# Où loger la lutte contre la fraude en entreprise ?

Virginie Srecki,

Co-directrice du Magistère de Sciences de Gestion à l'Université Paris-Dauphine,

Responsable du Certificat Fraud Risk Management

Co-responsable de l'Executive Master - Expert Conformité.

**Article paru dans la revue GRASCO n°15 – Mai 2016**

La fraude, acte intentionnel et illégal commis dans le but d'obtenir des avantages indus, dévoile de multiples facettes, se déploie jusqu'à toucher tous les individus et toutes les organisations. Vaste domaine, dont il convient tout d'abord de délimiter le périmètre d'analyse[1]: il s'agira ici de se focaliser sur les fraudes contre les entreprises, quel qu'en soit l'auteur et ses moyens d'action, contrevenant au Code pénal[2].

De nombreuses statistiques sur la fraude comptable et financière dont sont victimes les entreprises existent (ACFE, PwC, Kroll, McAfee…), mais la plupart sont biaisées par un échantillon nécessairement réduit d'entreprises ayant accepté d'évoquer le sujet.

Or, si la lutte contre les fraudes externes est souvent affichée[3], l'entreprise communique difficilement sur les fraudes internes[4]. Ces dernières, orchestrées par les propres salariés ou managers de l'entreprise victime, soit en tant que complices soit même en tant qu'instigateurs, restent plus complexes à déceler, tout en étant les plus fréquemment rencontrées.

Il ressort néanmoins une tendance générale : la fraude est en augmentation, notamment à cause du développement de la cybercriminalité, et les entreprises se sentent de plus en plus vulnérables face au risque financier qu'elle génère : préjudice direct, mais aussi sanctions, et risque de réputation.

La fraude est un risque permanent, espérons qu'il ne soit pas systémique[5], car la perception de la morale, de l'éthique ou même de la loi est différente en fonction de chaque individu inséré dans son environnement. Si, traditionnellement, l'individu est seul face à sa morale, la loi est la chose publique. Entre ces deux niveaux, la définition de la déontologie, étymologiquement « le discours de ce que l'on doit faire », est confiée à des organismes publics ou privés. Et, dans les faits, de plus en plus d'interactions surviennent entre ces différentes parties prenantes.

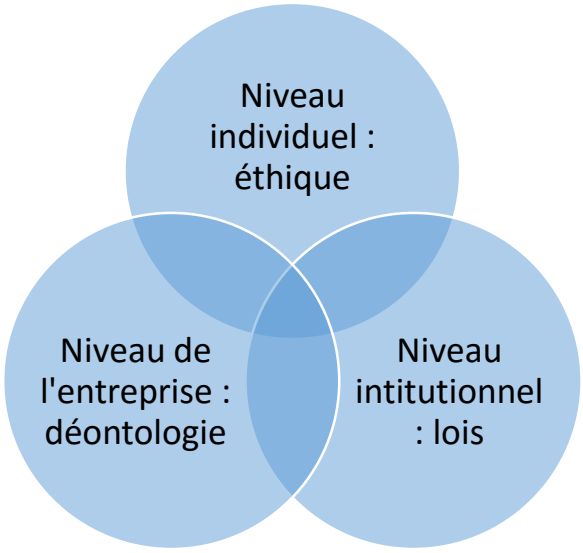
Ainsi, le risque de fraude contre les entreprises doit être combattu à différents niveaux interagissant entre eux :

- Au niveau individuel : grâce à l'éducation et la formation, principalement à l'université, dans un contexte d'échanges et de socialisation, les individus acquièrent le sens de l'éthique.

- Au niveau de l'entreprise : par le biais de structures dédiées, d'outils et de procédures adaptées, des normes déontologiques sont élaborées et leur respect contrôlé.

- Au niveau institutionnel : par l'élaboration de la loi et des normes réglementaires.

Ces règles sont établies par une autorité hiérarchique supérieure et légitime. La fraude est un acte répréhensible et constitue une violation de la loi ou du règlement. Mais une approche punitive et cloisonnée n'est plus suffisante : tous les acteurs doivent coopérer pour éduquer, former, sensibiliser, contrôler, dissuader et si nécessaire sanctionner la fraude.




