1. IDENTIFIER LES RISQUES

Alain Juillet *et al.*

A.D.B.S. | *Documentaliste-Sciences de l'Information*

2014/3 - Vol. 51
pages 30 à 43

ISSN 0012-4508

1 IDENTIFIER LES RISQUES

Protéger les entreprises : une affaire de gestion de l'information par des professionnels du risque

[stratégie] Les changements de l'entreprise, beaucoup plus souple, et de son environnement, avec l'explosion du Big data, mettent au premier rang les risques informationnels. Seuls des généralistes, connaissant bien également le fonctionnement de la firme étendue, peuvent la protéger.

Président du Club des directeurs de sécurité des entreprises (CDSE) depuis mai 2011, **Alain JUILLET** a dirigé de nombreuses entreprises françaises et étrangères avant d'être nommé Directeur du renseignement à la DGSE de 2002 à 2003. Il a ensuite occupé, jusqu'en 2009, les fonctions de Haut responsable à l'intelligence économique, rattaché au Premier ministre. Conseiller au Cabinet Orrick Rambaud Martel, il est également président de l'Académie de l'intelligence économique.

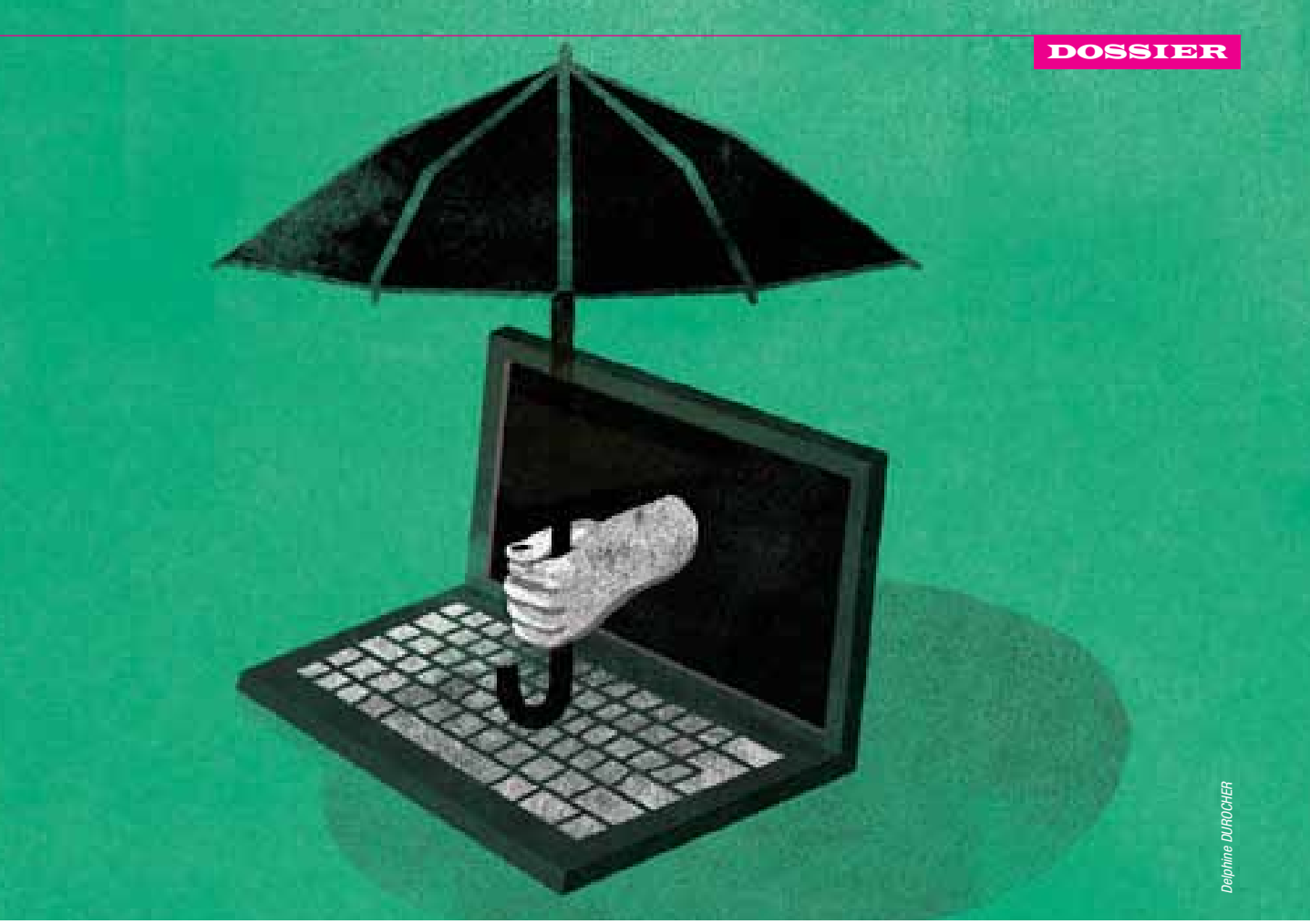
Dans la compétition économique moderne, que beaucoup assimilent à une véritable guerre à la dimension souvent planétaire, le supplément d'information par rapport aux concurrents est devenu le principal moyen pour se créer un avantage concurrentiel dans la conquête de marchés. Quand les entreprises et leurs dirigeants sont à un niveau équivalent sur le plan technique ou industriel, c'est la différence sur le plan informationnel qui génère la création de valeur. Ceci permet d'identifier les menaces existantes ou potentielles et les opportunités qui s'offrent de la manière la plus précise possible. Parallèlement, cette nécessité d'information, cette identification des risques positifs et négatifs potentiels, est essentielle pour assurer la protection des entreprises face aux attaques en tous genres qu'elles subissent ou, mieux encore, pour les anticiper.

