs finalités différentes. Et plusieurs bases de données peuvent aussi ne concourir qu'à une seule finalité.

Toutes les finalités doivent être divulguées aux personnes concernées et à l'autorité de protection des données. Les données ne doivent pas être traitées ultérieurement de manière incompatible. La notion de « compatible » renvoie à ce à quoi la personne concernée peut raisonnablement s'attendre.

Le dernier principe, clef de voûte de tout le système, est la proportionnalité. Elle renvoie à l'analyse menée par le juge ou l'autorité de protection des données pour déterminer si les moyens de traitement mis en œuvre pour atteindre la finalité ne sont pas excessifs. Ils doivent être proportionnés et nécessaires. Par principe, toutes les finalités doivent être divulguées. Cela peut poser problème. Il existe une exception lorsque la loi le prévoit explicitement. Ainsi, certaines dispositions contraignent le responsable du traitement à une certaine discrétion, dans l'hypothèse d'une banque suspectant un cas de blanchiment de capitaux aux autorités. Mais l'obligation de discrétion ne s'applique que dès lors qu'une déclaration a été faite auprès de l'autorité. Il convient de distinguer l'utilisation de l'information en vue de respecter une obligation légale qui consiste à faire une déclaration de soupçons, et les autres obligations pesant sur l'entreprise, en tant que responsable d'un traitement, qui consiste à porter à la connaissance d'un client l'existence et les modalités de ce traitement. Il existe quand même une obligation d'information générale sur la mise en œuvre d'un traitement, par exemple aux fins de lutte contre le blanchiment, sauf si ce traitement est régi par une loi qui prévoit une exception spécifique. Mais la loi sur les données personnelles ne prévoit pas d'exception spécifique pour ce type de traitement.

Le premier droit de la personne concernée par le traitement est d'être informée de l'existence et des conditions du traitement. L'entreprise doit donc s'identifier, indiquer qu'elle collecte des données, préciser la liste exhaustive des finalités, y compris la lutte contre le blanchiment de capitaux, informer la personne concernée des catégories de destinataires des données. Ces derniers n'incluront pas les autorités françaises ou ayant compétence en France, et agissant dans le cadre d'une mission légale d'enquête ou de contrôle. Enfin, l'entreprise doit mentionner l'existence d'un droit d'accès et de rectification.

Dans la pratique, le consentement de la personne concernée n'est pas nécessaire pour procéder au traitement, lorsque l'hypothèse de légitimité est une obligation légale. Il existe des exceptions très limitées à ce droit à l'information. Elles sont essentiellement applicables aux autorités, plus qu'aux entreprises. Sauf si la loi dispense de cette obligation, l'entreprise doit informer les personnes au début de l'entrée en relation. La personne concernée a un droit d'accès et de rectification pour pouvoir obtenir des données dont l'entreprise dispose à son sujet. Là aussi, il existe des exceptions, de nouveau très limitées. Par principe, le droit d'accès est complet et intégral. Je recommande la prudence avant tout refus de communiquer ou tout délai avant de communiquer des informations. En effet, la plupart des législations nationales prévoient des sanctions pénales dans ce cas.

Il existe ensuite un droit d'opposition. La personne peut, dans certains cas, s'opposer à un traitement, pour des raisons prépondérantes et légitimes tenant à sa situation particulière. A mon sens, ce droit d'opposition est inenvisageable pour s'opposer à un traitement requis par la loi. Les personnes n'ont à mon avis pas d'autre choix que de se plier à ce traitement.

III) Divulgation

Dans notre scénario, le responsable du traitement obtient des informations, soit directement de la personne concernée, soit de sources externes. Il communiquera ensuite les informations à un destinataire, par exemple une autorité étrangère. Tout ceci se passe sous la surveillance de l'autorité de protection des données, la CNIL en France.

Par principe, lorsque l'on communique des données à un tiers, il convient d'en informer l'autorité de protection des données et d'informer la personne concernée de l'existence et des conditions du traitement. Dès lors que l'autorité de protection des données et la personne concernée sont informées que des données sont susceptibles d'être envoyées à des autorités locales ou étrangères, il n'existe pas d'autre restriction, sauf un éventuel secret professionnel. La démarche est donc relativement simple.

Comme indiqué précédemment, il n'est pas nécessaire de fournir cette information si on communique les informations à une autorité intervenant dans le cadre d'une mission légale d'enquête ou de contrôle.

Dans le cas où l'on communique des données à une autorité ne bénéficiant pas de cette exemption de qualification de destinataire, comme par exemple une autorité étrangère, il faudra se soumettre à une obligation d'information préalable. Dès lors que les notifications sont effectuées, il est possible de communiquer directement une déclaration de soupçons. La mise en conformité est initiale. Dans l'hypothèse où une autorité française compétente demande des informations, ces dernières peuvent être communiquées directement et de manière totalement libre. De manière générale, rien ne permet aux entreprises de s'opposer à une communication des données à une autorité.

Enfin, très peu de pays dans le monde disposent d'une législation présumée conforme aux standards communautaires. Il n'existe ainsi aucune restriction au transfert de données vers les autorités d'un petit nombre de pays : Ile de Man, Norvège, Iles Féroé, Islande, Israël, Liechtenstein, Jersey, Guernesey, Andorre et l'Argentine. En revanche, les Etats-Unis ne figurent pas sur cette liste. Nous ne pouvons communiquer des informations aux Etats-Unis aux entreprises listées sur le *Safe Harbor*. Hormis ces quelques pays, l'hypothèse globale est donc la restriction des transferts.

Il existe toutefois des exceptions. Il est possible de transférer des données vers un pays qui n'a pas un niveau de protection des données équivalent aux standards communautaires, si la personne a donné son consentement, si ce transfert est nécessaire pour exécuter le contrat avec la personne concernée, s'il est nécessaire pour signer un contrat avec un tiers, dans l'intérêt de la personne concernée. Les autres cas justifiant une exception sont l'intérêt vital, l'intérêt public important, la constatation, l'exercice ou la défense d'un droit en justice, le transfert depuis un registre public ou l'existence de clauses contractuelles avec le destinataire.

En réalité, la seule possibilité restante est le consentement de la personne concernée. Nous nous trouvons donc dans une hypothèse où nous aurons besoin du consentement de la personne concernée. Nous pourrions nous baser sur la deuxième hypothèse, à savoir la nécessité du transfert de données pour l'exécution d'un contrat avec la personne concernée. Ainsi, une banque offrant un service à un citoyen américain doit fournir des informations au fisc américain dans le cadre de la loi FATCA. Or, depuis le début de mon exposé, je vous indique que nous ne considérons comme éligibles que les autorités locales. Si on considérait qu'une autorité hors Union européenne pouvait exiger un transfert de données, cela signifierait que l'on reconnaît une forme de compétence à cette

autorité. Or, les entreprises n'ont pas d'obligation légale de se conformer aux exigences d'une autorité étrangère.

IV)Perspectives

Contrairement à une directive, qui fixe des orientations et laisse une marge de manœuvre aux Etats, le projet actuel est un règlement communautaire, d'application directe dans les Etats membres. Cela réduit le champ d'interprétation de chaque Etat et fait progresser l'harmonisation.

En outre, le projet de règlement prévoit des règles beaucoup plus complexes et sévères. Les données personnelles sont amenées à devenir une matière à laquelle s'intéressent les membres des Conseils d'administration. Aujourd'hui, seul le service juridique s'intéresse à cette matière. Généralement, ces questions n'intéressent pas vraiment le top management. Les dispositions vont être calquées sur les dispositions existantes en matière de lutte contre la concurrence déloyale, avec la mise en place d'amendes d'ordre, prononcées par les autorités administratives, dont le montant pourra atteindre 2 % du chiffre d'affaires mondial hors taxes.

La notion de *compliance* en matière de données personnelles va donc devenir un sujet majeur pour les entreprises. Le projet de règlement communautaire modifiera notamment les exigences en matière de consentement. Ce dernier devra être explicite. Aujourd'hui, on peut se contenter d'un consentement implicite. La mise en conformité concrète du consentement explicite est complexe. La charge de la preuve incombera toujours au responsable du traitement. Le projet de règlement prévoit que le consentement d'un employé ou d'un administré sera sans valeur.

Ces règles poseront un certain nombre de problèmes. Elles requerront la mise en place de procédures permettant de documenter le consentement, de le recueillir de manière explicite. Or, certaines autorités de protection des données considèrent que le consentement explicite ne peut être obtenu par le biais d'une adhésion à des conditions générales. Un véritable consentement explicite séparé sera exigé.

Concernant la demande d'accès des autorités étrangères, comme je vous l'ai indiqué, cette disposition a été annulée. Aujourd'hui, nous sommes libres, moyennant notification à l'autorité de protection des données et information de la personne concernée, de communiquer des données à des autorités étrangères. Le législateur communautaire avait envisagé la mise en place d'une obligation d'obtenir une autorisation préalable, qui, à ce stade, semble être annulée.

En conclusion, de manière générale, la loi sur la protection des données s'applique à tous les traitements. Elle n'a pas pour effet de les bloquer. En d'autres termes, elle ne donne pas une bonne excuse pour ne pas s'y conformer. De ce fait, des difficultés surgissent lorsque nous sommes confrontés à des autorités étrangères agressives. Ainsi, les Etats-Unis ne disposent pas d'une loi globale en matière de protection des données personnelles. Ils sont donc généralement assez peu compréhensifs à l'égard de ces dispositions. Sur le fond, rien n'empêche l'Union Européenne de se conformer à une requête provenant d'une autorité étrangère sur le fondement de la loi sur la protection des données, à l'exception des restrictions aux transferts hors Union Européenne. Il s'agit donc d'une difficulté. Les entreprises peuvent contourner toutes ces difficultés en les prenant en compte en amont, et en ayant, dès le début de la relation client, sollicité un consentement pour communiquer les données en dehors de l'Union Européenne, en ayant informé la CNIL et les personnes concernées. Ce faisant, elles éliminent les obstacles existant en matière de protection des données pour communiquer ces informations.

L'approche à retenir en matière de conformité revient à effectuer une analyse régulière de tous les traitements. La plupart des entreprises effectuent des traitements qui évoluent dans le temps. Les obligations légales évoluent elles-mêmes dans le temps. Le travail doit donc être recommencé régulièrement. J'invite les entreprises à mener ce travail.

Ensuite, il convient de désigner un correspondant interne, chargé de la protection des données. Le projet de règlement communautaire rendra ceci obligatoire pour les entreprises de plus de 250 employés. Dans mon expérience, les anciens auditeurs internes deviennent souvent chargés de la protection des données.

Par ailleurs, il convient de penser en termes de « *privacy-by-design* », notion qui sera reprise dans le projet de règlement communautaire, c'est-à-dire de prévoir les problèmes en amont.

Enfin, il est nécessaire de conserver une approche risque. Aucune entreprise n'est 100 % conforme à la loi. Avec des lois si techniques et si complexes, cela est virtuellement impossible. C'est pourquoi, il faut conserver l'approche risque, revenant à éliminer les principaux risques par rapport aux buts que l'on s'est fixé.

De la salle

Au regard de la nécessité de recueillir l'assentiment de la personne concernée, le « nuage », ou « *cloud computing* » introduit-il des difficultés particulières ?

Cyril PIERRE-BEAUSSE

Un *cloud computing* est, en toute hypothèse, un sous-traitant, qui stocke les données. Dès lors, il existe une relation de responsable du traitement à sous-traitant.

Dans certains cas, des entreprises placent volontairement des données dans un pays, avec un dispositif de type *cloud*, pour que les autorités locales puissent effectuer une saisie sur place et avoir accès aux données. Dans ce cas, les entreprises peuvent nier toute responsabilité et affirmer qu'il s'agit d'un cas de force majeure.

Certaines autorités de protection des données laissent faire cela avec une certaine complaisance. Ainsi, en matière de données de trafic de télécommunications, certains pays veulent avoir accès à toutes les données relatives à des conversations téléphoniques ayant lieu sur leur territoire. Si le système ne prévoit pas de stockage des données, ils demandent la mise en place d'un serveur sur le territoire avec la complicité de l'autorité de protection des données étrangère. Quoi qu'il en soit, le responsable du traitement est toujours responsable de garantir la sécurité et la confidentialité des données. Cette problématique est prégnante au niveau du *cloud*.

De la salle

Pouvez-vous nous donner quelques précisions sur la protection des données des salariés dits « sensibles », notamment les syndicats ?

Cyril PIERRE-BEAUSSE

Les données relatives à l'appartenance syndicale sont considérées comme des données sensibles, que l'entreprise ne peut pas collecter et traiter dans n'importe quel cas de figure. Elle peut toutefois le faire sur la base d'une obligation découlant du droit du travail, liée par exemple à l'organisation d'élections.

Paul-Olivier GIBERT

En vertu de la loi « informatique et libertés », l'appartenance syndicale est une information sensible et personnelle, qui ne doit pas faire l'objet d'un traitement. En revanche, l'entreprise est tenue par une obligation de se doter d'une représentation syndicale et de lui donner un certain nombre de moyens. Il convient donc de gérer ces deux règles. D'expérience, dans ce type de problématiques, le droit du travail prévaut. Autrement dit, l'entreprise se doit de mettre en place les dispositifs nécessaires à l'exercice des libertés syndicales. Les références à la loi « informatique et libertés » interviennent ainsi en mode mineur.

Ces éléments répondent-ils à votre question ?

De la salle

Ma question porte aussi sur les aspects techniques. Ainsi, un salarié peut être amené à utiliser son poste de téléphone dans le cadre de son engagement syndical. Comment les entreprises peuvent-elles résoudre cette difficulté ?

Paul-Olivier GIBERT

Il faut revenir aux textes. En principe, un délégué syndical exerce ses fonctions de délégué syndical sur des heures de délégation. Son activité syndicale s'exerce dans le local syndical mis à disposition par l'employeur. Toutefois, dans la pratique, cela se passe rarement ainsi. Le délégué syndical travaille à partir de son poste de travail. Dans une certaine mesure, il le fait à ses risques et périls. Il existe parfois, et c'est préférable, un accord d'entreprise définissant les moyens mis à disposition des délégués syndicaux pour exercer leur mandat.

Au-delà du téléphone professionnel, l'utilisation de la messagerie ou le droit de tracter sont également réglementés. Normalement, ce droit s'exerce à l'extérieur de l'entreprise. Mais certaines entreprises tolèrent qu'il s'exerce à l'intérieur. Le droit du travail prévaut. Le pilote doit être plutôt du côté de la direction des ressources humaines, quitte à agir en étroite coopération avec la personne en charge de la protection des données à caractère personnel.