**C'est à mettre à la fin de l'introduction au milieu**

## I. L'éducation à l'intégrité comme protection contre les comportements non éthiques

Le sens de la morale, religieuse ou laïque, inculqué par les parents et le système éducatif est binaire : le mal s'oppose au bien, de manière universelle. Ainsi chacun s'accorde à dire que « tuer c'est mal. »

L'éthique, en revanche, s'appréhende dans un contexte donné, dans la relation avec l'autre et en intégrant des éléments de justification. Ainsi, tuer pour se défendre, et si l'on en a reçu l'ordre, n'est plus considéré de la même manière par l'ensemble des individus : la discussion est ouverte mais la réponse reste individuelle. Dès lors, l'éthique a été définie par Jean-Jacques Nillès[6] comme : « une disposition individuelle à agir selon les vertus, afin de rechercher la bonne décision dans une situation donnée. »

Dès la petite enfance, un élève est confronté à la tentation de tricher pour satisfaire aux exigences parfois trop lourdes des parents. Au lycée et au niveau supérieur, la réussite aux examens est capitale pour accéder aux meilleures formations. En entreprise, la performance est essentielle pour progresser et conserver ses primes. Et le regard des autres est corrélé à la réussite sociale. Dès lors, à chaque étape de sa vie, un individu doit résister à la pression et rester intègre malgré les tentations. Le message de son entourage, personnel, éducatif ou encore professionnel, va lui permettre de structurer sa réflexion.

Il en résulte qu'une partie de la population ne fraudera jamais tandis qu'une autre fraction fraudera toujours. Mais la majorité d'entre nous pourrait devenir fraudeur en fonction du contexte. Donald Cressey, sociologue américain, dans son triangle de la fraude[7], indique que la bascule pourrait s'expliquer par la combinaison de trois facteurs : la pression qui incite à frauder, l'opportunité qui se présente notamment du fait d'une faille dans le contrôle, et la rationalisation qui lui permet de justifier son acte : « tout le monde le fait ».

Ainsi, dans le contexte social, l'exemplarité contribue au développement personnel. Dès lors, les parents, le système éducatif, le management dans l'entreprise et les personnes publiques devraient à la fois donner des instructions claires et cohérentes mais aussi les appliquer scrupuleusement…

Tandis que la sensibilité éthique se développe au travers de la connaissance des vertus et la connaissance des autres, la discussion autour des valeurs à promouvoir et des bonnes pratiques, dans le respect des lois, demeure essentielle. L'Université a, dans ce contexte, un rôle privilégié à jouer dans la prévention du risque de fraude :

- Auprès des jeunes adultes en devenir, en véhiculant la connaissance, l'esprit critique et en les sensibilisant à l'éthique des affaires. L'Université Paris-Dauphine a développé des programmes de formation autour de l'éthique et du management du risque de fraude dans quelques masters de formation initiale : en master Comptabilité Contrôle Audit par exemple.

- En formation continue, elle devient le lieu de rencontre des individus d'organisations de taille et de secteurs différents, ayant des origines et fonctions variées, pour les mettre en situation, les amener à débattre et les conduire

à la meilleure décision. Tous les acteurs sont réunis au sein du certificat « Fraud Risk Management » de l'Université Paris-Dauphine, ou encore dans son « Executive Master : Expert Conformité ». Dans ces programmes, enseignants-chercheurs, salariés d'entreprises et institutionnels communiquent et échangent sur les meilleurs modes de prévention et de lutte contre la fraude. Ainsi, en plus d'acquérir les connaissances juridiques et techniques nécessaire à cette gestion du risque de fraude, le salarié saura mettre en œuvre une stratégie adaptée, tout en bénéficiant d'un réseau susceptible de l'aider dans ses démarches.

L'Université peut accentuer son rôle de partenaire des différentes parties prenantes, unies dans l'objectif commun de comprendre et éviter la fraude, en proposant des analyses et des formations toujours plus ciblées sur leurs besoins.

## II. La déontologie au service de l'entreprise contre la fraude

À l'échelle d'une organisation, la définition et la formalisation de normes collectives, applicables aux membres du groupe, relève de la déontologie. Elle peut se loger au sein d'une charte éthique (alors mal nommée…), d'un règlement intérieur ou de politiques claires énoncées par un management irréprochable et relayées par des formations internes. Elle doit être le fruit de débats collectifs. Pour pouvoir adhérer à ces conventions, le salarié doit pouvoir les comprendre, avoir la possibilité de s'adresser à un référent en cas de doute (un déontologue ou le management) et pouvoir déclencher une alerte le cas échéant[8].

Dans ce contexte, et pour loger la lutte contre la fraude, les grandes entreprises disposant de moyens peuvent mettre en place une direction de l'éthique mais souvent cette problématique est prise en charge, globalement ou de manière dispersée, par d'autres services : direction de la conformité, direction des risques, direction juridique, direction de l'audit interne, direction de la sécurité… En revanche, à l'échelle de la PME, elle va plutôt dépendre du management.