Au siècle dernier, la protection concernait essentiellement le patrimoine humain et le matériel. On s'appuyait sur le gardiennage et la surveillance des usines et des bureaux pour empêcher les vols et les détournements de produits, de plans ou de machines. La numérisation des données, les capacités du Big data, les possibilités offertes par le cyber espace, ne serait-ce que dans le développement du Web et des réseaux sociaux, ont déjà complètement changé nos approches. Pourtant, nous ne sommes qu'au début d'une évolution dont personne n'est capable de dire jusqu'où elle ira. Il suffit pour s'en rendre compte de constater la progression exponentielle des volumes d'échanges ou des capacités d'analyse et d'actions dans un temps de plus en plus réduit et la difficulté de leur intégration par les utilisateurs.

Respect de l'éthique

On peut ajouter que l'hyper-concurrence amène un certain nombre d'acteurs à enfreindre les règles éthiques en considérant que tous les coups sont permis. Loin de pratiquer l'intelligence économique, c'est à dire la recherche et l'acquisition de renseignements par des moyens légaux, ils veulent aller plus vite et plus loin par la pratique de l'espionnage. On ne peut donc plus compter sur le respect de la loi pour être protégé d'autant que certains États n'hésitent pas à s'impliquer directement ou indirectement en créant un déséquilibre au profit de leurs protégés. Les révélations de l'affaire Prism sont là pour le rappeler et convaincre ceux qui en doutaient encore. On ne doit pas non plus oublier l'arrivée des organisations criminelles dans le monde des affaires avec pour conséquences des pratiques douteuses pour ne pas dire inacceptables. Tout ceci doit être pris en compte dans les analyses de risques à travers des schémas pas toujours enseignés dans les écoles de management.

De fait, tout ce qui touche à la sécurité, tout ce qui consiste à éviter ou à bloquer les agressions et intrusions en tous genres, s'est complexifié par la multitude de risques auxquels on est confronté. Il faut désormais des professionnels capables de gérer les problématiques de risques dans la transversalité des fonctions de l'entreprise en s'appuyant sur des spécialistes dans chaque domaine. L'impact de chaque



Delphine DUROCHER

risque, sa probabilité d'occurrence, sa complexité de traitement et son impact financier et industriel amènent l'entreprise à privilégier certains d'entre eux et à faire appel à des experts généralement extérieurs pour s'y préparer, organiser la défense et réagir en cas d'attaque.

Dans tous les cas c'est l'importance des enjeux qui a obligé les entreprises à implanter en leur sein des services spécialisés ou à faire appel à des conseils. Ceci nous éloigne chaque jour un peu plus de la société hiérarchique pyramidale traditionnelle pour entrer dans une organisation en râteau dont une part est interne et l'autre externe, avec tous les problèmes d'organisation et de contrôle que cela pose.

Importance de l'immatériel

La recherche, l'identification et le traitement des risques négatifs ou positifs doivent également prendre en compte la localisation géographique des actions. Les lois, la culture et l'environnement sont différents selon le pays ou le continent dans lequel on se trouve. Chacun comporte des problématiques spécifiques, des risques particuliers, un mode différent de traitement des problèmes auquel il faut s'adapter car il n'existe pas de modèle international applicable partout. C'est pourquoi partout le succès repose sur une parfaite information concernant les pratiques locales, les habitudes de la justice et le respect des règlementations. *A contrario*, la méconnaissance provoque l'erreur stratégique destructrice de valeur.

Aujourd'hui, on assiste dans le monde industriel et commercial, en dépit de sa forte médiatisation, à une diminution relative du risque humain ou matériel. Elle est contrebalancée par une montée croissante des atteintes au patrimoine immatériel. Les nouvelles technologies de l'information nous permettent un accès à l'information et son stockage d'une manière immédiate, efficace et plus rapide. En contrepartie, tous nos types de données sont généralement très accessibles aux prédateurs en tous genres, qu'ils soient internes ou externes à l'entreprise. Depuis le rapport Jouyet-Levy[1], chacun sait l'importance de l'immatériel dans la valorisation de l'entreprise, et l'évolution actuelle ne fait que l'amplifier. C'est pourquoi la priorité est d'identifier les éléments clés pour la pérennité de l'entreprise et sa création de valeur, puis de mettre en place les mesures de protection appropriées.