De la salle

Pouvez-vous nous dire quelques mots sur la collecte de données des clients sur les réseaux sociaux ?

Cyril PIERRE-BEAUSSE

Une jurisprudence commence à émerger à ce sujet dans la plupart des pays de l'Union Européenne. Selon la tendance qui se dégage, dès lors qu'une donnée est accessible publiquement sur un mur Facebook, sans qu'il soit nécessaire d'être « ami » avec la personne, elle relève d'une information publique. A ce titre, elle est donc susceptible d'être collectée et utilisée. Dès lors que l'accès aux informations est restreint par la nécessité d'être « ami », ces informations sont considérées comme équivalentes à une correspondance. Par conséquent, le secret s'applique.

Paul-Olivier GIBERT

Des personnes ont été licenciées au motif que sur leur mur Facebook, elles avaient critiqué un collaborateur. Cette information avait été relevée et utilisée contre elles comme étant licite. Le problème provient du fait que beaucoup de personnes ne maîtrisent pas le paramétrage de Facebook. Elles croient parler avec trois ou quatre amis, alors que potentiellement, les deux milliards de personnes ayant accès à Internet peuvent prendre connaissance de ces propos. Le droit général sur la prise de parole en public s'applique sur Internet.

Par ailleurs, il est possible de réutiliser les données publiées sur les réseaux sociaux, avec une limite. Ces sujets en sont encore au stade de la R&D. La situation est tout à fait nouvelle et pose deux questions. La première question consiste à savoir si la réglementation actuellement applicable aux données à caractère personnel est totalement pertinente pour encadrer les « objets » que sont les réseaux sociaux. Certains éléments militent en faveur d'une réponse positive, dans la mesure où il existe des sociétés qui administrent le réseau social. En contrepartie de la mise à disposition d'un espace de stockage, ces sociétés s'octroient un certain nombre de droits. La charge de travail que représenterait la lecture de la totalité des conditions générales d'utilisation des réseaux sociaux est estimée à environ une vingtaine de jours. Autrement dit, personne ne les connaît, et signe les yeux fermés dans une logique de contrat d'adhésion.

La loi de 1978 et la directive de 1995 répondent à une logique dans laquelle un tiers utilise une partie des données personnelles pour un objet déterminé. Les données personnelles étaient comparables à une voiture que l'on confie à un garagiste. Ce dernier en a les clefs, il peut la réparer. Mais il ne partira pas en week-end avec la voiture. Aujourd'hui, avec les réseaux sociaux, la situation est plutôt celle d'une personne qui se retrouve avec sa voiture sur un circuit. Il utilise ses propres données et les communique. On peut donc se demander si la réglementation issue des textes du milieu des années 1970 est adaptée à ce type d'objet, qui est tout à fait nouveau.

Cyril PIERRE-BEAUSSE

Pour moi, dès lors qu'une collecte d'information est effectuée par l'entreprise, cette dernière en devient responsable. Toutes les dispositions de la loi continuent donc à s'appliquer aux informations importées. La connaissance seule de l'information n'est pas encore considérée comme un acte de traitement. En revanche, remplir le dossier d'un employé avec des mentions que ce dernier a placées sur son Facebook ou son LinkedIn relève d'un acte de traitement. Or, si un acte de traitement est posé, la loi s'applique. L'information de la personne n'aura pas été collectée directement, mais obtenue via un tiers, à savoir Internet. En tout cas, la personne concernée ne l'aura pas transmise en connaissance de cause. Dans ce cas, l'entreprise est tenue par l'obligation d'informer la personne de l'existence du traitement et de lui communiquer les catégories de données obtenues. Si l'employé est curieux et s'enquiert des sources des données, l'entreprise aura l'obligation de les lui communiquer. Certes, l'information est publique, il est donc possible de l'utiliser. Pour autant, cela ne donne pas le droit de s'en servir en échappant à la loi. Il est toujours nécessaire de tenir compte de la finalité de la collecte des informations. Le *data mining* doit toujours pouvoir être justifié, car il comporte des risques de déviance.

Paul-Olivier GIBERT

A mon sens, le point fait débat. C'est parce que quelqu'un a donné des informations à son sujet que ces dernières sont publiques, et que l'entreprise peut les utiliser de manière légitime pour son activité. Le sujet est donc encore très sensible.

Mettre en place des dispositifs de protection des droits et libertés des personnes

Paul-Olivier GIBERT

Directeur associé R2M-Partners, CIL, Président de l'Association Française des Correspondants aux Données Personnelles

Actuellement, il existe d'un côté une réglementation complexe, qui fixe des comportements interdits et un certain nombre de comportements obligatoires. Ces comportements sont basés sur des principes d'évaluation des risques, de proportionnalité, de pertinence, qui requièrent une adaptation des diligences mises en œuvre aux caractéristiques propres de l'entreprise. Ces obligations réglementaires comportent un risque d'image. Ainsi, la CNIL a émis récemment une délibération motivée au sujet d'un organisme de logement social, qui contrevenait à la loi « Informatique et libertés ». L'entreprise a réagi, a fait faire un audit qui a été publié sur Internet. Il comporte le recueil de toutes les actions qui n'auraient pas dû être menées par l'entreprise, qui a servi de base à un dispositif de protection.

La loi « Informatique et libertés » et les obligations de lutte contre le blanchiment de capitaux, contre le terrorisme ou contre la corruption mettent en tension l'ensemble de l'entreprise. Avec le nouveau règlement européen, les entreprises devront être totalement impliquées. La question ne restera pas un problème à gérer au sein de la direction juridique, ou en termes d'organisation ou de processus. Désormais, la totalité de l'entreprise sera mise sous tension, du Conseil d'administration au sous-traitant, avec en plus une vision assez large. Ce qui est vrai pour le blanchiment l'est également pour la protection des données à caractère personnel.

La finalité des dispositifs mis en place par l'organisation ne doit pas être perdue de vue. Les organisations qui entrent dans une logique de formalisation très forte de leur activité aboutissent à une logique de formalisation qui génère un travail à part entière, et au final, elles font du formalisme pour faire du formalisme, sans véritablement rentrer dans la réalité du métier. Si l'on veut protéger l'entreprise contre les risques liés aux atteintes portées aux droits et libertés des personnes, il faut oublier cela. C'est sur les dossiers concrets que le problème pourra se manifester.

L'entreprise doit prendre un certain nombre de dispositions pour intégrer le sujet dans la culture et le référentiel de l'entreprise. Il n'est pas simple aujourd'hui pour une entreprise de connaître les obligations à laquelle elle est soumise dans son activité. D'un côté, il lui est demandé de surveiller, pour éviter qu'un certain nombre de manquements ne surviennent. D'un autre côté, elle doit respecter les droits et libertés des personnes. Elle est toujours confrontée à cette dualité. En France, à ce jour, nous n'avons pas encore assisté à un procès entre la CNIL et le régulateur bancaire. Mais les négociations sont parfois délicates. Le cadre français s'efforce de trouver un mi-chemin raisonnable entre ces différents impératifs.

Il importe également de savoir qu'il faut mettre en place des processus. Un travail doit être mené pour assurer ce respect. Dans l'animation de ce processus, il convient qu'une personne soit en mesure de porter un regard distancié et expert sur ce qui est mis en œuvre par l'entreprise, par exemple en matière de lutte contre la corruption, en matière de protection des droits et libertés des personnes, ou en matière de lutte contre le blanchiment de capitaux. Cela peut relever de la fonction de *compliance*, à savoir une logique de regard permanent pour s'assurer que les dispositifs sont équilibrés par rapport aux obligations parfois contradictoires que l'entreprise doit mettre en œuvre.

Le système de communication et de mise à disposition de ces différents dispositifs requiert le plus grand pragmatisme, en fonction du schéma de fonctionnement de l'entreprise. Certaines entreprises sont dotées de démarches qualité ou de contrôle interne très structurées. D'autres ont des modes de fonctionnement beaucoup plus informels, où les réseaux personnels sont importants. Il conviendra de recourir à des actions de sensibilisation, de formation, d'explication auprès des principaux relais d'opinions au sein de l'organisation. Une approche purement formaliste peut apparaître inefficace, voire contre-productive.

De la salle

Lorsqu'un salarié quitte l'entreprise, il laisse un certain nombre de fichiers personnels, comme les carnets d'adresse ou les mails. Les collaborateurs ont souvent besoin de consulter ses mails. Ont-ils le droit de le faire ou convient-il de tout détruire au moment du départ ? Existe-t-il une jurisprudence en la matière ?

Paul-Olivier GIBERT

Il existe des éléments de jurisprudence à ce sujet. Certaines organisations, mais trop rarement, mettent également en place des règles en matière de gestion des départs. En théorie, le salarié quittant l'entreprise devrait laisser les mails qu'il a reçus à titre professionnel à l'entreprise, et récupérer les mails reçus à titre personnel. Il en va de même pour ses fichiers. Dans la pratique, la distinction n'est pas aisée. En outre, les fichiers supprimés sont parfois restaurés par les sauvegardes automatiques des systèmes informatiques de l'entreprise. Il existe donc un risque. La jurisprudence sur le contrôle des salariés oscille entre deux pôles : la protection d'un espace de vie privée quasi indestructible au sein de l'entreprise et le devoir de contrôle de l'employeur, qui fournit des moyens à l'employé pour qu'il travaille. L'entreprise doit jouer entre les deux, n'intervenir que pour un besoin très identifié, en étant très vigilante à respecter ce qui apparaît *a priori* comme personnel.

Cyril PIERRE-BEAUSSE

En droit luxembourgeois, le Code du commerce prévoit une obligation de conserver les correspondances entrantes et une copie de toutes les correspondances sortantes. Cette règle est analysée comme s'appliquant à l'Email, considéré comme une correspondance. Nous conseillons à nos clients d'organiser leur système informatique de manière à ce que tout Email entrant et une copie de tout Email sortant soient stockés, pour faire face à l'obligation de documenter un cas précis, et ce sur une période de dix ans, qui correspond à la prescription de droit commun en matière commerciale. Concernant le tri des mails privés et professionnels, mon analyse personnelle est que, sauf s'il existe un moyen simple d'y procéder, il s'agit d'une procédure assez dangereuse et contre-productive, revenant à entrer davantage dans la vie privée des employés. La plupart des entreprises procèdent à des stocks sans regarder les informations ayant un caractère privé.

Paul-Olivier GIBERT

Dans la pratique, le problème devrait décroître en raison du développement des Smartphones. En effet, il y a dix ans, un ordinateur était nécessaire pour accéder à sa messagerie. Aujourd'hui, la plupart des personnes ont accès en permanence à leurs messageries sur leur téléphone.

De la salle

Comme vous le savez, les personnes assujetties doivent se mettre en conformité avec l'autorisation unique AU-003 au plus tard le 7 juillet 2012. Je souhaiterais savoir quelle articulation doit être faite entre cette autorisation et les textes réglementaires sur la lutte anti-blanchiment. Nous sommes notamment soumis à une obligation d'échange d'information sur les clients à l'intérieur du groupe. L'Autorité de Contrôle Prudentiel (ACP)

a précisé ce contenu. Comment cette obligation s'articule-t-elle dans le cas de clients communs ? Un chargé de clientèle d'une direction A disposant d'informations sur un client peut-il transmettre à un homologue d'une direction B les informations préalablement collectées pour un même client commun ?

Paul-Olivier GIBERT

L'autorisation unique prévoit la communication d'informations autour des besoins de traitement de la déclaration. Elle prévoit également l'utilisation ou la réutilisation des données collectées dans le cadre des traitements ou de la collecte d'information anti-blanchiment à des fins de gestion de la relation bancaire. Je persiste à dire qu'il est nécessaire de préciser de quelles activités il s'agit, de quelle manière la personne est connue par la gestion privée et par le département Entreprise.

La communication entre chargés de clientèle renvoie à une finalité annexe tolérée par l'utilisation unique de la CNIL, qui prend un risque de dérive.

La lutte contre la corruption : quelles perspectives ?

Dominique LAMOUREUX
Directeur Ethique et Responsabilité d'Entreprise, Thales

Bonjour à tous. Je suis, au sein du groupe Thales, Directeur de l'Ethique et de la Responsabilité d'Entreprise, notamment chargé des questions liées à la prévention de la corruption. Comme vous le savez, Thales est un leader mondial dans les domaines de la défense, de la sécurité, de l'espace, de l'aéronautique comme du transport terrestre. Son chiffre d'affaires s'élève à 13 milliards d'euros, avec plus de 67 000 salariés, présents dans une cinquantaine de pays...

Depuis une dizaine d'années, j'ai participé à la mise en place des dispositifs de prévention de la corruption, dans un secteur industriel particulièrement concerné par ce sujet et je suis très honoré de pouvoir partager avec vous cette expérience.

Mon exposé sera complété cet après-midi par l'intervention de Madame ROY et de Monsieur DARBO.

Il faut constater que la plupart des entreprises sont de plus en plus sensibilisées sur les risques pénaux, mais aussi sur les effets négatifs en termes d'image et de notoriété en cas de non-respect des lois anti-corruption. Les acteurs économiques sont, en effet, confrontés à un environnement réglementaire de plus en plus contraignant et exigeant, au niveau national et international. Par ailleurs, s'ajoutent à ces législations de multiples référentiels, dictés non seulement par les organisations internationales (ONU, OCDE, etc.), mais également par des organisations non gouvernementales ou encore les associations professionnelles.

Dans cet esprit, on peut citer le récent *UK Bribery Act* qui, non seulement fixe les sanctions en cas de corruption, mais oblige les entreprises à prévenir les risques de "pot-de-vin" grâce à la mise en place volontaire de "*adequate procedures"*.

Enfin, les mécanismes de contrôle sont de plus en plus efficaces, avec une transparence accrue dans la façon dont l'entreprise conduit ses activités alors que de nombreux dysfonctionnements rendent légitimes les exigences éthiques des diverses parties prenantes. Récemment encore, certaines entreprises semblaient avoir comme principe "*Don't get caught"*, c'est-à-dire "faites ce que vous voulez, à condition de ne pas vous faire attraper". Cette époque me semble largement révolue.