Toutes les entreprises ne possèdent pas de dispositifs, d'outils et de moyens pour prévenir le risque et lutter contre la fraude. Un minimum de « pare-feux », si l'on reprend la terminologie de la cyber-sécurité, reste nécessaire. La prévention est donc un axe majeur à développer au sein des organisations en fonction de leur exposition au risque et de leur volonté d'assurer leur croissance dans le respect de valeurs professionnelles communes.

Mais, quelle que soit la structure organisationnelle adoptée, il est nécessaire d'appréhender les risques, propres à chaque secteur d'activité, de les cartographier et de mettre en œuvre une stratégie globale mettant en avant :

- Une veille juridique et réglementaire accompagnée d'une campagne de communication et de formation (s'assurer par exemple qu'un salarié connaisse les politiques internes, ait déclaré les éventuels conflits d'intérêt…) ;

- La mise en place de procédures claires tenant compte des obligations, mais aussi des règles de management de bon sens visant à réduire les opportunités : la séparation des tâches en est un exemple ;

- Le déploiement d'un système de contrôle du respect de ces règles : permanent au niveau opérationnel et du contrôle interne, ou ponctuel au niveau de l'audit interne ;

- L'ouverture d'un espace de discussion sur ces sujets et, plus globalement, le développement d'une culture d'entreprise ;

- La démonstration d'une justice organisationnelle, notamment au travers d'alertes éthiques, et de communication autour de la détection des fraudes et des sanctions appliquées.

Face à la multiplicité des types de fraudes, le travail de prévention devra être adapté. Ainsi, par exemple :

- Pour limiter la corruption des politiques-cadeaux peuvent être développées ;

- Contre les cybermenaces l'entreprise devra tout d'abord connaître son environnement juridique et technique, maîtriser ses risques spécifiques, se doter d'outils techniques (antivirus…) et de processus de contrôle pour protéger ses données et ses actifs, puis s'assurer qu'à tous les niveaux et en tous lieux, les salariés adoptent les bonnes pratiques en matière de sécurité numérique (charte informatique).

- Face aux fraudes aux faux ordres de virements internationaux[9], la communication auprès des salariés est primordiale (usage des réseaux sociaux, demande de validation d'opérations suspectes déclarées secrètes,

vérification des contacts…), la séparation des tâches et les délégations de pouvoir (signatures multiples) doivent être claires et le temps de réaction en cas de détection doit être rapide.

- Pour dissuader les détournements d'actifs, le sentiment de cohésion et de cohérence du message autour de la lutte anti-fraude sont essentiels. D'autre part, les procédures de contrôle interne, tant sur les mouvements de biens que sur les fonds, doivent être constamment améliorées afin d'éviter les opportunités.

Néanmoins, la prévention peut finalement se révéler insuffisante et l'entreprise devra alors mettre en œuvre des procédés d'investigation en interne, dans le respect des prérogatives de l'auditeur, afin d'étayer une éventuelle procédure pénale. S'il est certain que l'entreprise va analyser la fraude et revoir ses procédures afin de combler la faille trouvée par le fraudeur, chacune définit alors ses propres limites : comment l'entreprise peut-elle gérer la crise, sa communication et le risque d'atteinte à sa réputation ? Comment le mis en cause sera-t-il sanctionné ? La société déposera-t-elle plainte ou non ?

Réalisera-t-elle en interne l'investigation ou sera-t-elle externalisée [10]? Va-t-elle partager son expérience afin d'alerter les autres victimes potentielles ?

L'entreprise ne doit plus être seulement victime ou auteur mais participer au processus de collecte et d'analyse des renseignements, afin d'anticiper et combattre les phénomènes de fraude.

## III. L'évolution du rôle des institutions, garantes de la loi, vers un rôle préventif autant que répressif

Les institutions sont tout d'abord responsables des plans nationaux et stratégies de lutte contre la fraude, définissant les budgets nécessaires à la réalisation des objectifs, les besoins de formation et les plans de communication. Ainsi, et à titre d'exemple, l'un des cinq objectifs de la stratégie nationale pour la sécurité du numérique est d'informer le grand public.

Garantes du respect des lois, l'image des institutions régaliennes[11] est souvent associée au volet répressif. Les entreprises voient souvent comme des contraintes les normes des régulateurs[12], le risque de sanction étant prégnant. Dès lors, les obligations de déclaration de soupçon auprès de TRACFIN sont souvent mal perçues.