Dans le même ordre d'idées, il faut s'intéresser aux risques issus de la pratique du Web. Sa bonne utilisation donne un avantage compétitif par rapport à ceux qui n'en ont ni l'expertise nécessaire ni ne sont équipés d'outils suffisamment performants. Mais c'est aussi le chemin qui permet à des agresseurs de s'introduire dans vos ordinateurs et vos réseaux pour détourner des informations, consulter vos dossiers ou utiliser votre adresse pour des actions de grande envergure. L'absence d'identité numérique infalsifiable a ouvert des champs d'actions pour les criminels qui ont appris à ////

1. Jean-Pierre JOUYET, Maurice LÉVY, *La France face au défi de l'économie de l'immatériel*. Rapport au gouvernement, novembre 2006

1 IDENTIFIER LES RISQUES

//// transférer ou vider des comptes, à détourner des commandes ou à pirater des données personnelles. Mais ces inconvénients graves ne justifient pas de rejeter en bloc un système qui multiplie nos possibilités. Il faut simplement apprendre à le maîtriser dans tous ses aspects.

On évoque souvent la sécurité informatique des entreprises en pensant que les responsables ont mis en place des systèmes de protection efficaces en optimisant la balance entre leur coût et leur niveau de performance. La réalité, c'est que les *hackers* en tous genres, et parfois les États, sont de plus en plus efficaces dans ce combat permanent entre l'épée et la cuirasse. Tous les spécialistes savent que les attaques ne sont pas réservées qu'aux grandes entreprises. C'est pourquoi il faut non seulement mettre en place des barrières techniques mais surtout commencer par la sensibilisation des salariés à tous les niveaux en commençant par l'encadrement. La gestion de la sûreté informationnelle dans une organisation ne concerne pas que les gestionnaires de l'informatique : c'est un état d'esprit qui doit être porté par la direction et être accompagné par des professionnels de ce type de risque. ■

La collecte d'information, clé de l'analyse des risques

[gestion] La gestion des risques n'est plus une fonction spécifique de l'entreprise. Elle est intégrée à toutes ses actions. Si bien que la collecte d'information, clé de l'analyse des risques, devient une mission essentielle afin de mettre à la disposition des décideurs les éléments nécessaires pour réduire ces risques.

Olivier HASSID est docteur en sciences économiques, directeur général du Club des directeurs de sécurité des entreprises et de la revue *Sécurité & Stratégie.* Chargé de cours à l'Université Paris X Nanterre et collaborateur du Centre international de criminologie comparée de l'Université de Montréal, il est également auteur de nombreux ouvrages dans le domaine de la sécurité et la maîtrise des risques.

olivier.hassid@voila.fr

Jean-Paul A. LOUISOT, titulaire d'un Master of business administration (MBA), Associate in Risk Management (ARM), Fellow of the Institute of Risk Management (FIRM), est directeur pédagogique de CARM Institute. Professeur associé à la Sorbonne (2001-2010), il enseigne à l'Institut catholique de Lille, au sein de masters spécialisés et en formation continue en France, au Maghreb, et en Afrique francophone. Il est l'auteur de nombreux articles professionnels et d'ouvrages spécialisés en *risk management.*

jpl@carmin.org

C'est l'objet de la gestion des risques de permettre aux organismes, et à leurs responsables de tout niveau, de se préparer pour l'improbable. C'est ainsi que la gestion des risques contribue à la définition d'objectifs soutenables, dans la phase de développement de la stratégie, et à leur atteinte effective lors de la phase de mise en œuvre.

La gestion des risques moderne est née dans les années 1960 aux États-Unis de la dérive des coûts d'assurance, et plus particulièrement de l'assurance accidents du travail. Cette gestion s'appuyait à cette époque sur les techniques statistiques, calculs de probabilité et analyse de tendance, c'est-à-dire le domaine de l'actuariat. Ces risques ont une caractéristique commune essentielle : ils sont probabilisables. Ils se prêtent donc à une analyse du passé pour établir des prévisions pour l'avenir, l'espérance mathématique de perte ayant un sens économique et permettant de servir de base à une réflexion stratégique.

Aujourd'hui, la vraie question est celle des risques dont la survenance est très improbable, parfois jugée impossible et qui, malgré tout, se produisent. Les organismes sont confrontés à des aléas dont la réalisation entraîne une catastrophe. L'ampleur de l'incertitude est telle que le passé ne peut plus servir de base de modélisation mathématique et il faut recourir à d'autres approches qui s'apparentent à la construction de scénarios.

Changement de paradigme

De fait, le décideur public ou privé, le *risk manager* ou le directeur sécurité ne peuvent élaborer une analyse et concevoir une stratégie de maîtrise des risques comme il y a cinquante ans. Ils doivent fonctionner en ayant à l'esprit l'éventualité d'un risque extrême non prévu, un choc

qui ne corresponde à aucun qui ne se soit déjà produit dans le passé.