Les entreprises, même dans le secteur de la défense intimement lié à la souveraineté nationale, sont de plus en plus mondialisées. Dans ce contexte, une prétendue protection des administrations nationales au nom d'un pseudo-patriotisme n'a plus cours. Aujourd'hui, le Politique et l'Etat sont très attentifs à une opinion publique qui ne tolère plus la corruption et ses "rétro-commissions". Tous ces éléments conduisent au développement d'un nouveau paradigme de gouvernance.

Pour répondre à ces exigences réglementaires contraignantes, et sans entrer dans trop de détails, je résumerai les principaux dispositifs mis en place par les entreprises pour prévenir la corruption.

Le principe de base est l'affirmation de la tolérance zéro à l'égard de tout acte de corruption, exprimé au plus haut niveau de la hiérarchie, a priori, par le Président de l'entreprise.

Il s'agit ensuite de mettre en place une organisation et des ressources adaptées, avec des moyens suffisants. Il convient aussi de se doter de procédures rigoureuses intégrées dans l'ensemble des processus opérationnels de l'entreprise. Il importe, en parallèle, de

mettre en place un système de droit d'alerte - ou *Whistleblowing* - même s'il me semble que ce droit ne doit être utilisé que lorsque tous les autres dispositifs de *reporting* n'ont pas fonctionné.

Bien entendu, l'information et la sensibilisation des collaborateurs sont absolument critiques. Par exemple, chez Thales, nous avons formé plus de 2 000 collaborateurs entre 2001 et 2003 et avons lancé - depuis 2 ans - une nouvelle campagne de formation qui a touché 5 000 collaborateurs.

Il importe d'effectuer régulièrement une cartographie des risques, afin de mettre en place les dispositifs les plus adaptés aux activités, aux marchés, en lien avec l'environnement commercial de la société. Enfin, un système d'audit et de contrôle internes performant est fondamental.

Pour conclure, il est essentiel que toutes ces mesures s'inscrivent dans un cercle permanent d'amélioration des pratiques.

Les dispositifs mis en place doivent être fondés sur des principes communs :

- Conformité aux législations internationales et nationales ;
- Identification et qualification des risques mais aussi vérifications préalables (*due diligence)* ;
- Proportionnalité des dispositifs de prévention au regard des niveaux de risques ;
- Procédures d'escalade pour arbitrage en présence de risques résiduels ;
- Sollicitation de la hiérarchie et/ou d'un référent local en cas de doute ;
- Dissociation des rôles et responsabilités avec recours à des structures expérimentées et expertes ;
- Transparence et traçabilité ;
- Et surtout responsabilité, rigueur, professionnalisme et intégrité.

Il est assez habituel, dans le commerce international, de recourir à des agents ou intermédiaires, rémunérés par un "*success fee*" si l'affaire est remportée. Le Président de Thales, M. Luc VIGNERON, a pris la décision, à son arrivée, de supprimer ces agents. Pour maintenir sa présence sur ses marchés export, le Groupe a alors choisi de mettre en place un nouveau *business model* qui s'appuie sur des partenariats industriels - structurant à long terme - noués avec des entreprises locales. Si ces partenariats ne peuvent pas être conclus, Thales se retire éventuellement du pays, notamment lorsque la corruption y est endémique. La répartition géographique du chiffre d'affaires du Groupe a ainsi profondément changé au cours de ces dernières années.

En revanche, il est essentiel que ces règles rigoureuses et ces contraintes fortes soient partagées par tous les concurrents. Thales a donc été très actif pour créer, au sein de son secteur industriel, un "*level playing field"*. Les distorsions de concurrence ne sont pas tolérables et les mêmes législations et règles du commerce doivent être respectées par tous les agents économiques, dans chaque pays exportateur. Ainsi, le secteur de l'aéronautique, de l'espace et de la défense a développé une démarche proactive dans cet esprit.

Les premières discussions ont eu lieu en 2002 entre BAe Systems, Dassault, EADS et Thales. Parallèlement, un dialogue régulier a été initié avec Transparency International, l'ONG qui lutte contre la corruption. En 2006, un Comité Anti-Corruption a été créé au sein de l'association européenne (l'ASD). En 2007, ont été rédigés les *Common Industry Standards*, qui fixent les mesures pertinentes et nécessaires pour prévenir la corruption. Ces standards ont été adoptés par plus de 400 entreprises européennes du secteur.

Ces *Common Industry Standards* ont donné lieu, de manière inédite, à un échange des "meilleures pratiques", entre concurrents, sur un sujet considéré jusqu'alors comme tabou. Un document a été élaboré collectivement, préconisant un engagement très strict de tolérance zéro, des procédures détaillées et des actions de formation des collaborateurs. Ces procédures sont particulièrement adaptées aux PME, mettant à leur disposition une "boîte à outils" avec des formulaires et des questionnaires préparés. Ces *Common Industry Standards* sont enfin régulièrement mis à jour pour tenir compte des évolutions réglementaires.

Il a ensuite été décidé d'internationaliser cette initiative européenne, d'abord avec les Etats-Unis. L'objectif est de démontrer que l'ensemble des grandes entreprises du secteur respecte des standards éthiques rigoureux au niveau mondial. Il convient donc de contraindre tous les pays exportateurs à adopter les mêmes standards, et d'obtenir en parallèle que les donneurs d'ordre sélectionnent exclusivement les entreprises ayant adopté des règles éthiques strictes.

Nous avons travaillé sur une première série d'engagements dès 2009, portant sur la tolérance zéro en matière de corruption, l'emploi de consultants, la gestion des conflits d'intérêts, mais aussi le respect de la confidentialité des informations. Nous sommes en train de faire évoluer ces *Global Principles of Business Ethics*.

Nous avons également décidé de créer l'*International Forum on Business Ethical Conduct* (IFBEC). Le premier s'est réuni à Berlin en 2010 et a rassemblé 60 participants, représentant non seulement les industries européennes et américaines, mais aussi japonaises et australiennes, ainsi que nos "parties prenantes" majeures, à savoir les institutionnels, comme l'OTAN, l'OCDE, l'Agence européenne de Défense, mais aussi les ONG comme *Transparency International.* Ce rassemblement a permis un échange sur les bonnes pratiques et les attentes de l'ensemble des acteurs.

Cette initiative a été institutionnalisée, l'année dernière, avec la définition d'une Charte, la nomination d'un Président et la mise en place d'une "*Task Force"* dotée de moyens humains et financiers. En même temps, dans l'esprit d'une démarche de progrès continu, un second forum s'est réuni à Washington en 2011. Afin de contribuer à un processus de "*outreach",* des sociétés brésiliennes, canadiennes, etc. ont été invitées, à se joindre à nous, dans l'optique de développer un standard véritablement mondial sur les bonnes pratiques en matière de lutte contre la corruption. Le prochain forum aura lieu en septembre prochain en Espagne.

Il s'agit d'une initiative originale d'autorégulation d'un secteur industriel en liaison avec la société civile et les clients.

Par ailleurs, il nous a semblé nécessaire d'aller au-delà de cette initiative qui ne s'impose qu'aux entreprises. Il est, en effet, important de rappeler que la corruption est l'œuvre de deux acteurs : celui qui donne, mais aussi celui qui reçoit et exige. Or, aucune initiative efficace n'a encore été prise pour combattre ce dernier phénomène. Cette corruption - dite "passive" - ne fait aujourd'hui l'objet d'aucune condamnation tant soit peu exemplaire. Certes, il existe bien une Convention, dite de Merida ou UNCAC (*United Nations Convention Against Corruption*), mais celle-ci n'est pas effectivement mise en œuvre, en l'absence d'une gouvernance mondiale.

Nous avons donc décidé de mener cette action dans le cadre du "Business 20" ou "B20", qui accompagne le G20. Notre objectif est de faire dire aux 20 premières puissances mondiales que si les principales entreprises des pays occidentaux se sont mises en conformité avec la loi, la corruption semble bien rester endémique. Les entreprises sont, en vérité, les otages de leurs clients. Il faut sortir d'une idée fausse qui voudrait que les entreprises soient les méchants corrupteurs. En vérité, les entreprises sont à la merci de décideurs publics et de fonctionnaires, qui exigent, en toute impunité, la part d'un butin qu'ils estiment avoir le droit de s'arroger.

Lors du Sommet de Cannes, en novembre 2011, les entreprises ont donc, pour la première fois, demander aux gouvernements de combattre la corruption passive mais

aussi d'accroître la transparence dans les marchés publics et l'intégrité dans les financements internationaux. Les Etats doivent reconnaître et soutenir les entreprises intègres qui ont mis en place des programmes de conformité sérieux. Ils doivent les encourager, en réservant les appels d'offres publics aux industriels qui ont pris des engagements d'intégrité et participent à des initiatives sectorielles. Tel est le message que nous avons porté à cette occasion.

L'initiative "RESIST" constitue une autre forme de démarche proactive. Il s'agit d'une démarche responsable, initiée par *l'International Chamber of Commerce* (ICC) avec le soutien de *Transparency International*, du *Global Compact* de l'ONU et du *World Economic Forum*. Le document "RESIST", construit à partir de cas réels, consiste à mettre à la disposition des collaborateurs des entreprises un outil pratique sur "Comment résister à l'extorsion et la sollicitation dans les transactions internationales". Le document est traduit en six langues et appartient désormais au domaine public. Il fera bientôt l'objet d'une formation en e-learning.

Pour conclure, je souhaiterai aborder un dernier point. Les entreprises en vue d'améliorer leur dispositif de prévention de la corruption, sont confrontées à une réflexion managériale pour savoir si elles ne doivent pas passer d'une *rule-based approach* à une *value-based approach*. Cela signifie passer de la simple conformité - avec des processus prédéfinis - à une appropriation des enjeux par chaque salarié, s'appuyant sur des comportements responsables. Le tout répressif rencontrant des limites évidentes, il importe que chaque collaborateur de l'entreprise devienne le vecteur et l'acteur de la conformité et de l'éthique. Les seules procédures ou référentiels sont insuffisants, comme l'a montré l'affaire Kerviel. A l'inverse, une approche *bottom-up* peut développer une nouvelle culture et des comportements adaptés et pertinents chez les collaborateurs. Il convient de mettre d'abord l'accent sur la responsabilisation dans une démarche construite autour d'un échange permanent des meilleures pratiques.

Je terminerai en citant une très belle phrase de Jean-Baptiste Say : « *Si l'on veut que telle manière d'être, telle habitude de vie s'établisse, la dernière chose à faire est d'ordonner que l'on s'y conforme. Voulez-vous être obéi ? Il ne faut pas vouloir qu'on fasse : il faut faire qu'on veuille* ».

De la salle

Toutes ces initiatives, pour l'instant limitées au secteur de la défense, l'un des secteurs cibles de la corruption, seront-elles amenées à se répandre dans d'autres secteurs, comme la pharmacie, le nucléaire ou autre ?

Dominique LAMOUREUX

Des initiatives majeures ont été également lancées dans le secteur des industries extractives. Nous sommes aussi en contact avec le secteur des travaux publics, ainsi qu'avec celui du médicament. Ce type d'échanges se développe régulièrement. Les entreprises doivent être mues par un intérêt concret, et pas simplement par la peur de sanctions. Dix ans se sont écoulés entre les premières prises de contact et les réalisations d'aujourd'hui. Il faut laisser un peu de temps au temps.

Paul-Olivier GIBERT

Vous avez engagé des discussions entre concurrents pour établir des standards anti-corruption. Avez-vous rencontré des difficultés en matière de concurrence ? Avez-vous mené des démarches spécifiques pour expliquer le sens de vos actions ?

Dominique LAMOUREUX

Nous avons été très sensibles à ces questions, en nous entourant de juristes compétents. Nous en avons notamment tenu compte dans la formulation des *Common Industry Standards*.

Paul-Olivier GIBERT

Cela signifie que nous sommes vraiment dans un contexte où les injonctions paradoxales surviennent de toutes parts.

De la salle

Quelle a été l'évolution du chiffre d'affaires de Thales au cours des dix dernières années ?

Dominique LAMOUREUX

Le chiffre d'affaires de Thales est en croissance régulière, bien que nous traversions une crise économique et que les budgets de la défense sont en contraction.

Certes, nous perdons quelques affaires (généralement portant sur des montants limités) mais il faut être conscient que nous améliorons considérablement notre notoriété auprès des grands donneurs d'ordre internationaux.

L'enjeu est selon moi de trouver une troisième voie entre le *soft power* et le *hard power*, à savoir le *smart power*. Ce dernier consiste à développer de nouvelles stratégies d'influence. Il s'agit de mettre en place une intelligence collective au sein de l'entreprise mais aussi entre entreprises comme avec les administrations nationales, pour développer de nouveaux moyens d'approche des clients, afin de les convaincre de notre excellence et maintenir notre leadership et notre compétitivité, sans obérer notre intégrité.

De la salle

Nous parlons essentiellement de la corruption. Or, l'actualité en matière de concurrence est assez forte, avec l'autorité française qui attend que les entreprises mettent en place des programmes de mise en conformité. Nous assistons donc à une multiplication des textes de référence au sein des entreprises. Comment faites-vous pour « hiérarchiser » en quelque sorte les différentes règles, et faire en sorte que les opérationnels sachent quelle est la règle à suivre ? N'en ressort-il pas des incohérences ?

Dominique LAMOUREUX

En effet, nous sommes confrontés à une multiplication de réglementations dans de très nombreux domaines. En ce qui concerne la corruption, nous avons décidé d'élaborer notre propre corpus de règles et de directives, dans le cadre d'une initiative globale. Nous veillons, par ailleurs, à être à l'écoute des signaux faibles, afin de faire évoluer nos procédures internes en fonction des nouvelles normes émergentes. Et en s'assurant que nos collaborateurs puissent s'approprier intelligemment ces règles.

Paul-Olivier GIBERT

Vous parlez de hiérarchisation entre différentes règles. La hiérarchie des normes ne prévoit pas la supériorité du droit de la concurrence sur le code pénal pour ce qui relève des dispositions relatives à la corruption. Le problème provient de l'éclatement des sources de normes, qui contraignent l'entreprise à placer le curseur elle-même. Ainsi, la lutte contre la corruption donne lieu à des rencontres entre professionnels d'un même secteur. Si ces dernières se font de manière transparente et claire, cela ne soulèvera pas de problème. En d'autres termes, les équipes juridiques de l'entreprise doivent mener un travail important pour synthétiser les différentes obligations de l'entreprise, en tenant compte des spécificités du secteur d'activité de l'entreprise. Cela relève du service *Compliance*, en relation avec le management et les fonctions juridiques. Par ailleurs, il convient d'adapter le cadre de référence à chaque fonction dans l'entreprise. Ainsi, un commercial doit apporter des contrats. Il faut lui fournir un cadre avec des repères à cet effet. Ce travail mobilise toute l'entreprise.