Mais rappelons aussi que les différents services d'enquêtes sont aussi là pour recueillir les plaintes et aider les entreprises victimes. Différents services ont été ainsi créés au fur et à mesure des ans permettant de spécialiser les enquêteurs. Dans ce contexte, l'office central de lutte contre la corruption et les infractions financières et fiscales (OCLCIFF), est compétent, depuis 2013, pour diligenter des enquêtes d'envergure en matière de corruption nationale et internationale et plus largement d'atteintes à la probité, d'infractions au droit des affaires (notamment d'abus de biens sociaux), de grande fraude fiscale et de blanchiment de ces infractions. D'autre part, la sous-direction de la lutte contre la cybercriminalité (SDLC) intègre dans son plan d'actions des missions de prévention et de répression.

Ces actions d'information du grand public, mais aussi du tissu économique, permettent de sensibiliser, de prodiguer des conseils et d'encourager les victimes à déposer plainte. Elles peuvent se matérialiser par la présence de membres de ces différents services dans des groupes de réflexion, des colloques[13] mais aussi dans des formations universitaires.[14]

Devant la nécessaire coopération entre entreprises et administration, différentes actions sont développées. À titre d'exemple on peut citer l'accord de partenariat entre les adhérents du Medef (organisations territoriales et fédérations professionnelles) et les services territoriaux de la police judiciaire. Cet accord du 10 mars 2015 repose sur l'échange régulier d'informations en matière de fraudes et d'escroqueries, - dans le respect des impératifs liés au secret des enquêtes judiciaires et la préservation du secret des affaires -, et sur la prévention : « Le Medef informera la police judiciaire de toute infraction dont il pourra avoir connaissance et incitera ses adhérents à en faire autant. Il informera, sensibilisera et mobilisera ses adhérents afin d'assurer les contacts avec les services territoriaux de police judiciaire de leur ressort.
La police judiciaire, quant à elle, pourra informer les entreprises sur les menaces émergentes, mener des actions de prévention, d'information et de sensibilisation et fournir conseils et assistance dans les démarches judiciaires à mettre en œuvre en cas de fraudes ou d'escroqueries avérées. »[15]

On peut noter par ailleurs que le lien entre services de police et entreprises était déjà mis en œuvre par le détachement de certains fonctionnaires dans des services de sécurité, ou de conformité, d'entreprises.

Enfin, le 8 février 2016, et sur un plan très opérationnel, on peut noter l'association inédite d'Interpol avec la banque britannique Barclays, pour renforcer la lutte contre la cybercriminalité. Ce partenariat doit permettre de partager des renseignements et d'affiner les connaissances sur les cyberattaques afin de « pouvoir donner des recommandations concrètes aux institutions, publiques comme privées, pour lutter contre le phénomène », explique Interpol, dont le siège est à Lyon. Au sein de la plate-forme d'Interpol à Singapour (IGCI – Interpol Global Complex for Innovation) seront associés des policiers, des universitaires et des acteurs du secteur privé dont un analyste de la banque Barclays. "L'ampleur et la complexité des cyberattaques aujourd'hui requièrent une coopération dans tous les secteurs", a souligné Noboru Nakatani, responsable de la cellule singapourienne, cité dans le communiqué d'Interpol.

Cette forme de coopération, devrait se développer à l'avenir faisant disparaître les silos.

## Conclusion

Le risque de fraude est permanent et en constante évolution. Le fraudeur a souvent de l'avance, notamment en matière technologique, car son objectif unique est la fraude tandis que l'entreprise, ouverte sur le monde, ne peut consacrer des moyens illimités à la lutte contre celle-ci. Développer l'intégrité au travers de l'éducation et de la formation et sanctionner les comportements non éthiques ne suffiront plus. Demain, les comportements éthiques devront être mieux valorisés.

La démarche proactive et concertée mise en œuvre dans la lutte contre la fraude devra s'accentuer, à l'instar de l'exemple de Barclays et d'Interpol : « Le Complexe mondial transcende le modèle traditionnel répressif en matière d'application de la loi. Il mène un travail de recherche proactif dans de nouveaux domaines et diffuse les toutes dernières techniques de formation. L'objectif est de doter les policiers du monde entier des outils et des capacités leur permettant de relever les défis toujours plus complexes et sophistiqués que présentent les malfaiteurs[16] ». Désormais l'État, dans sa conception régalienne, ne se contente plus d'intervenir à titre répressif mais s'implique dans un processus de prévention en partenariat avec les entreprises, et, plus en amont, auprès du monde universitaire afin de prévenir la fraude plutôt que de la combattre a posteriori.