En clair, tout organisme doit opérer dans un contexte d'incertitude extrême. En résumé, il faut passer d'une gestion des risques *a posteriori* à une gestion des risques *a priori*. Cela implique plusieurs conséquences importantes :

- tout organisme peut provoquer des crises qui ont une incidence non seulement sur sa survie mais également sur son environnement. En ce sens, les externalités négatives qu'il est susceptible de provoquer peuvent être tellement graves qu'il ne peut plus prendre ses décisions en faisant abstraction de l'impact possible sur ses parties prenantes.
- la notion de risque, comme analyse objective d'un aléa, est remise en cause par la montée de l'aberrant[1];
- l'approche purement financière des risques comme volatilité des résultats ne rend pas compte des dimensions humaines et sociales de ce phénomène ;
- l'approche par silo n'est plus possible et tous les risques, y compris les risques accidentels ou purs, doivent être gérés globalement ;
- l'approche intégrée suppose de positionner la gestion des risques comme volet de la stratégie globale d'entreprise ;
- la fonction centrale est encore en devenir car le périmètre d'action n'est pas figé ;
- le cœur de la révolution actuelle est l'appropriation des risques et de leur maîtrise, par chacun des acteurs.

Des risques émergents

Fort de cette transformation paradigmatique, la clé de toute gestion reste la connaissance. Pour gérer les risques, il faut donc les connaître, c'est-à-dire les identifier et les évaluer. En un mot, la collecte d'information, clé de l'analyse des risques, devient l'une des missions au cœur de tout programme de gestion des risques. C'est elle seule en effet qui permet de mettre à la disposition des décideurs de tout niveau - stratégique, tactique et opérationnel - les éléments nécessaires à la prise de décision. L'analyse des risques ne doit pas se limiter aux risques standards ou conventionnels, mais intégrer également des risques hors cadres ou ce que les spécialistes appellent des risques émergents[2]. L'éventail des risques doit être élargi et analysé sans parti pris et sans subjectivité. Encore faut-il être en mesure d'envisager l'inattendu et les surprises de façon à ce que les décideurs puissent réagir efficacement et maîtriser la prise de décision en état de stress. Cela suppose également de réunir de manière efficace de plus en plus de parties prenantes (pouvoir public, ONG, université, population, etc.) et d'organiser la communication et la consultation de l'ensemble de ces parties, ce qui n'est pas un exercice facile même s'il est indispensable (cf. schéma 1).

La complexité croissante des organismes et des contextes dans lesquels ils opèrent conduit également à la définition d'une nouvelle approche du management des risques, global et intégré, dans laquelle il est essentiel que chacun des « propriétaires » de risques ait non seulement la responsabilité mais également l'autorité nécessaire pour gérer les risques qui entrent dans son domaine de compétences et qu'il a d'ores et déjà identifiés.

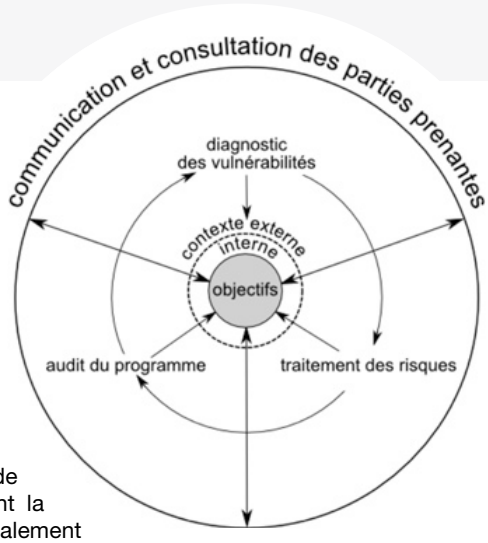


Schéma 1

Le processus de gestion des risques

Source : CARM Institute, J.-P. Louisot

Aussi, afin d'aider les dirigeants à mieux apprivoiser l'incertitude, Jim DeLoach[3] propose une démarche en six points.

- Tirer profit de la valeur temps des pionniers : cela permet aux dirigeants de saisir les opportunités et de prendre des mesures de contrôle avant la concrétisation de toute menace.
- Veiller à ne pas trop valoriser les données historiques, les anecdotes, les sondages et les articles spécialisés : il est essentiel de valider les faits en questionnant les méthodologies et les hypothèses sous-jacentes.
- Accepter de faire face au changement, qui est inéluctable : il faut pouvoir identifier très en amont les éléments précurseurs du changement, et en anticiper les conséquences.
- Éviter les « angles morts » au sein de l'organisme : il faut se méfier, en particulier, de tous les modèles dont les hypothèses sous-jacentes reposent sur le postulat que l'avenir sera un reflet fidèle du passé.
- Veiller à aligner les hypothèses stratégiques avec les réalités du terrain : il faut rester en prise avec l'extérieur pour recueillir l'information pertinente qui permettra de modifier les hypothèses si elles se révèlent dépassées ou obsolètes.
- S'assurer que toutes les craintes des responsables sont mises sur la table : il faut organiser au besoin des ateliers de réflexion pour discuter l'impensable et se poser la question de la préparation de la réponse si de telles circonstances se produisaient.