De la salle

En tant qu'auditeur interne certifié, je souscris totalement à vos propos. Mais je souhaiterais savoir si vous avez une visibilité sur l'activité des grandes entreprises de pays émergents qui deviennent internationales, que ce soit lorsqu'elles exportent ou lorsqu'elles ont pris des parts dans des sociétés installées en Europe.

Par ailleurs, vous avez évoqué un travail mené sur les dix dernières années. Peut-on s'attendre à une démarche similaire sur le domaine des droits de l'homme ?

Dominique LAMOUREUX

Nos concurrents des pays émergents, comme les BRICS, ne sont soumis à peu sinon à aucune contrainte en matière de lutte contre la corruption. Ces entreprises dépendent de législations nationales peu contraignantes, avec des pouvoirs publics qui ont peu de scrupules, non seulement en matière de corruption, mais également sur le plan environnemental, social, sociétal. Nous ne devons avoir aucune naïveté à cet égard.

De la salle

Les entreprises de pays émergents adhérant à une logique anti-corruption ne risquent-elles pas de se mettre en situation de très grande fragilité, avec ce que cela implique en termes d'emploi pour les pays où elles se trouvent ?

Dominique LAMOUREUX

C'est absolument évident. Il nous revient de le dénoncer auprès des Nations Unies, de l'OCDE, des grands donneurs d'ordre, tel que l'OTAN ou l'Agence Européenne de Défense. Il est inadmissible que des entreprises qui ne respectent pas les mêmes contraintes se trouvent à égalité dans un appel d'offres. Le G20 a repris cette question dans ses déclarations de 2011. Nous sommes dans un environnement compétitif très défavorable.

Concernant la question sur les droits de l'Homme, nous commençons à nous poser très sérieusement ces questions dans notre secteur. Le sujet ne concerne pas seulement les armes, mais également les technologies de surveillance et de sécurité, qui, lorsqu'elles sont utilisées sans contrôle, pourraient porter atteintes à certains droits fondamentaux.

Pour mémoire, Il existe une interdiction totale de vendre des armes. Nous ne pouvons exporter qu'avec des dérogations, prises au plus haut niveau de l'Etat, par une commission interministérielle présidée par le Premier ministre. La décision revient donc au Politique en la matière. En revanche, nous développons des activités civiles, qui peuvent porter atteinte aux droits de l'Homme. Nous sommes donc en train de lancer des initiatives pour y réfléchir. Certains secteurs sont plus en avance que nous en la matière. Je suis convaincu que les droits de l'Homme vont devenir une question cruciale pour les entreprises dans les dix années qui viennent. Comme sur la corruption, nous cherchons à mener le même type de démarche responsable.

Ouverture de l'après-midi

Christiane LEGAT
Directrice de l'Audit interne, Corporate Finance Bank, Groupe General Electric

J'ai l'honneur de présider les interventions de l'après-midi, dans le cadre de notre journée de travail sur les questions liées au blanchiment de capitaux. Les différentes étapes de l'après-midi seront les suivantes. Dans un premier temps, Manon ROY, que vous avez déjà entendue ce matin, et Nicolas DARBO traiteront le sujet « développer et optimiser ses systèmes de lutte contre la corruption, contre le blanchiment et le financement du terrorisme ». Dans un deuxième temps, Marie-Agnès NICOLET nous rejoindra pour nous parler du règlement bancaire 97-02 de la troisième directive et des projets de quatrième directive sur la lutte anti-blanchiment et le financement du terrorisme. Elle évoquera également les lignes directrices qui complètent ce dispositif. Après une pause, le thème « Comment développer une approche proportionnelle et équilibrée de la lutte contre la corruption, le blanchiment et le financement du terrorisme » fera l'objet d'une table ronde animée par Blandine CORDIER-PALASSE. Enfin, Philippe MONTIGNY clôturera nos travaux sur le thème « La conformité : entre loi et éthique ».

Je cède à présent la parole à Manon ROY et Nicolas DARBO qui, après avoir exercé différentes responsabilités de direction au sein de groupes financiers et bancaires, est associé au Cabinet Accuracy France.

Développer ou optimiser ses systèmes de lutte contre la corruption, contre le blanchiment et le financement du terrorisme

Manon ROY
Vice-Présidente, Accuracy Canada

Nicolas DARBO
Associé, responsable de l'expertise dédiée aux institutions financières, Accuracy France

Manon ROY

Bonjour à nouveau. Nous allons d'abord traiter le volet de lutte contre la corruption, qui sera complémentaire à ce que je vous ai présenté ce matin. Mon collègue poursuivra sur le volet spécifique du blanchiment de capitaux.

I) Secteur industrie, commerce et services : corruption dans le cadre d'un processus d'appel d'offres

1) Distinction entre fraude et corruption

La corruption est un acte visant à influencer ou abuser d'une autorité publique par l'octroi ou l'acceptation d'une situation ou d'une récompense illicite en échange d'un avantage personnel ou privé indu.

Au contraire, la fraude est un acte caractérisé par une présentation inexacte délibérée de faits et/ou d'informations importantes pour obtenir un avantage financier indu ou illicite. Elle peut être interne, c'est-à-dire émaner de l'intérieur de l'organisation, ou externe, c'est-à-dire impliquer des clients, des fournisseurs ou d'autres tiers.

Nous sommes appelés à mener des investigations sur chacun de ces cas. Nous retraçons des informations dans des registres comptables pour mener l'enquête. Au niveau de la corruption, il existe rarement des informations en interne, puisque les transactions sont souvent effectuées hors registre comptable. Pour la fraude, nous trouvons plus fréquemment des informations dans les registres comptables.

2) L'intégrité

L'intégrité renvoie aux conditions de l'utilisation des fonds, des ressources, des actifs et des pouvoirs conformément à leur intention officielle et à l'intérêt général. La corruption et les différents types de fraudes sont tout à fait le contraire de l'intégrité.

3) L'affaire Siemens

Le groupe Siemens a dû payer une pénalité d'un montant total d'1,6 milliard de dollars en Allemagne et aux Etats-Unis, pour des faits qui se sont déroulés entre 2002 et 2006. Le budget annuel du groupe de corruption dédié à l'unité télécommunication s'élevait entre 40 et 50 millions de dollars par an. L'objectif était de conserver la compétitivité et de développer des marchés face à la concurrence.

L'entreprise a fait appel à des consultants externes pour aider à gagner des soumissions. Ces consultants étaient des résidents locaux. Des honoraires étaient versés

au consultant, qui lui était lié aux personnes en autorité et pouvait leur transférer l'argent pour obtenir des contrats très importants. Parmi les pots de vin ainsi versés, cinq millions de dollars ont été payés au Bangladesh pour obtenir des contrats téléphoniques, 40 millions de dollars en Argentine pour produire des cartes d'identité, etc.

Je vais à présent vous montrer un court extrait vidéo, avec le témoignage du comptable qui a mis en œuvre les processus pour faciliter ces paiements.

La vidéo est diffusée.

Nous avons déjà eu plusieurs échanges interactifs ce matin au sujet du blanchiment de capitaux. Je suis curieuse d'entendre vos réactions au sujet de cet extrait.

De la salle

Ce témoignage souligne le danger d'un intérêt supérieur de l'entreprise, qui donne l'impression qu'il est nécessaire de tout faire pour sauver l'entreprise.

De la salle

Il met également en évidence l'absence de contrôle croisé, c'est-à-dire que cet homme agissait seul sans contrôle émanant d'une personne n'ayant aucun lien hiérarchique avec lui. Or, il s'agit du meilleur moyen d'éviter ce genre de dérive. Cela permet de relativiser les démarches menées dans d'autres départements et de s'apercevoir d'une anomalie. Toutefois, si le *top management* autorise ces pratiques, il est très difficile de mordre la main qui vous nourrit.

Manon ROY

Prenons le cas théorique d'une entreprise soumise à une concurrence féroce, qui aimerait pouvoir conquérir de nouveaux marchés pour conserver sa santé financière et ses emplois. Un haut dirigeant a-t-il avantage à parler de pots-de-vin officiellement ? Non, bien évidemment. Il existe une sorte de zone grise. Lorsque nous menons des investigations, nous nous trouvons face à des situations contrastées. Certaines personnes ont suivi la façon de faire, par crainte de perdre leur emploi. D'autres ont eu le sentiment qu'il était nécessaire d'aider l'organisation à maintenir sa place sur un marché concurrentiel, où tous les concurrents agissent de la même façon.

4) Bonnes pratiques pour les contrôles internes, la déontologie et la conformité (OCDE)

Parmi les bonnes pratiques en matière de contrôle interne, de déontologie et de conformité, il est envisagé de créer une entité chargée de lutter contre la corruption, similaire aux agents de conformité qui aident les entités à lutter contre le blanchiment de capitaux. L'importance d'un soutien par les plus hautes instances de l'entreprise est soulignée. Par ailleurs, il est essentiel pour l'entreprise d'afficher une politique interne claire, se traduisant par l'absence de contradiction entre une éventuelle charte et la réalité de ce qui est demandé aux salariés dans leurs méthodes de travail, leurs résultats et leur manière d'atteindre les résultats.

Si vous étiez investigateur, quels seraient les postes les plus à risques au sein de la comptabilité des entreprises, pouvant témoigner d'actes de corruption ? En réalité, les montages sont ingénieux, et tous les postes sont concernés. Il convient donc de raisonner par comparaison et de mener une approche globale. Certains postes standards, comme la traduction, permettent parfois d'identifier des paiements problématiques dans certaines entreprises. Parfois, il convient de se mettre dans la peau d'un individu souhaitant dissimuler de telles transactions, pour déceler les éventuelles incohérences. Cela peut se faire manuellement, en analysant des postes ayant varié de manière inexpliquée, soit grâce à des outils de forage informatiques, en lançant des requêtes multiples sur des postes, des périodes, des intervenants. Dans les grandes entreprises, l'émission de

rapports périodiques constitue une manière optimale de mener une veille. Il est nécessaire d'établir clairement les responsabilités de chaque intervenant au sein de l'organisation. Enfin, l'évaluation des risques doit tenir compte des circonstances particulières de l'entreprise.

Je mène régulièrement des investigations financières en entreprise. Les personnes avec lesquelles je travaille au sein des entreprises sont la plupart du temps extrêmement honnêtes. Leur talon d'Achille est de ne pas voir la criminalité autour d'eux et de ne pas disposer de paradigmes sur l'efficacité des contrôles mis en œuvre. Les gens qui ont l'esprit tordu sont au contraire très créatifs et trouvent des façons de contourner les contrôles pour arriver à leurs fins. Quand les auditeurs internes interviennent, les travaux sont beaucoup plus efficaces que lorsque ce sont des personnes qui ne connaissent que les aspects théoriques de ces problématiques.

Les bonnes pratiques portent aussi sur la prévention et la détection avec les intermédiaires, l'importance d'une *due diligence* fondée sur les risques, ainsi que des communications et des formations périodiques. Il importe également de fournir un soutien continu et de susciter la conviction, afin que les signalements soient efficaces.

5) Contrôles et audits internes : assurer l'intégrité et la responsabilité du secteur public (OCDE)

L'OCDE a publié, en avril 2011, un rapport intitulé « Contrôles et audits internes : assurer l'intégrité et la responsabilité du secteur public ». Une étude a été réalisée auprès de douze pays, dans 73 ministères dont la France faisait partie. L'étude montre que le rattachement hiérarchique de l'audit interne est de très haut niveau en France. Il a été demandé aux différents pays quelles mesures ont été mises en place pour prévenir la corruption dans les transactions financières et renforcer la résistance à la corruption. Les réponses apportées ont évoqué la séparation des demandes et des autorisations de paiement, mais aussi les procédures électroniques d'examen ou d'approbation des paiements, la séparation de la réception et de la vérification des biens services, ou encore la rotation périodique des agents.

L'audit interne porte davantage sur la fraude que sur la corruption. Ainsi, 51 % des ministères interrogés ont mentionné que leur mandat faisait référence à la fraude. Seuls 37 % ont un mandat faisant référence à la corruption. Les enjeux de la corruption requièrent beaucoup de ressources, d'énergie et de spécialisation. Le questionnaire a demandé aux ministères si les mesures anti-corruption mises en place sont suffisantes. En France, 75 % des ministères ont répondu positivement. Pour 86 % des ministères interrogés, les auditeurs internes doivent être dotés de qualifications particulières.

6) Les 4 grands axes des principes visant à renforcer l'intégrité dans les marchés publics (OCDE)

Le dernier rapport de l'OCDE traite des quatre grands axes importants pour renforcer l'intégrité des marchés publics. Ces quatre axes se déclinent en dix grands principes :

a) Axe A : transparence

1. Instaurer un degré de transparence adéquat à toutes les étapes du cycle, afin d'assurer un traitement juste et équitable des fournisseurs potentiels ;

2. S'efforcer d'assurer une transparence maximale dans les appels d'offres et prendre des mesures de précaution pour renforcer l'intégrité, en particulier en cas de dérogation aux règles d'appel à la concurrence ;

b) Axe B : bonne gestion

3. S'assurer, lors de la passation de marchés, que l'usage des deniers publics est conforme à leur intention ;

4. S'assurer que les fonctionnaires chargés de la passation des marchés publics satisfont à des normes professionnelles élevées en termes de savoir, de compétence et d'intégrité ;

c) Prévention des comportements réprouvés et respect des règles de surveillance

5. Mettre en place des mécanismes destinés à prévenir les risques pesant sur l'intégrité dans les marchés publics ;

6. Encourager une coopération étroite entre les pouvoirs publics et le secteur privé pour préserver des normes d'intégrité élevées, en particulier dans la gestion des contrats ;

7. Prévoir des mécanismes spécifiques pour surveiller les marchés publics ainsi que déceler les comportements réprouvés et les sanctionner ;

d) Obligation de rendre compte et contrôle

8. Définir clairement la chaîne de responsabilité et mettre en place des mécanismes de contrôle efficaces ;

9. Traiter les réclamations des fournisseurs potentiels de manière équitable et dans les délais prévus ;

10. Permettre aux organisations de la société civile, aux médias et au grand public de suivre de près la passation des marchés publics.