Ainsi, pour développer une action globale efficace, la coopération inter-entreprises mais aussi entre les secteurs public et privé devra être amplifiée. Et, forte de son activité de recherche et de formation, l'université devrait devenir un lieu d'analyse et de rencontre privilégié pour tous les acteurs unis dans la lutte contre les fraudeurs.

*Notes*

[1] La notion de crime économique induit la volonté de tromper, par différents moyens, à son profit, une victime qui peut être son employeur, un client, un investisseur, un banquier, un assureur ou encore l'État. La classification des types de fraudes n'est pas universelle : dans toutes les cartographies, et notamment celle de l'ACFE, on retrouve les détournements d'actifs, la corruption, la fraude aux états financiers.

[2] Ainsi, seront exclues du périmètre les infractions au Code de commerce (abus de biens sociaux ou entente), au Code monétaire et financier (délit d'initié), au droit fiscal (fraude fiscale), au droit du travail (travail dissimulé) etc.

[3] Dans les entreprises victimes de fraudes externes, comme les assurances ou encore les télécommunications, on trouve aisément des services dédiés dont la dénomination reprend le terme de fraude : « Fraude et Revenue Assurance » par exemple. Ceci ne constitue pas la majorité des organigrammes qui masquent la lutte contre la fraude dans des services différemment dénommés : conformité, contrôle ou audit interne…

[4] Au sein de la fraude économique, la fraude interne ou fraude organisationnelle, est perpétrée par un membre de l'organisation, souvent contre cette dernière, parfois distinction faite entre les salariés et les cadres : c'est le cas le plus fréquemment rencontré des détournements d'actifs. Mais la fraude aux états financiers, ainsi que la fraude fiscale ou la fraude sociale, également internes, lèsent essentiellement l'État ou les actionnaires.

[5] Si le terme de risque systémique s'applique généralement au domaine de la finance, Philippe Trainar, dans la Revue d'économie financière n°101, nous indique : « *Stricto sensu*, le risque systémique correspond à la propagation des problèmes rencontrés par un agent ou un sous-groupe d'agents à tous les autres agents, c'est-à-dire au « système » ». Il le définit plus globalement comme tout risque pouvant, de manière exponentielle, provoquer l'effondrement du système financier, puis du marché jusqu'à celui du système économique incluant celui des États.

[6] JJ Nillès est Maître de Conférence à l'Université de Savoie, membre du laboratoire de recherche IREGE, conseil scientifique pour la société Socrates spécialisée dans l'éthique en entreprise, et auteur de « Ethique et déontologie de la vente » (Economica).

[7] Donald Cressey : *Other People's Money: A Study in the Social Psychology of Embezzlement*. Montclair, N.J.: Patterson Smith, 1973. Pour illustrer ce triangle de la fraude, prenons le cas d'un vol : un salarié est submergé par ses dettes (pression), il constate que l'entrepôt n'est pas surveillé et qu'aucun inventaire physique n'a été réalisé depuis longtemps (opportunité), et il est sûr que d'autres salariés en ont déjà profité ! (rationalisation). Il se laisse tenter et vole de la marchandise au sein de son entreprise.

[8] Il ne s'agit pas là de démontrer l'efficacité du whistleblowing, surtout devant le statut incertain du lanceur d'alerte en France, mais de rappeler que ce dispositif d'alerte éthique, rendu obligatoire par la loi Sarbanes-Oxley en 2002, se généralise.

[9] FOVI ou sa déclinaison en changement de RIB : communication/ prévention : http://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime/L-arnaque-au-president-ou-escroquerie-aux-faux-ordres-de-virement-FOVI

[10] L'externalisation, souvent auprès de professionnels forensic, permet à l'entreprise de ne pas confronter elle-même son salarié. Elle est par ailleurs utilisée quand l'entreprise ne possède pas de compétences internes en data-mining.

[11] Police, gendarmerie, douanes, justice, en particulier dans ce contexte.

[12] AMF, ACPR, TRACFIN notamment

[13] A titre d'exemple on peut rappeler la présence de la SDLC à la conférence sur la cybercriminalité de l'Université Paris-Dauphine du 12 octobre 2015

[14] La BEFTI (brigade d'enquêtes sur les fraudes aux technologies de l'information) par exemple sera présente dès septembre 2016 dans une formation de l'Université Paris-Dauphine sur la sécurité du numérique.

[15] www.cdcf.com/doc-755-protocole-d-accord-medef-dcpj.html

[16] http://www.interpol.int/fr/Internet/À-propos-d'INTERPOL/Le-Complexe-mondial-INTERPOL-pour-l'innovation