En résumé, la gestion de l'incertitude suppose de s'appuyer sur une stratégie construite sur des hypothèses réalistes, prenant en compte les contraintes du contexte, présentes et futures, de prendre le temps de la réflexion sur l'inattendu et les scénarios qui pourraient faire dérailler la stratégie, et préparer des réponses aux situations de rupture.

La notion de risque stratégique n'est pas nouvelle ni sans doute figée mais, dans un ////

1. Bertrand ROBERT, *Nouvelles pratiques en management des crises.* Argillos, 2002 et *La Gestion de crises en agroalimentaire : anticipation et pilotage.* Afnor, 2002

2. Catherine Antoinette RAIMBAULT, Anne BARR, *Emerging Risks, A strategic management guide.* Gower Publishing Limited, 2012

3. Jim DELOACH, « Knowing What You Don't Know. Six steps organizations can take to manage uncertainty ». NACD Directorship, November 27, 2013, www.directorship.com/knowing-what-you-dont-know

1 IDENTIFIER LES RISQUES

//// monde dont la complexité et la volatilité ont déjà été soulignées, la gestion des risques stratégiques revêt une nouvelle urgence qui se reflète dans une enquête récente. En effet, dans l'enquête conduite par Forbes pour Deloitte auprès de 300 entreprises[4], 94 % d'entre elles ne se contentent pas de renforcer leur attention sur les risques stratégiques mais revoient complètement leur approche pour associer la gestion des risques dans leurs processus de développement stratégique et de planification de façon à prendre en compte l'impact total de ces risques, à court, moyen et long terme.

Des banques de données pour anticiper l'avenir

Toutefois, cette extension stratégique de la gestion des risques implique d'intégrer dans son périmètre toutes les fonctions qui visent à assurer le développement soutenable de l'organisme dans un contexte volatile. Sans que la liste soit limitative, on peut penser, à côté de la sécurité, de la gestion des risques et de l'intelligence économique, dans un premier cercle à la qualité, à la logistique, à l'hygiène et sécurité, à la communication interne et externe, à l'environnement. Mais, dans un second cercle, on comprend que toutes les grandes fonctions

4. *Exploring Strategic Risk. 300 executives around the world say their view of strategic risk is changing.* Deloitte Touche Tohmatsu, 2013.

5. Hubert SEILLAN, *Piloter par le management global des risques.* Éd. Préventique (coll. Les kits de Préventique), 2013

Excès d'information, défaut de formation : les nouveaux risques de la finance

[ressources humaines] Les lois destinées à lutter contre les dérives de la finance engendrent un stress considérable pour les financiers auxquels il est demandé de gérer une information toujours plus importante et complexe. Au risque du « *burn out* ».

Coach, consultante et auteur, **Marie-Christine DUPUIS-DANON** est spécialiste de la lutte contre la criminalité financière. À ce titre, elle a conseillé de nombreux gouvernements dans la gestion de leurs finances publiques avant de rejoindre les Nations Unies comme conseiller anti-blanchiment. Elle a fondé et dirige le Cabinet C3COM qui accompagne par le coaching les entreprises soumises à de fortes pressions dans le domaine de l'éthique et des risques complexes.

contact@c3comcoaching.fr

Pour limiter les risques liés aux dérives de la finance, la réponse première des États a été d'élaborer des textes de loi de plus en plus restrictifs pour tenter de contrôler la circulation de l'argent. Le 11 septembre 2001 puis la crise économique ont accéléré le processus de réglementation du système financier international pour en traquer les flux liés à une activité criminelle : lois anti-blanchiment, lois anti-financement du terrorisme, lois anti-corruption, chasse à la fraude fiscale, normes prudentielles, etc. La pression s'est incontestablement accentuée au fil des ans sur les secteurs financiers soumis à une régulation contraignante, sommés de se mettre en conformité avec les dispositifs juridiques élaborés par les instances internationales et de transmettre leurs soupçons de malversation à une autorité nationale compétente, comme Tracfin[1] en France. À chaque tour de vis supplémentaire, de nouvelles contraintes viennent peser sur les professionnels assujettis. Ils doivent rassembler toujours plus d'informations pour limiter les risques et rester en adéquation avec les lois.

Pour les organismes financiers (métiers de la banque, de l'assurance et professions associées) soumis à ce cadre contraignant, l'évaluation des risques se résume encore souvent à vérifier la bonne intégration des dispositions obligatoires dans les processus opérationnels. Il s'agit en effet de limiter le risque juridique (de poursuites judiciaires) ou le risque réputationnel (d'atteinte à l'image) en s'assurant de la bonne adéquation entre ce qui est demandé et ce qui est mis en œuvre pour satisfaire à ces obligations.