7) La cartographie des risques

Il importe d'analyser la situation à l'aide d'une cartographie des risques, en amont, lorsque l'on prévoit le processus d'appel d'offres, et en aval, au niveau de l'attribution des contrats et des paiements.

Il n'est pas toujours facile de mener des contrôles efficaces, lorsqu'une situation résulte d'un enchevêtrement complexe de plusieurs éléments.

Au Québec, plusieurs enquêtes sont en cours. Tout le système de lutte contre la corruption est considéré comme insuffisant et devant être renforcé. Il en va de toute la réputation du pays, mais aussi de ses entreprises. Notre rôle est d'aider les organisations à mettre en place non seulement des mesures de contrôle, mais aussi de suivre la trace de l'argent. Une importante commission d'enquête est en cours sur la corruption dans l'industrie de la construction. Ces entreprises auraient obtenu plusieurs contrats avec le gouvernement québécois depuis plusieurs années, à travers une collusion avec les fournisseurs. Nous verrons si des fonctionnaires ont effectivement utilisé leur situation pour favoriser certains fournisseurs.

En conclusion, l'enquête sur Siemens a été effectuée par une équipe allemande et américaine. Siemens a souhaité faire maison nette et s'assurer que toutes les problématiques avaient été soulevées. Ils ont embauché différents spécialistes. Ainsi, 300 avocats, analystes et juricomptables ont effectué 1 700 auditions auprès d'intervenants internes et externes. Ces enquêtes ont coûté au total un milliard de dollars.

II) Secteur financier : blanchiment de capitaux relatif aux produits/services de la Banque

Nicolas DARBO

Bonjour à tous. L'ACP vient de publier un rapport sur le domaine de la gestion de fortune. Il me semble intéressant de vous présenter les enjeux et les risques identifiés par l'ACP dans son rapport, autour des quatre thématiques suivantes.

1) La place dans la gouvernance d'un groupe

Les mesures de lutte contre le blanchiment de capitaux s'inscrivent dans le pilotage d'un groupe. Si elles ne viennent pas d'en haut et ne sont pas placées dans les priorités par le management du groupe, elles auront peu d'impact. Elles nécessitent une adaptation au contexte local. Étant donné la taille des grands groupes aujourd'hui, elles ne peuvent provenir que du niveau central. Elles doivent relever d'une action coordonnée des fonctions centrales d'une holding et des différentes filiales et entités régionales. L'entreprise mère assure la cohérence. Enfin, Les organes exécutifs et délibérants du groupe dépendent de la qualité de l'échange d'informations intragroupe.

S'agissant des risques en matière de gouvernance, les dispositifs locaux peuvent être lacunaires, notamment lorsque l'implémentation et le suivi de ces dispositifs sont délégués par les organes centraux. Par ailleurs, l'information peut être difficile en l'absence de procédures et d'outils d'information efficients.

2) La cartographie des risques

La cartographie des risques est nécessaire. Dans cette cartographie, les risques doivent être classés sur la base de critères pertinents, afférant aux spécificités des activités, des clients, des implantations et des risques dans l'activité de gestion de fortune. Un profil de risque doit être élaboré pour chaque relation d'affaire, en fonction duquel des mesures de vigilance adaptées sont attribuées.

Les risques relèvent d'abord d'une cartographie non mise à jour. Ils peuvent provenir d'une omission d'informations ou du manque d'informations disponibles. Enfin, il est parfois difficile de trouver les modalités de détermination des clients présentant un risque élevé.

3) Les dispositifs d'alerte

En matière de vigilance, la lutte contre le blanchiment de capitaux passe par l'élaboration de procédures internes opérationnelles et adaptées aux situations rencontrées. Ces procédures doivent être à disposition des collaborateurs. Les clients doivent être systématiquement identifiés, leur identité vérifiée et leurs dossiers tenus à jour. Des dispositifs de surveillance sont mis en place sur les relations d'affaire et les opérations en espèces.

En matière de contrôle, il convient de mettre en place des dispositifs adaptés, à la fois de manière permanente et périodique.

Les risques sur les procédures de vigilance ont trait à des procédures inefficaces ou non mises à jour. Les procédures doivent rester adaptées à la réalité. Un autre risque provient de l'insuffisance de la documentation utilisée dans les analyses, ou des justificatifs conservés en cas d'examen approfondi. Les risques peuvent aussi résulter d'erreurs dans la base de données du groupe. Enfin, le dispositif peut être affaibli par l'absence d'implication du chargé d'affaires. Ce dernier doit être au cœur du dispositif et faire remonter les informations.

Sur les dispositifs de contrôle, les risques peuvent résulter d'un manque de moyens humains et techniques. L'insuffisance du contrôle permanent est un risque important, de même qu'un manque de profondeur des contrôles périodiques.

4) Les plans d'actions mis en œuvre

La déclaration de soupçons doit être effectuée auprès de Tracfin dans des délais raisonnables. Le groupe doit détecter les personnes ou entités sujettes à une mesure de gel de fonds et être capable d'en geler automatiquement l'ensemble de leurs avoirs. Il convient enfin de dispenser des formations opérationnelles et adaptées aux personnels concernés.

Les risques relatifs à la déclaration de soupçons proviennent de l'absence d'obligation légale de déclarer à Tracfin les clients qui se sont vu refuser l'entrée en affaires. Par ailleurs, l'automatisation des déclarations de soupçon risque d'aboutir à une non-détection du blanchiment sur des opérations atypiques. Enfin, la durée de déclaration est parfois trop longue.

Concernant le gel des avoirs, les délais de traitement sont longs, et les personnes faisant l'objet de gel de leurs avoirs usent de modifications orthographiques de leurs noms qui ne sont pas systématiquement détectées.

Enfin, concernant la formation, le périmètre des formations n'est pas toujours pertinent, les formations sont parfois trop généralistes. Elles manquent souvent d'un suivi.

Manon ROY

Le rapport soulève un grand nombre de problématiques, pour un secteur particulier, qui est celui de la gestion de fortune. En tant qu'auditeurs internes, quelles mesures recommanderiez-vous de mettre en place ?

Nicolas DARBO

Il convient de bien déterminer les processus et les sous-processus, et ne pas perdre de vue les risques Bâle II. Il convient également de faire preuve de pragmatisme et de partager la cartographie avec les opérationnels.

Manon ROY

Les institutions financières que nous avons approchées avaient toutes les qualifications nécessaires pour effectuer une cartographie optimale des risques. Mais dans les faits, elles n'avaient pas toujours les ressources suffisantes pour vaincre le blanchiment d'argent, qui ne porte pas à conséquence pour l'organisation au niveau financier, au contraire de la fraude. Par ailleurs, comme vous l'avez souligné, il importe de travailler avec les opérationnels, qui connaissent bien le terrain, mais pas forcément les risques relatifs au blanchiment de capitaux.

De la salle

Vous insistez beaucoup sur les ressources nécessaires pour la mise en place d'un dispositif sûr et fiable. Existe-t-il des standards ou des *guidelines* en termes de ratio d'effectifs participant à la lutte contre le blanchiment ?

Manon ROY

Il n'existe pas de tels ratios à ma connaissance. On parle en général de « ressources suffisantes ». Dans les faits, il s'agit d'une réelle problématique, du moins au Canada.

Christiane LEGAT

Pour vous donner un élément de réponse, l'ACP recommande un ratio de l'ordre de 1 % du total de l'effectif d'auditeurs internes. Elle se réserve à tout instant de recommander une augmentation de ce pourcentage en fonction de la nature des risques portés par l'établissement.

Nicolas DARBO

J'ajouterais que l'ACP ne se prive pas de faire des remarques explicites dans ses rapports de suite, recommandant sur le recrutement d'auditeurs internes ou la nomination de responsables de conformité.

Par rapport au risque lié à la déclaration de soupçons, l'ACP exige ce type de déclarations, mais il faut savoir que Tracfin les refuse. Il les accepte mais ne peut rien en faire tant qu'elles sont hors opérations, hors flux.

Manon ROY

Le système de déclaration canadien est un peu différent. Il n'est pas nécessaire d'investiguer un cas de soupçon avant de le transmettre à l'autorité. Je comprends que Tracfin ne souhaite pas être envahi par des informations qui ne sont pas bien documentées, car son action est limitée.

Nicolas DARBO

Selon la directive, la déclaration ne constitue pas une obligation à proprement parler. Il convient de se poser la question de la nécessité de déclarer. Certains établissements procèdent à des déclarations lorsqu'ils détectent, par exemple, de faux documents d'identité.

De la salle

Pour l'utilisation de documents faux, la saisine de Tracfin n'est pas indispensable. Cela relève d'un délit pénal. Il convient de saisir la police ou la gendarmerie.

Manon ROY

Le gouvernement américain s'est mis à imposer des sanctions de plus en plus importantes aux institutions financières ne se conformant pas à toutes les obligations législatives et réglementaires. En 2007, la banque Amex a fait l'objet d'une inspection ayant détecté la non-transmission de déclarations de soupçons. La banque a été obligée d'embaucher des consultants pour reconstituer la trace des transactions effectuées au cours des années précédentes et identifier les déclarations qui auraient dû être transmises. Il s'est agi du premier cas de pénalités importantes décidées. D'autres cas s'en sont suivis. Plus récemment, la banque JP Morgan a dû payer une pénalité de 88 millions de dollars. Les actionnaires de l'entreprise ont décidé de poursuivre ses dirigeants pour ne pas avoir mis en place des mesures de prévention.

Christiane LEGAT

Monsieur DARBO, vous parlez de profils de risques et de modalités de détermination des clients présentant un risque élevé. Pouvez-vous nous donner quelques clefs pour combiner ces deux aspects ? Est-ce à dire que vous ne considérez que les clients à profil de risque élevé ?

Nicolas DARBO

Il convient de connaître quelques éléments clefs sur le patrimoine financier des clients, comme la localisation du patrimoine, les revenus. Ces informations permettent d'identifier quelques profils types, qui présentent un risque plus élevé.

Manon ROY

Il convient de sensibiliser les employés, pour leur dire de ne pas prendre pour acquis que les personnes avec qui ils ont une relation privilégiée sont hors de tout soupçon. Ils doivent rester en veille.

Nicolas DARBO

Cela est d'autant plus vrai que parmi les personnes fortunées, les personnes honnêtes et les autres présentent des caractéristiques communes. Ils font tous appel à force conseillers juridiques, fiscaux, financiers. Ils ont également tendance à fréquenter les mêmes lieux, à savoir les paradis fiscaux, donc nous avons peu parlé aujourd'hui.

Manon ROY

En effet, ils sont assistés d'une équipe d'intervenants pour ficeler les différents stratagèmes. L'important est de protéger votre entité. Il s'agit de pouvoir démontrer, en cas de survenue d'un scandale, qu'un programme raisonnable a été mis en place.

Christiane LEGAT

L'exercice d'un jugement critique permanent constitue également une clef de la détection. L'accroissement du rythme de *turnover* facilitera également la détection.

De la salle

Vous évoquez l'accélération du rythme de *turnover* des équipes pour détecter des cas de corruption. Toutefois, un certain temps est nécessaire pour que les équipes connaissent l'entreprise ou l'institution en profondeur. Comment gérez-vous ce dilemme ?

Manon ROY

A mon humble avis, dans la pratique, il convient de mettre en place un juste équilibre au sein des équipes, assorti d'une supervision adéquate. Les employés doivent en effet acquérir une connaissance suffisante pour bien identifier les situations. Malheureusement, dans certains cas, des personnes en interne sont en collusion avec les criminels, de façon consciente ou inconsciente, par négligence.

Nicolas DARBO

Il importe d'embaucher des opérationnels, d'identifier des personnes dont le profil est déjà adapté, ce qui permet de gagner du temps. A leur arrivée, elles ont juste à acquérir des connaissances complémentaires.

La rotation du personnel est à relativiser en raison de la complexité des opérations à traiter. Statistiquement, les opérations sont normées, relativement habituelles dans les banques. Il importe surtout de suivre si certains clients suivent leur chargé de clientèle.

Christiane LEGAT

La mise en place de *back ups* est extrêmement importante. La même personne ne doit pas vérifier les états chaque jour. Si une opération malencontreuse survient, une autre personne devrait pouvoir la détecter le jour suivant, à tout le moins poser la question.

Je remercie vivement Manon ROY et Nicolas DARBO pour la clarté et la pertinence de leurs exposés. Je souhaiterais à présent ouvrir le deuxième temps de l'après-midi, où nous allons parler du règlement 97-02, de la troisième directive européenne et du projet de quatrième directive relative à la lutte contre le blanchiment et contre le financement du terrorisme. Nous évoquerons également les lignes directrices qui complètent ce dispositif.

Je remercie Madame Marie-Agnès NICOLET, présidente du Cabinet Regulation Partners, d'avoir accepté d'intervenir aujourd'hui dans un délai très court.

Lutte anti-blanchiment : quelles évolutions ?

Marie-Agnès NICOLET
Présidente du Cabinet Regulation Partners

Nous venons d'évoquer la lutte contre le blanchiment. L'objectif de mon exposé est de vous présenter les éléments les plus récents. Au-delà de l'ordonnance de 2009 et de ses décrets d'application, l'ACP a faculté de publier des principes sectoriels et des lignes directrices. Ces derniers donnent des précisions sur certains points de la réglementation, dans un cadre où des évolutions sont à venir, notamment avec une quatrième directive amenée à sortir prochainement.

Comme vous le savez, l'ordonnance transposant la troisième directive de 2005 a été adoptée en janvier 2009. Un certain nombre de décrets ont suivi. Par ailleurs, des modifications du règlement général de l'AMF sont intervenues. Parallèlement, des éléments ont été adoptés en matière de classification des risques de blanchiment dans le règlement 97-02.