À voir le nombre d'affaires retentissantes ces dernières années (qui ne sont que la partie visible de l'iceberg), la politique de contrôle des risques semble avoir occulté une dimension potentiellement explosive : le facteur humain. Comment les hommes réagissent-ils à ce nouveau contexte professionnel ? De quel accompagnement ont-ils bénéficié pour intégrer les nouvelles règles du jeu de ces métiers complexes, stressants, soumis à la pression du résultat ? Et si trop de règles s'avérait finalement contreproductif et exposait les entreprises financières à des risques aussi graves que mal connus ?

1. www.economie.gouv.fr/tracfin/accueil-tracfin

sont impliquées et doivent inclure la dimension risque dans toutes leurs réflexions.

De plus, si l'irruption du Big data et du *cloud computing* est prise en compte, elle permet de développer et de maintenir à jour la « *business analytics* », croisement de banque de données qui seules permettent de disposer de ces informations indispensables au discernement de l'avenir. Mais il est clair que l'ensemble des fonctions qui ont pour mission de renforcer la résilience des organismes, et donc de la société, doivent collaborer de façon encore plus intime dans le cadre d'une stratégie de gestion des risques définie au niveau du conseil d'administration. C'est le seul moyen effectivement de prendre en compte les surprises évoquées plus haut, c'est-à-dire ce que le radar des risques émergents ne détecte pas encore.

C'est précisément pour cela que *risk management*, sécurité et intelligence économique doivent travailler de concert pour éclairer les décideurs et renforcer la sécurité globale des objectifs, non seulement lors de la prise de décision, mais encore en accompagnement de leur exécution pour prendre en compte cet inconnu lorsqu'il se manifeste, même avec des signaux faibles. Ils se trouvent donc associés dans un véritable management global, tel que défini par Hubert Seillan[5] dans la création de valeur et l'optimisation de la performance. ■

Cinq facteurs de stress majeurs, autant de nouveaux risques pour l'entreprise

Les environnements à forte contrainte juridique s'avèrent des vecteurs de stress qui fragilisent la bonne intégration des consignes données aux équipes. Généralement, les financiers répugnent à en parler mais, interrogés individuellement et sous couvert d'anonymat, ils ne cachent ni leur exaspération, ni pour certains leur mal-être. Les facteurs de stress qui se dégagent se classent en cinq familles : les deux premières sont relativement classiques et donc prises en charge (tant bien que mal) par les banques ; les trois autres sont plus pernicieuses.

Éric NOSAL

L'accumulation de règles contraignantes

Connaître son client, vérifier l'origine et la destination des fonds, s'assurer qu'une opération ne relève pas de la corruption, ni de la fraude fiscale, ni de la violation d'un embargo, ni, ni... Les règles sont de plus en plus nombreuses et complexes : elles doivent être comprises, assimilées et intégrées à tous les niveaux de l'organisation. Les salariés reçoivent l'information et la formation correspondante mais la peur est là de ne pas tout comprendre, de ne pas retenir toutes les bonnes pratiques.

La peur d'omettre de respecter une règle importante

Le non respect des règles engage la responsabilité de l'entreprise mais aussi celle du salarié : l'entreprise qui a failli à sa diligence s'expose à des poursuites judiciaires (aggravées si elle a agi délibérément). Le salarié qui commet une erreur de bonne foi n'est pas exposé à des poursuites pénales. Il n'empêche que son emploi est menacé. En tout état de cause, la gravité des conséquences génère des stress forts (peur de la faute grave, peur de ne pas détecter une opération criminelle ou terroriste, etc.).

Ces deux familles de stress sont voisines et leurs effets sont connus des employeurs financiers. Sur l'individu, les conséquences peuvent aller d'un malaise à un vrai décrochage (impression de non maîtrise de son métier, regret que ce dernier change de nature, peur de ne pas être à la hauteur, impression d'être débordé). Le salarié qui commet une faute peut être tenté de la dissimuler par peur des conséquences, avec des effets gravissimes.

Face à ce risque croissant de dérapage, les banques renforcent le contrôle interne des ////

1 IDENTIFIER LES RISQUES

//// opérations et les services des ressources humaines mettent en place des plans de prévention des risques psycho-sociaux. Cela suffit-il à prévenir les défaillances ? Pas toujours car trois autres facteurs de stress et de risques sont globalement laissés de côté.

Le dilemme des injonctions paradoxales

« *Respectez scrupuleusement les règles prudentielles MAIS prenez tous les risques pour gagner plus* »... Mises en lumière par Gregory Bateson[2] dans les années cinquante, les injonctions paradoxales (*double bind*) contraignent le sujet à désobéir à l'une pour obéir à l'autre, d'où une tension insupportable pour l'individu. Les injonctions de ce type sont de plus en plus nombreuses dans les métiers financiers. Sur les marchés, la contradiction entre performance et régulation des risques ne dit pas son nom mais son ombre hante les *floors* de *trading*. Autre exemple : les règles de connaissance du client (Know your client) imposent une entrée en clientèle longue, laborieuse, voire intrusive donc peu appréciée. Le chargé de clientèle en gestion privée va devoir faire preuve de diplomatie au risque de perdre le client au profit de la concurrence. L'injonction paradoxale se formule alors ainsi : « *Soyez compliant*[3] *ET nouez ou développez d'excellentes relations client tout en augmentant votre portefeuille d'actifs sous gestion* ».

Le poids de sa décision s'exerce aussi à l'encontre de sa tutelle. Prenons par exemple le même chargé de clientèle concevant un soupçon à propos d'évasion fiscale. S'il alerte sa hiérarchie, il craint d'apparaître comme paranoïaque (surtout si son soupçon s'avère infondé) : la banque ne va-t-elle pas lui retirer son portefeuille ? Ou le « placardiser » ? Son client risque-t-il de l'apprendre ? Sa prime de résultat pourrait-elle en souffrir ? Mais s'il tait son soupçon, il sait qu'il peut commettre une faute grave car il est tenu d'avertir sa hiérarchie en cas de soupçon… Au final, l'humain est seul face à sa décision et il sait qu'elle peut avoir des conséquences lourdes.

Au-delà du malaise et de la difficulté du salarié à arbitrer entre les injonctions paradoxales, il pourrait avoir du mal à évaluer et à bien négocier les prises de risques, mettant ainsi potentiellement en danger l'activité de son employeur.

L'obligation de transparence

La frontière qui délimite les opérations protégées par le secret professionnel est subtile et elle évolue avec les nouvelles exigences dérivées des amendements aux législations anti-blanchiment. Ainsi, pour de nombreux professionnels, l'obligation de déclarer ses soupçons en cas d'opération douteuse constitue un cas de conscience difficile à résoudre, surtout depuis que les infractions de nature fiscale sont entrées dans le champ des infractions sous-jacentes au blanchiment d'argent. En réaction à cet impératif de transparence, on assiste au développement de cultures du secret et à une sacralisation de la confidentialité parfois excessive ou injustifiée.

Les facteurs de pression contextuels

Retenons-en deux, pertinents dans le monde de la finance. Le facteur temps est le plus évident : la finance et notamment les marchés financiers sont régis par le temps court : simultanéité de l'accès à l'information, de son traitement et de la décision. Difficile, dans la frénésie, de discerner le pourquoi du comment et le bien du mal.

Il s'y ajoute souvent un facteur rémunération : le mode de récompense de la performance par l'attribution d'un bonus lié aux gains tend à orienter l'action vers le résultat à tout prix en incitant parfois à prendre des risques excessifs. L'effet pervers des bonus est étudié par le champ de la psychologie sociale portant sur la finance comportementale. Premier constat : le bonus fait office d'étalon de référence pour les traders. Deuxième constat : l'attribution d'un bonus comporte une dimension symbolique qui dépasse la gratification financière ; qu'il baisse d'une année sur l'autre et l'on voit fréquemment surgir des troubles psychologiques liés à la perte de statut, aux sentiments d'échec et de déclassement et ce, indépendamment des performances des marchés eux-mêmes. Principale conséquence : avec la variation de ce point de référence (qui fluctue avec les variations des marchés), on observe que les comportements de *trading* tendent vers des prises de risque de plus en plus élevées.

Derrière la finance, il y a... des financiers

Alors que faire ? Il n'existe pas de recette miracle... Sans règles ni lois, le monde financier deviendrait vite la pire des jungles. Mais croire que c'est en réduisant sans cesse les trous du tamis que l'on parviendra à contrôler le monde de la finance est une absurdité fonctionnelle. Et cette pression grandissante accroît le risque de voir le facteur humain se manifester de manière explosive. Alors, il convient de revenir à de la mesure, du bon sens, de l'équilibre. Il est indispensable de prendre le temps du recul, d'offrir aux individus et aux équipes la possibilité de s'exprimer, dans un espace de parole sécurisé (prévu par les institutions financières mais extérieur à la hiérarchie), pour les aider à mieux discerner les objectifs du quotidien des finalités qui confèrent un sens à l'action humaine. ■

2. Chercheur américain, Gregory Bateson s'est intéressé à la communication. Il est l'un des fondateurs de l'école de Palo Alto (Source Wikipédia).

3. La « compliance », anglicisme courant dans les institutions financières, désigne l'ensemble des obligations liées à la conformité obligée aux dispositions des réglementations bancaires et financières (directives, lois, normes de droit, règlements).

Le risque informationnel
au filtre du droit

[droit] Les individus peuvent être victimes de rumeurs et de l'absence du droit à l'oubli mais aussi des atteintes au droit d'auteur ou de surveillance exacerbée. Tandis que les entreprises peuvent voir leurs données volées et leurs secrets des affaires dévoilés…

Avocat à la Cour, ancien auditeur de l'IHESI (désormais INHESJ) et de l'IHEDN Session IE, Maître **Thibault du MANOIR DE JUAYE** a publié plusieurs ouvrages dont les deux derniers sont *Le droit de l'intelligence économique* et *Les robes noires dans la guerre économique*. Conseiller prud'homme à Nanterre, il a été responsable de la commission d'Intelligence économique de l'Ordre des avocats de Paris, pendant près de 2 ans.

juaye@france-lex.com, www.France-lex.com

Le juriste ou l'avocat appréhende le risque informationnel à l'aune des contentieux qu'il traite ou dont il a connaissance et que l'on regroupera en deux grandes catégories :

- celle concernant le risque de voir une information appréhendée contre la volonté de son détenteur ;
- celle concernant la diffusion de fausses informations, d'informations mensongères, de manière volontaire ou non.