Le délit général de blanchiment englobe aujourd'hui les infractions résultant de la fraude fiscale, notamment de toute opération dont « les sommes proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an, ou qui participe au financement du terrorisme ». C'est donc assez large. C'est pourquoi l'un des décrets parus en 2009 énumère les situations relatives à de potentiels cas de fraude fiscale nécessitant une déclaration de soupçon. Ces situations sont les suivantes :

- Utilisation de sociétés écrans dont l'activité n'est pas cohérente avec l'objet social, ou ayant leur siège social dans un Etat ou territoire qui n'a pas conclu avec la France une convention fiscale qui permette l'accès aux informations bancaires, identifié à partir d'une liste publiée par l'administration fiscale ;
- Réalisation d'opérations financières par des sociétés dans lesquelles sont intervenus des changements statutaires fréquents non justifiés par la situation économique de l'entreprise ;
- Recours à l'interposition de personnes physiques n'intervenant qu'en apparence pour le compte de sociétés ou de particuliers impliqués dans des opérations financières ;
- Réalisation d'opérations financières incohérentes au regard des activités habituelles de l'entreprise ou d'opérations suspectes dans des secteurs sensibles aux fraudes à la TVA de type carrousel, tels que les secteurs de l'informatique, de la téléphonie, du matériel électronique, du matériel électroménager, de la hi-fi et de la vidéo ;
- Constatation d'anomalies dans les factures ou les bons de commande lorsqu'ils sont présentés comme justification des opérations financières ;
- Recours inexpliqué à des comptes utilisés comme des comptes de passage ;
- Difficulté d'identifier les bénéficiaires effectifs ou les liens entre l'origine et la destination des fonds ;
- Opérations financières internationales sans cause juridique ou économique apparente ;
- Refus du client de produire des pièces justificatives ;
- Transfert de fonds vers un pays étranger suivi de leur rapatriement sous forme de prêts ;
- Organisation de l'insolvabilité par la vente rapide d'actifs à des personnes physiques ou morales liées ;

- Utilisation régulière par des personnes physiques domiciliées et ayant une activité en France de comptes détenus par des sociétés étrangères ;
- Réalisation d'une transaction immobilière à un prix manifestement sous-évalué.

Conformément à la troisième directive, les établissements doivent adopter une approche par les risques lorsqu'ils nouent une relation d'affaires. Les relations d'affaires seront classées en fonction de leur niveau de risque. Elles feront ainsi l'objet de mesures de vigilance différenciées.

Les éléments de tierce introduction ont été complétés par les lignes directrices. Ils sont à distinguer de la prestation externalisée. Lorsqu'un établissement bancaire délègue des prestations, il doit contrôler ce qu'il délègue. L'approche est un peu différente dans la tierce introduction. Il ne s'agit pas de contrôler le tiers, mais s'assurer que l'on peut disposer de ses documents. Ainsi, lorsque des produits financiers sont distribués par l'intermédiaire d'un CIF, c'est-à-dire d'un conseil en instruments financiers, ce dernier est considéré comme un tiers introducteur. Cela signifie que l'on peut récupérer les documents dont il dispose sur ses clients. En revanche, les crédits distribués par le biais d'un intermédiaire en opération de banques et en services de paiements (IOBSP) sont considérées comme des prestations externalisées qui requièrent un contrôle par la banque. Ce sujet d'actualité a suscité des échanges entre le monde bancaire et l'ACP récemment.

Les diligences allégées ont pour corollaire les diligences renforcées. A cet égard, la quatrième directive pourrait modifier les règles en la matière. A l'heure actuelle, les diligences renforcées existent lorsque le risque est estimé élevé. Ainsi, si la relation d'affaire n'est pas physiquement présente lors de l'entrée en relation, il convient de collecter une seconde pièce d'identité ou des documents d'identification certifiés, et de réaliser le premier paiement au moyen d'un compte ouvert au nom du client auprès d'un établissement de crédit si le prospect souhaite ouvrir un compte. Le dispositif actuel est donc assez lourd sur ce point, mais il devrait faire l'objet d'évolutions.

Le risque est considéré comme élevé lorsque le type de transaction ou de produit est susceptible de favoriser l'anonymat.

Lorsque la relation d'affaires est une Personne Politiquement Exposée (PPE), plusieurs démarches doivent être entreprises, notamment obtenir l'autorisation d'un niveau élevé de la hiérarchie de nouer des relations d'affaires avec ce type de relation d'affaires et disposer de procédures permettant d'identifier la relation d'affaire en tant que PPE.

La réglementation cite également comme situations présentant un risque de blanchiment élevé : une relation transfrontalière faisant intervenir un correspondant bancaire, ou une relation d'affaires avec des sociétés bancaires écran.

La troisième directive, précisée par des lignes directrices complémentaires, prévoit l'obligation, pour l'établissement, d'identifier le bénéficiaire effectif. Ce dernier renvoie à une personne physique répondant à au moins un des critères suivants : elle détient, directement ou indirectement, au moins 25 % du capital ou des droits de vote de la société ; elle exerce par tout autre moyen un pouvoir de contrôle sur les organes de gestion, d'administration ou de direction de la société, ou encore sur l'assemblée générale des associés.

Plusieurs lignes directrices ont complété ce dispositif : certaines ont été émises par l'AMF, d'autres conjointement par l'AMF et Tracfin, d'autres par l'ACP et Tracfin. Des principes d'application sectorielle assez détaillés ont par ailleurs été publiés dans le domaine de l'assurance. En 2011, des lignes directrices sont parues sur la tierce introduction, les bénéficiaires effectifs, les clients occasionnels. L'ACP est désormais habilitée à réglementer de manière complémentaire. Ces lignes directrices complètent la réglementation, et sont assorties de cas pratiques et de schémas.

Le socle des lignes directrices est, en volume, au moins aussi important que la réglementation elle-même.

Pour terminer, j'évoquerai les évolutions qui sont susceptibles d'intervenir avec l'adoption prochaine de la quatrième directive européenne. La Commission a transmis un rapport au Parlement Européen et au Conseil au sujet de l'application de la troisième directive. Même si rien n'est définitif, on peut en tirer des pistes de réflexion pour la quatrième directive.

Le rapport souligne que peu d'orientations ont été données aux établissements bancaires au sujet de l'approche fondée sur les risques. Le GAFI demande que les entités évaluent les risques liés aux clients, aux pays ou zones géographiques et aux produits, services, opérations et canaux de distribution.

Une extension du champ de la directive aux agents immobiliers effectuant des opérations de location est envisagée.

La proposition de la Commission devrait également abaisser le seuil à partir duquel des diligences sont nécessaires dans le cas d'opérations occasionnelles.

Par ailleurs, la directive pourrait assouplir les mesures renforcées pour les entrées en relation à distance, compte tenu des nouvelles technologies et des nouveaux moyens de paiement.

Concernant les diligences allégées, la quatrième directive pourrait opérer un léger retour en arrière, en exigeant l'application d'une approche par les risques lors de l'entrée en relation avec un autre établissement financier de l'UE ou pays tiers équivalent.

S'agissant des personnes politiquement exposées, le rapport de la Commission souligne que « la disponibilité, le coût et l'exactitude des informations disponibles dans les bases de données posent problème ».

La quatrième directive pourrait faire passer de 25 % à 20 % le seuil des personnes physiques détenant un capital ou un droit de vote. Le rapport estime souhaitable d'accompagner ces changements de mesures visant la transparence des personnes morales, notamment au niveau juridique.

Le rapport envisage de clarifier les liens entre le régime du passeport de la directive sur les services de paiement et la directive sur la monnaie électronique et le respect des règles du pays d'accueil en matière de lutte contre le blanchiment.

La Commission soulève également la question sur le caractère suffisant des lignes directrices produites par des organismes d'autorégulation. L'ACP n'est pas ici visée, mais plutôt certains organismes d'autorégulation de certaines professions.

Enfin, le rapport demande une amélioration de l'interaction entre la lutte anti-blanchiment et la protection des données personnelles (notamment par l'interaction des régulateurs de ces deux domaines).

Christiane LEGAT

Je vous remercie pour cette présentation. L'heure est à présent aux questions. Pour faire écho à la question de Manon ROY sur les sanctions, je crois que Marie-Agnès NICOLET a de bonnes réponses à apporter.

Marie-Agnès NICOLET

En effet, par rapport au monde anglo-saxon, les sanctions, même si leur seuil maximal a été récemment relevé, ne sont pas très lourdes dans la pratique pour les établissements bancaires. Certes, les sanctions ont incité les établissements à mettre en place des dispositifs plus importants qu'auparavant. Ce processus s'est développé en trois grandes étapes : le questionnaire de lutte anti-blanchiment, qui existe depuis les années 2000, les affaires sur des chèques à multiples endos, qui ont fait un peu de bruit en France au début des années 2000 également, et le fait que 90 % des sanctions de l'ACP et de la Commission Bancaire des dernières années ont porté sur ce sujet. Il n'en reste pas moins que nos sanctions sont moins dissuasives que dans d'autres pays. Toutefois, les

établissements essaient d'éviter d'entrer dans des processus de commission des sanctions. Ils tiennent en outre compte du risque en termes de réputation.

Christiane LEGAT

Les établissements négocient pour éviter la publication des sanctions. Cela démontre que la réputation est importante pour les établissements.

Je vous propose à présent de faire une courte pause avant de reprendre avec une table ronde animée par Blandine CORDIER-PALASSE.

Comment développer une approche proportionnelle et équilibrée de la lutte contre la corruption, le blanchiment et le financement du terrorisme

Table ronde animée par Blandine CORDIER-PALASSE
Fondateur de Cordier Conseil Executive Search

Participaient à cette table ronde

Marc LEVY, Directeur de la Conformité, La Banque Postale

Sylvie KANDE DE BEAUPUY, Group Compliance Officer, Technip

José BOUANICHE, Auditeur, Caisse des Dépôts et Consignations

Blandine CORDIER-PALASSE

Bonjour à tous, j'invite tout d'abord chacun des intervenants à se présenter et à expliquer ce qui l'a conduit dans ces fonctions.

Sylvie KANDE DE BEAUPUY

Je suis *Group Compliance Officer* chez Technip, entreprise industrielle d'ingénierie, qui fabrique du matériel destiné à l'industrie extractive de pétrole et de gaz, et plus récemment à l'éolien. J'ai passé une vingtaine d'années au Cabinet Clifford Chance, que certains d'entre vous connaissent peut-être, en charge de fusions-acquisitions. Ensuite, j'ai intégré une filiale d'EADS à Toulouse, où j'ai commencé à travailler sur la conformité et la lutte contre la corruption, pour rejoindre le groupe Technip, au sein duquel je suis en poste depuis bientôt quatre ans.

Marc LEVY

Je suis le directeur de la conformité de La Banque Postale, où je travaille depuis octobre 2005. J'ai contribué à la création de cette banque, qui a été créée le 1er janvier 2006. Elle est donc à la fois une vieille dame, puisque les comptes chèques postaux existent depuis longtemps, et une start-up.

J'ai commencé à travailler dans la banque en 1973, dans ce qui était pour ainsi dire « un village d'Astérix », une banque parisienne orientée vers les PME. J'y suis resté trente ans, puis cette banque a été peu à peu intégrée au deuxième ou troisième plus grand groupe mondial, HSBC, pour lequel la conformité est un enjeu important de gouvernance et de cohérence. J'ai été quinze ans exploitant dans cette banque, puis quinze ans inspecteur général. J'ai intégré en juin 2003 l'Inspection générale du CCF, avant de prendre la responsabilité de la conformité de la banque de détail du groupe CCF. Puis j'ai fait acte de candidature spontanée à la Poste, en pensant qu'il serait intéressant de participer à cette aventure de la création de La Banque Postale.

José BOUANICHE

Je suis auditeur dans le groupe Caisse des Dépôts et des Consignations. Antérieurement, j'exerçais dans l'ingénierie des logiciels et la sécurité informatique. J'interviens aujourd'hui en tant que porte-parole des auditeurs, mais également en tant que président de l'unité de recherche informatique de l'IFACI.

Blandine CORDIER-PALASSE

A présent, je vous propose d'entrer dans le vif du sujet de notre table ronde. Les interventions précédentes vous ont donné quelques exemples très concrets de la lutte contre le blanchiment et la corruption. L'orientation de la table ronde consistera à montrer jusqu'où aller dans la réglementation et le contrôle pour être efficace sans toutefois porter atteinte à la vie privée ou au business.

Je propose que nous parlions pour commencer de l'organisation des services, de la répartition des responsabilités pour que les organisations soient efficaces et efficientes. Je vous invite à nous parler de vos organisations et de nous présenter le cadre dans lequel vos organisations ont mis en place la *compliance*. J'ai lu dans les journaux que Technip avait rencontré quelques difficultés à cet égard.

Sylvie KANDE DE BEAUPUY

En effet, le groupe Technip a eu le malheur d'être soumis à une investigation du *Department of Justice*. Après de longues années d'investigations, qui ont mis à jour une affaire de paiement de commissions au gouvernement nigérian, le groupe a signé un accord avec l'administration aux termes duquel, en contrepartie d'un certain nombre d'engagements, le groupe n'était pas poursuivi au pénal, ce qui aurait signé l'arrêt de mort de l'entreprise.

Il s'agissait donc de sauver l'entreprise. Le groupe a payé une amende de plusieurs centaines de millions de dollars et octroyé un moniteur pour une longue durée. Il s'est notamment engagé à mettre en place un « *Compliance program* » suffisamment robuste pour éviter que la situation ne se reproduise.

Cet événement a en quelque sorte donné un coup de pouce à la mise en place d'un programme de lutte contre la corruption. J'ai été recrutée pour la mise en place de ce programme, les dirigeants étant bien conscients que le monde du pétrole et du gaz devait changer de culture et de mentalité.

Notre département existe depuis 2008. Nous avons volontairement opté pour une organisation restreinte, appelée à monter progressivement en puissance. Il s'agissait en effet de maîtriser au maximum les tenants et aboutissants de ce programme et de ne pas se disperser.

Je me suis appuyée sur un cabinet pour mettre en place un programme répondant aux standards internationaux. Aujourd'hui, nous sommes une trentaine de personnes, pour une entreprise de près de sept milliards d'euros de chiffre d'affaires. Notre organisation reste donc assez restreinte, mais nos collaborateurs sont totalement dédiés à cette problématique. Ils sont répartis dans la holding et dans les divisions auprès des opérationnels.

Blandine CORDIER-PALASSE

La *compliance* dans les groupes diffère légèrement de la conformité dont il est question dans les groupes bancaires. Je vais donc vous laisser nous présenter la manière dont vous êtes organisés au sein de vos institutions.

Marc LEVY

La Conformité est une direction à part entière de La Banque Postale. Elle compte aujourd'hui 56 personnes, qui me sont directement rattachées, et 450 personnes que je pilote fonctionnellement. Je suis membre du Comité exécutif de la banque. La direction de la Conformité se situe à la fois en amont et en aval des sujets et est une direction « productrice » sur les sujets liés à la lutte contre le blanchiment et financement du terrorisme. Nous venons d'y adjoindre la lutte contre la fraude, pour des raisons de cohérence. Nous comptons quatre autres départements. Deux sont situés en amont, dédiés à la déontologie et à l'expertise conformité, qui valide l'ensemble des supports de

mise en marché et pilote le dispositif de comité d'examen des produits. En aval, un département est en charge du pilotage des contrôleurs permanents qui interviennent dans les bureaux de poste en France et les centres financiers. Enfin, quelques personnes sont dédiées à un dispositif d'auto-évaluation des dispositifs de contrôle interne. Parmi les organes de gouvernance, nous disposons d'un comité des risques et un comité dédié à la conformité, présidé par le président du directoire, et animé par mes soins.

José BOUANICHE

Ma présentation n'aura aucun caractère exemplaire, dans la mesure où la Caisse des Dépôts et des Consignations est un organisme assez particulier. Nous ne sommes une banque que depuis très peu de temps. L'ACP n'a le droit d'intervenir à la Caisse des Dépôts et des Consignations que depuis deux ans, et encore, en des termes restrictifs. En tant qu'auditeurs, nous menons des contrôles de troisième niveau, périodiques, au-dessus de tous les contrôles permanents. Nous intervenons sur tous les dispositifs de pilotage, de gouvernance et de maîtrise des risques.

Blandine CORDIER-PALASSE

Intervenez-vous en amont et en aval des opérations ?

José BOUANICHE

Il est difficile de répondre à cette question. En tant qu'auditeurs, nous intervenons périodiquement. Dans la mesure où il s'agit de périodes relativement courtes, nous sommes constamment amenés à nous positionner sur des éléments.

D'autre part, le service d'audit central participe systématiquement en tant qu'observateur. Nous sommes donc informés en amont, mais nous n'intervenons pas systématiquement en amont.

Blandine CORDIER-PALASSE

En ce qui concerne la sensibilisation de la direction et des salariés à ces problématiques, pouvez-vous nous indiquer comment vos directions sont impliquées dans les problématiques de conformité et la mise en place d'une culture d'entreprise ?

Marc LEVY

La Banque Postale a pour caractéristique de faire travailler en son nom et pour son compte 10 000 conseillers qui ne sont pas des banquiers, mais des postiers. Ces derniers, par un dispositif que je ne détaillerai pas ici, sont habilités à agir au nom et pour le compte de La Banque Postale.

La banque n'est pas l'employeur de ces conseillers. Un dispositif doit donc être mis en œuvre pour mener à bien le pilotage. Par ailleurs, environ 75 % de ces conseillers étaient en poste avant la création de La Banque Postale. L'un des rôles de la direction de la Conformité est donc bien de contribuer à diffuser la culture bancaire. Pour ce faire, des formations sont dispensées. Comme vous le savez, une certification de l'AMF est désormais obligatoire avant la prise de fonction. La Banque Postale avait mis en œuvre cette démarche avant que l'AMF ne l'exige. Par ailleurs, nous dispensons des formations récurrentes sur la lutte anti-blanchiment et la déontologie. Nous organisons également des ateliers de sensibilisation à destination des directeurs d'établissements, qui ne sont pas chargés uniquement d'activités bancaires. Ces ateliers sont animés par le responsable de la lutte anti-blanchiment de La Banque Postale et reposent sur la présentation de cas pratiques issus directement des bureaux que les personnes dirigent. Cette méthode est très efficace.

Nous sommes en outre dotés de dispositifs, qui nous permettent d'identifier de manière très précise les zones présentant des risques plus élevés en matière de blanchiment. La

Banque est dotée d'un Correspondant Informatique et Liberté, et travaille avec lui sur ces sujets sensibles.

Blandine CORDIER-PALASSE

La *compliance* est souvent vécue, dans un premier temps, comme une contrainte dans les entreprises. Pouvez-vous nous expliquer comment vous avez transformé la contrainte en atout dans votre Groupe et comment les salariés adhèrent au programme de *compliance* que vous mettez en place ?

Sylvie KANDE DE BEAUPUY

Nous sommes encore en train d'y travailler, car il s'agit d'un *process* relativement long. Le processus a commencé par un message très clair de notre président, qui à son arrivée, il y a environ cinq ans, a fait passer des messages. Il a expliqué que le monde avait changé et qu'il s'agissait à présent de faire des affaires de manière éthique. Le message a été largement renforcé au moment de la signature de l'accord avec l'administration américaine. La tolérance zéro a été mise en avant. Le sujet est également évoqué de façon périodique dans les comités exécutifs, aussi bien au niveau de la holding que des filiales. Pour toucher une grande partie de la population, nous avons mené des actions très ciblées de formation. Nous avons commencé par le haut pour descendre dans toute l'organisation. Une formation *online* a été imposée à une certaine catégorie de salariés. L'octroi du bonus était lié à la participation à cette formation. Nous avons doublé ces formations par des séances de formation adaptées en fonction des métiers, afin d'affiner les messages.

Blandine CORDIER-PALASSE

Vous avez évoqué les bonus liés à la participation à ces programmes de formation. Concernent-ils l'ensemble de l'entreprise ou uniquement le *top management* ?

Sylvie KANDE DE BEAUPUY

Ces incitations concernent essentiellement le *top* et le *middle management*.

Blandine CORDIER-PALASSE

Vous avez dit que certaines populations se sont montrées réservées à l'égard de ce programme de *compliance*, notamment les commerciaux, qui pensent devoir renoncer à certaines affaires, ou en tout cas ne peuvent plus les mener comme ils étaient habitués à le faire. Comment avez-vous transformé cette contrainte en avantage concurrentiel ?

Sylvie KANDE DE BEAUPUY

Il est certain qu'au départ, vous êtes considéré comme un empêcheur de faire des affaires, en mettant en place des systèmes trop lourds d'un point de vue administratif. Il est nécessaire de montrer que nous sommes là pour accompagner, et non pas pour empêcher de faire du business. Au bout d'un moment, les salariés commencent à s'apercevoir que cela comporte un avantage compétitif. J'admets que ce programme a été dans un premier temps un désavantage, dans le sens où certains clients se sont éloignés. Or, désormais, il s'agit d'un avantage. Nos clients, qui sont les majors du pétrole, sont astreints aux mêmes obligations que nous. Sous l'effet de l'entrée en vigueur de réglementation du type *UK Bribery Act*, ils pourraient eux-mêmes se retrouver responsables d'un certain nombre de nos agissements, et sont par conséquent très intéressés par les processus que nous avons mis en place. Il nous arrive de dispenser des formations communes pour être dans la même ligne et conduire nos projets de la façon la plus éthique possible, et en toute transparence. Ce programme d'éthique à la pointe se transforme en avantage compétitif, dans la mesure où les entreprises ne disposant pas d'un tel programme sont regardées avec suspicion.

Marc LEVY

En vous entendant, j'ajouterais qu'un point fondamental a trait à l'éthique et à la déontologie. Aujourd'hui, nous assistons à une défiance des clients vers les banquiers. La crise a accentué ce phénomène. En matière de déontologie, il s'agit de maintenir et développer la relation de confiance entre la banque et l'ensemble des clients. J'ai la chance de travailler dans un établissement où cette relation de confiance est forte. Et il convient de la protéger. Ainsi, nous faisons en sorte que la part variable des commerciaux soit liée à hauteur d'un tiers à des « incontournables », à savoir les aspects déontologiques.

La formation est l'un des vecteurs permettant de marquer les esprits et de faire évoluer les comportements. Il existe d'autres vecteurs d'ordre plus « répressif ». Si nous constatons des manquements déontologiques graves, j'ai le pouvoir de demander la déshabilitation à agir au nom et pour le compte de la banque des personnes concernées, ce qui se traduit en général par un licenciement. Cela peut survenir dans des cas d'abus de faiblesse ou de captation d'héritage, à travers la modification des clauses bénéficiaires de contrats d'assurance-vie. La banque est très attentive à ce genre de sujet.

Blandine CORDIER-PALASSE

Monsieur BOUANICHE, quel est le rôle préventif et les éventuelles missions correctives de l'audit interne dans la lutte anti-blanchiment ?

José BOUANICHE

Les approches en matière de lutte contre la corruption et de lutte contre le blanchiment diffèrent totalement. La lutte contre la corruption est beaucoup plus complexe. Nous essayons de travailler en particulier sur les appels aux marchés. Il s'agit alors d'un travail de conformité ou de revue de dossiers. Les collusions sont quasi-impossibles à détecter. Nous avons par ailleurs le projet de travailler sur des cas de recours à des sociétés de formation liées à des sectes.

Concernant la lutte anti-blanchiment, nous intervenons sur les aspects de respect de la réglementation. A ce sujet, vous trouverez un cahier de l'IFACI sur l'audit relatif à la lutte contre le blanchiment, qui date de 2004 mais reste pertinent. Il est fondamental de toujours réfléchir par rapport aux risques. Les grilles de lecture diffèrent d'une entreprise à l'autre.

Blandine CORDIER-PALASSE

Comment les nouvelles technologies vous aident-elles dans cette lutte contre la corruption et le blanchiment ?

José BOUANICHE

Pour la lutte contre le blanchiment, nous avons mis en place, au niveau du contrôle permanent, des programmes de vérification des flux, des origines ou des destinations des fonds. Il en va de même pour les PPE.

Toutefois, le recours à des prestataires extérieurs ou l'achat de logiciels ne permet pas à l'auditeur d'avoir une vision globale des dispositifs en place. Il n'est donc pas possible de garantir la mise en place d'algorithmes susceptibles de nous protéger de manière suffisante. En outre, les systèmes de détection sont de plus en plus complexes et posent un problème pour le travail critique.

Blandine CORDIER-PALASSE

Sylvie, pouvez-vous nous parler du rôle préventif de l'audit interne ?

Sylvie KANDE DE BEAUPUY

Nous sommes deux départements séparés mais nous travaillons main dans la main. Je suis d'ailleurs en train de proposer à l'audit interne une charte de coopération pour définir les rôles de tout un chacun. L'objectif est de ne pas les placer en situation de conflit d'intérêt, tout en maintenant une surveillance utile à la *compliance*. Cela se traduit par une coopération au quotidien, un échange d'information permanent. Chaque fois que l'audit interne part en mission, un groupe de travail lui confie des axes prioritaires. Evidemment, ces axes touchent en premier lieu nos consultants, qui sont indispensables mais constituent en quelque sorte l'un des foyers les plus à risques. La coopération se déroule très bien. L'audit interne joue un rôle préventif, mais aussi curatif. Il vérifie l'application des procédures mises en place au sein de la *compliance*. Les informations qu'il nous donne peuvent nous inciter à mener des enquêtes plus précises. Quant aux moyens utilisés, ils sont fonction de l'importance de l'alerte. Ils peuvent aller d'une simple investigation jusqu'à des moyens plus intrusifs comme l'*imaging* des ordinateurs.

Blandine CORDIER-PALASSE

Monsieur LEVY, pouvez-vous nous expliquer quel système de protection des données personnelles vous avez mis en place au sein de La Banque Postale ?

Marc LEVY

Avant de répondre à votre question, en termes de prévention de la corruption interne, notre déontologue participe à la commission des achats de la banque et intervient sur les achats d'un montant supérieur à 1,5 million d'euros. Comme nos confrères, nous avons des filiales en charge de commercialisation d'immobilier. Nous intervenons à cet égard avec droit de veto sur le choix des partenaires et des programmes.

Pour répondre à votre question, nous sommes très attentifs à la protection des données. Concrètement, nous avons été la première banque à mettre en place un correspondant informatique et libertés. Tous nos confrères du comité Conformité de la Fédération Bancaire Française (FBF) nous ont regardés avec étonnement. Certains ont aujourd'hui suivi le chemin, mais ils sont peu nombreux. L'inspection générale est extrêmement attentive à nos dispositifs informatiques. Dès la création de la banque, j'avais fait admettre que l'administration des systèmes de détection LAB soit conduite par nous. Par ailleurs, nous sommes régulièrement soumis à des tests d'intrusion par l'inspection générale, jusqu'ici les « hackers » mandatés par ses soins, s'y sont cassés les dents.

Le traitement des alertes LAB sont traités dans des locaux séparés.

Blandine CORDIER-PALASSE

Monsieur BOUANICHE, en tant qu'auditeur interne, que regardez-vous dans vos missions d'audit en matière de protection des données personnelles ?

José BOUANICHE

Nous veillons au respect de la réglementation française, puisque nous n'intervenons qu'en France. Nous travaillons sur la sécurité des données. Les données doivent rester dans le périmètre d'autorisation qui leur a été initialement assigné, et les traitements doivent rester dans le cadre prévu. Nous sommes par ailleurs attentifs à la durée de rétention des données.

Blandine CORDIER-PALASSE

Les délais vous permettent-ils de sauvegarder les données en cas d'enquête ou de procès ?

José BOUANICHE

Nous n'intervenons jamais sur des audits à caractère pénal. Dès lors qu'une affaire relève du domaine pénal, nous cédons la place aux personnes compétentes.

Blandine CORDIER-PALASSE

Monsieur LEVY, comment coordonnez-vous vos actions avec les autres services de votre organisation ? Quelles sont les éventuelles interactions ?

Marc LEVY

Les interactions sont bien sûr considérables, puisque nous irriguons l'ensemble des activités de La Banque Postale. La coopération intervient par un échange d'information à travers les organes de gouvernance. D'abord, je fais partie du comité exécutif. Par ailleurs, une bonne partie des membres du comité exécutif siègent au comité conformité, avec un autre angle de vue.

Par ailleurs, je participe à un certain nombre de comités de gouvernance, notamment le comité marketing de la banque, mais le comité de développement commercial. Je participe également à une commission des achats.

Parallèlement, notre sujet majeur au quotidien est d'identifier le plus en amont possible les sujets liés à la conformité sous ses différents angles. L'un de mes collaborateurs consacre 40 % de son temps à identifier les nouveaux projets de la banque, et les risques qu'ils comportent en termes de conformité.

Les rapports des contrôleurs bancaires sont systématiquement restitués aux responsables de métiers. Les interactions sont donc permanentes. Enfin, notre direction est en interaction constante avec la direction des risques.

Blandine CORDIER-PALASSE

La conformité que vous mettez en place est donc très transversale et impliquée dans toutes vos opérations.

Marc LEVY

Les points de vue de la profession sur l'évolution de la fonction conformité sont variés. A mon sens, notre rôle consiste bien sûr à s'assurer du respect de la réglementation, à contribuer à la protection de la banque et de son image, de ses collaborateurs. Notre mission me parait très importante pour la protection de la primauté de l'intérêt des clients.

Christiane LEGAT

J'invite à présent Philippe MONTIGNY à conclure nos travaux sur le thème : « la conformité : entre loi et éthique ».

La conformité : entre loi et éthique

Philippe MONTIGNY
Président d'Ethic Intelligence

Nous avons beaucoup parlé de conformité et de *compliance*, mais nous ne nous sommes pas encore posé la question du fondement de cette conformité et de cette *compliance*.

Nous avons aussi utilisé de manière un peu indifférenciée les termes de *compliance* et de conformité. Je m'exprime certes devant une Canadienne, qui est forcément plus bilingue que moi. Mais si nous regardons dans le dictionnaire, le terme de « conformer » signifie « se calquer », « respecter des règles », alors que dans le verbe « *to comply with* », il existe une notion plus forte d'action. Le terme de conformité renvoie à une norme à laquelle se conformer, alors que dans le terme de *compliance*, la notion de loi apparaît assez rapidement. Selon moi, la *compliance* a peut-être un sens un peu plus large que la conformité. Néanmoins, dans le cadre de mon exposé, je considérerai que les deux termes sont à peu près équivalents.

Je distingue trois cadres de références auxquels les entreprises doivent se conformer. Le premier est la loi pénale, dont l'objet est clairement ce qu'il ne faut pas faire. Ainsi, la corruption est interdite, les délits d'initiés sont interdits, les pratiques anti-concurrentielles sont interdites.

Le second cadre de référence renvoie aux normes professionnelles. La logique de ces dernières est très différente, puisqu'elles consistent en des obligations. Ainsi, il convient de se conformer à des obligations de type réglementaire, que celles-ci soient très générales ou très spécifiques. Certaines obligations sont de nature déontologique et varient en fonction des métiers. Progressivement, des organisations gouvernementales ou professionnelles édictent des règles, ou bonnes pratiques, auxquelles les entreprises doivent se conformer.

Le troisième cadre de référence peut être appelé le corpus socio-éthique. Il contient des règles auxquelles il faudrait se conformer. Je distingue volontiers les règles en vigueur dans les pays de la zone OCDE, c'est-à-dire les pays industriels et démocratiques, qui concerneront la vie privée, la non-discrimination, etc. Il existe aussi les règles locales, qui varieront en fonction des environnements géographiques. Enfin, il existe des règles internationalisées, qui viennent de la zone OCDE, qui nous paraissent très importantes. Elles portent par exemple sur le travail des enfants, le respect de l'environnement, la non-ingérence politique. Elles nous concernent et nous les appliquons lorsque nous opérons à l'étranger, même dans des environnements où le contexte est beaucoup plus laxiste.

A partir de ces trois cadres de référence, qui interagissent les uns sur les autres, deux mouvements se développent. Le premier est un mouvement progressif de pénalisation de la *soft law*. L'opinion publique a des attentes. Ces dernières doivent être reprises par les entreprises sous forme de normes professionnelles. Si l'entreprise ne les reprend pas, elles passent du côté de la loi. Ainsi, l'opinion publique a considéré que la rémunération des traders, quand elle est importante, peut avoir une relation avec les phénomènes de crise financière. On a attendu des banques qu'elles adoptent des principes directeurs sur ces questions. Comme elles ne l'ont pas fait, des recours de nature législative ont pris le relais.

D'un autre côté, la loi commence à s'intéresser à ce domaine et à édicter des règles dans le code pénal sur des sujets qui relevaient auparavant du domaine privé, comme par exemple les questions de non-discrimination.

A partir de ce cadre, l'entreprise est soumise à trois obligations. La première consiste à ne pas enfreindre la loi, dans un objectif de conformité pénale. La seconde revient à se

conformer aux obligations de son entreprise et de son secteur, dans un objectif de conformité professionnelle. Enfin, l'entreprise a une obligation de conformité de nature éthique, dans un enjeu réputationnel.

L'ensemble de ces conformités dessine une politique de conformité, en réponse à une attente de plus en plus marquée des citoyens, qui sont aussi des consommateurs et des employés.

La politique de conformité des entreprises se construit à partir de chaque cadre de référence. Dans le premier cadre, il s'agit de transcrire des interdictions dans des politiques de prévention. S'agissant du second cadre, il s'agit de mettre en place des procédures d'exécution, des mécanismes que les collaborateurs devront suivre pas à pas. Enfin, ces incitations vont être transcrites en règles de comportement, avec des chartes éthiques valorisant certains comportements ou en en condamnant d'autres.

En fonction de leurs métiers, les entreprises sont confrontées à des environnements assez différents. La conformité répond à des risques très variés suivant les entreprises. En guise d'illustration, j'ai choisi quatre secteurs significatifs : la défense, les délégations de service public (eau, traitement des déchets), les télécommunications et le secteur de la beauté et du luxe.

I) Les risques pénaux

Dans la défense, au niveau pénal, le risque est élevé sur la corruption publique. Par ailleurs, le secteur doit obéir à des obligations de contrôle à l'exportation sur toutes les technologies. En revanche, le risque d'entente est faible.

Dans les délégations de service public, la notion de corruption publique peut s'avérer très présente, notamment parce que certains marchés sont gérés par l'administration. Les entreprises ont parfois intérêt à s'entendre. En revanche, l'impératif du contrôle à l'exportation est bien sûr inexistant.

Dans le domaine des télécommunications, la notion d'entente, notamment tarifaire, constitue un risque élevé. En revanche la corruption publique sera très variable. Elle sera très faible pour les opérateurs historiques nationaux. En revanche, s'ils développent leur activité à l'étranger, les opérateurs seront peut-être confrontés à des risques de corruption publique pour l'obtention des licences.

Enfin, dans le secteur de la beauté et du luxe, la notion de corruption est quasi inexistante dans la partie vente. Le risque d'entente n'existe pas. Le contrôle à l'exportation ne se pose même pas dans le domaine.

II) Les risques professionnels

Dans la défense, les enjeux sont liés à la perte et au vol de données stratégiques, aux normes de sécurité.

Dans les délégations de service public, les principaux enjeux sont liés à la sécurité des consommateurs et à l'environnement.

Dans le secteur des télécommunications, l'enjeu porte sur le respect des règles de l'ART, ainsi que sur la gestion des données personnelles.

Dans le domaine de la beauté et du luxe, notamment dans la cosmétique, la santé des consommateurs constitue un enjeu.

III) Les risques éthiques spécifiques

Ils diffèrent également dans chaque secteur. Ainsi, dans la défense, le risque éthique proviendrait d'une critique de la part d'une ONG, dans le cas où des produits auraient été vendus à des pays non démocratiques.

Le domaine de la délégation de service public peut être confronté à des critiques sur la justesse du prix au regard de la qualité des produits ou services offerts.

En matière de beauté et de luxe, des questions de discrimination avérées au sein de l'entreprise auraient un impact réputationel grave en raison de la diversité des clients de par le monde. L'expérimentation animale peut également entraîner des problèmes.

Chaque entreprise doit donc procéder à sa propre analyse de risques, au niveau pénal, professionnel et éthique. Les politiques de conformité d'un L'Oréal, d'un MBDA, qui vend des missiles, ou d'un France Télécom, seront globalement assez différentes.

La politique de conformité est censée protéger l'entreprise d'un certain nombre de risques. Mais l'entreprise ne doit pas prendre le risque du conformisme. En effet, si elle se contente de déclarations de principes, des chartes, l'ensemble de sa politique sera décrédibilisé.

Par ailleurs, si l'entreprise met en place des procédures trop codifiées, sans les accompagner de séances de sensibilisation à l'attention des collaborateurs, ces derniers ne seront pas suffisamment vigilants.

Enfin, le troisième risque pour l'entreprise revient à utiliser des procédures pour rendre des délits conformes : l'idée étant que si les procédures permettent de protéger l'entreprise, il suffit de détourner l'esprit de ces procédures et de les utiliser pour dissimuler des actes pénalement répréhensibles. Par exemple, utiliser une procédure de «agent commercial » qui a pour but de s'assurer que l'agent présente toute les garanties d'intégrité tout en lui demandant explicitement de « porter une valise » à un agent public. J'ai été très intéressé, notamment dans l'exposé de Sylvie KANDE DE BEAUPUY, de voir que la formation dispensée insiste sur le haut niveau du management. Il serait en effet dommage que des personnes, ayant un haut niveau de responsabilité, aient l'idée de détourner les procédures pour commettre des délits.

La conformité constitue aussi un véritable enjeu, à condition de ne pas rester dans le conformisme, et d'en faire un enjeu de modernité, c'est-à-dire une manière de faire du business. Beaucoup plus qu'à un programme, la conformité renvoie peut-être à une façon de conduire les affaires, de traiter du commercial avec un certain sens de respect des lois, des pratiques et de l'éthique.

La conformité peut ainsi conduire à une différenciation tout à fait positive. Le problème de corruption Siemens dans les années 2000 en constitue un contre-exemple. Dans la filiale télécommunication, où sont apparus les problèmes de corruption, lorsque le nouveau PDG est arrivé, il a décrété la tolérance zéro. Six à huit mois plus tard, le chiffre d'affaires avait considérablement chuté. Siemens a donc fait venir un cabinet spécialisé en technologie, qui a diagnostiqué que les standards commercialisés par Siemens avaient plusieurs années de retard sur les concurrents. Les investissements à consentir en R&D pour les remettre à niveau étaient colossaux.

Une entreprise qui verse un pot-de-vin remporte certes un marché. Si ses concurrents sont déçus, ils reviennent ensuite avec un produit plus sophistiqué. Si l'entreprise ne perçoit pas que son produit est remis en question par le marché, elle ne l'adapte pas. Le commercial continue à payer des pots de vin, peut-être plus élevés pour faire la différence. En d'autres termes, dans la corruption, le rapport au marché est totalement faussé. L'entreprise ignore quelle est la qualité du produit par rapport au marché, l'appréciation du marché sur ce produit et sur son prix. Le problème de la corruption n'est pas uniquement éthique et légal. Il représente également un véritable problème de business. Si dans vos équipes vous devez évoquer ce sujet, je vous invite à mettre en évidence ce décalage par rapport au business. A l'inverse, toutes les entreprises ayant mis en place des politiques de prévention de la corruption assez pointues, comme General Electric, Siemens aujourd'hui, ou Alstom, sont parmi les meilleures de la classe. Autrement dit, la qualité d'un programme de conformité n'est pas l'autre du chiffre d'affaires. Cette question a été soulevée ce matin. Certes, la politique de conformité peut d'abord entraîner une baisse faciale du chiffre d'affaires. Mais un chiffre d'affaires de 100 qui s'appuie sur 20 de

pratiques illégales s'élève en réalité à 80. Alors que si le chiffre d'affaires s'appuie totalement sur des pratiques légales, il sera réellement de 100.

Je terminerai par un dernier exemple, pour montrer à quel point les entreprises ayant décidé d'intégrer la lutte contre la corruption en font un facteur d'innovation.

Nous avons certifié Schneider Electric en Egypte, qui vend notamment des stations électriques, permettant chacune de fournir de l'électricité à 50 000 personnes. L'entreprise a décidé de vendre ces stations au Soudan, à Khartoum, où les Chinois sont très présents. Les Chinois proposent les mêmes centrales, moins chères, accompagnées de pots de vins. Dans ce contexte, les commerciaux de Schneider Electric ont travaillé sur le financement avec une banque à Dubaï. La banque a accepté d'avancer l'argent et de se faire rembourser par les revenus du gouvernement issus des personnes connectées au réseau électrique. Or, la population de Khartoum est très pauvre. La collecte de revenus n'y est donc pas facile. Schneider Electric a donc travaillé sur un système de compteurs électriques prépayés, installés gratuitement dans les habitations. Les habitants souhaitant de l'électricité doivent acheter un ticket. Le système de vente est relié par Internet aux centrales de Khartoum. Schneider Electric a donc expliqué au ministre que l'installation des centrales allait générer rapidement des revenus et a remporté le marché.

La corruption est certes une contrainte. Mais lorsque ces contraintes sont intégrées, elles deviennent des facteurs différenciants.

L'enjeu est par conséquent de distinguer la lettre et l'esprit de la conformité. Il convient de s'orienter vers une *compliance* plutôt *value-based* que *principle-based*. Nous observons dans nos entreprises que la fonction de responsable conformité évolue lentement vers la fonction de responsable éthique et conformité. Si nous voulons faire en sorte que la conformité soit autre chose qu'un programme auquel il faut se conformer en pliant la tête, mais au contraire un facteur d'innovation et de valorisation de l'entreprise, il convient d'y intégrer la dimension d'éthique.

Je terminerai par cette citation de Emmanuel LEVINAS :

« *L'éthique est une exigence essentielle qui me fait être responsable de la responsabilité d'autrui* ».

Je vous remercie de votre attention.

Christiane LEGAT

Je vous remercie pour l'acuité de votre propos, notamment pour avoir attiré notre attention sur une manière de conduire les affaires de l'entreprise en se fondant sur la responsabilité et l'éthique. Je partagerai avec vous un résumé de cette journée de travail à travers quelques mots clefs qui ont retenu mon attention :

- « L'exemple vient du haut ». Il convient de former son comité exécutif aux notions de conformité, de blanchiment, d'éthique.
- En matière de corruption, il convient de savoir penser aux risques de collusion, aux faisceaux d'informations, à l'enchevêtrement des informations.
- Pour les aspects de blanchiment, il convient de classifier les risques de blanchiment.
- Nous avons aussi entendu qu'il fallait bien distinguer la tierce introduction de l'externalisation des prestations, lesquelles sont à contrôler.
- Il convient aussi de tenir compte des lignes directrices émises par le régulateur, qui complètent la réglementation et demeurent un socle extrêmement important pour nos établissements.
- En matière de conformité, j'ai retenu l'importance du corpus socio-éthique et de la mise en place d'une politique de conformité, dans ses trois volets : pénale, professionnelle et éthique.

Ainsi, mener une politique de conformité constitue un élément de modernité et d'excellence. Voici un bon contrat pour l'avenir de nos entreprises. A chaque entreprise ses risques, sa conformité et ses dispositifs contre la corruption, le blanchiment et le financement du terrorisme.

Il me reste à présent à remercier tous les intervenants pour la qualité et la clarté de leurs présentations. J'espère que ces dernières vous seront utiles dans les jours à venir dans vos établissements. Je vous remercie pour l'attention soutenue dont vous avez fait preuve tout au long de cette journée.