Le droit des risques informationnels est une matière vivante que, en raison de son ampleur, il est impossible d'aborder dans sa totalité. On se bornera ainsi à examiner les points qui suscitent le plus de débats ou qui sont d'une actualité brûlante.

La protection de l'information

De tout temps, on a cherché à protéger son droit sur l'information que l'on possède soit en la gardant secrète, soit en bloquant sa réutilisation en s'appuyant sur les dispositions du Code de la propriété intellectuelle (CPI). Parfois, les infractions résultent d'une méconnaissance des textes ou d'un manque de vigilance. Des entreprises ont été ainsi poursuivies parce que, en toute bonne foi, leurs documentalistes avaient dupliqué des articles de presse sans s'assurer qu'ils en avaient le droit.

Des textes récents, comme celui sur le brevet européen[1] ou, en France, sur la répression de la contrefaçon[2], ne seront pas évoqués dans cet article. La sécurité de l'information, qui passe également par la sécurisation physique des locaux - ce qui conduit à s'intéresser au droit de la sécurité privée avec notamment la récente mise en place du Conseil national des activités privées de sécurité (Cnaps) -, ne sera pas abordée non plus. Nous examinerons ici les principaux risques informationnels vus au filtre du statut des salariés, du statut limité des bases de données et du secret des affaires.

Le statut des salariés

Lorsque l'on aborde la protection de l'information, on disserte abondamment sur les risques que font courir les salariés à l'entreprise. Mais n'oublions pas que les salariés sont la principale source de richesse de l'entreprise et qu'une politique de motivation est souvent plus efficace que des mesures coercitives.

La sécurité de l'information est l'affaire de tous les salariés et non du seul service informatique ou du département chargé de la sécurité.

• Sauvegarde et destruction de données

L'un des principaux risques auxquels sont confrontées les entreprises est la disparition de données à la suite d'un acte volontaire d'un salarié ou d'une absence de sauvegarde. La jurisprudence considère qu'un salarié qui efface volontairement des données commet une faute grave. Ce type de faute rend le maintien du salarié dans l'entreprise impossible et celui-ci peut donc être mis à pied dès la constatation des faits. En principe, l'acte a été accompli dans l'intention de nuire à l'entreprise et le salarié peut être licencié pour faute lourde et perdre tout droit sur les sommes que pourrait lui devoir son employeur (solde de congés payés, indemnité de licenciement, etc.). En outre, il peut être condamné à réparer le préjudice qu'il a causé. Mais les tribunaux qualifient avec réticence ces faits de faute lourde et se rangent souvent à l'affirmation du salarié qui prétend avoir effacé par mégarde des données sans importance.

Le fait de ne pas procéder à des sauvegardes demandées par l'employeur est considéré comme une cause réelle et sérieuse de licenciement, à l'image de ce qu'a décidé la cour d'appel de Riom en mars 2014[3]. La cour d'appel d'Amiens abonde dans le même sens[4]. Enfin, les salariés sont tenus de communiquer à l'entreprise les informations dont elle aurait besoin, par exemple un mot de passe[5]. Il s'agit d'un élargissement de la notion de loyauté dans l'exécution du contrat de travail.

• Droit d'auteur et salariés

Le droit d'auteur peut se définir comme la production intellectuelle formalisée traduisant l'expression de la personnalité du salarié. De ce fait, un grand nombre de productions réalisées dans l'entreprise relève du droit d'auteur : rapports, dessins réalisés le cas échéant par ordinateur, etc. Le CPI ne prévoit pas cependant de transfert automatique ////

1. Le 14 février 2014, l'Assemblée nationale a adopté la loi de ratification du Traité sur le brevet européen.
2. Adopté le 11 mars 2014.
3. Cour d'appel de Riom, 11 mars 2014, n° 12/00524
4. Cour d'appel d'Amiens, 4 septembre 2012, n° 11/04861
5. Cour d'appel de Douai, n° 2299/13, 13/00258

1 IDENTIFIER LES RISQUES

/ / / / des droits de l'auteur - salarié au profit de l'entreprise - et affirme même le contraire[6]. La situation est intenable pour l'entreprise qui rémunère un salarié sans être propriétaire des fruits de son travail. Il a donc fallu dans des domaines sensibles des textes spéciaux, par exemple pour les logiciels[7] ou pour les agents publics[8], qui organisent un transfert automatique des droits au profit de « l'employeur ». Quant au régime des œuvres collectives auquel l'entreprise pourrait recourir, il est parfois difficile à mettre en œuvre.

Il existe un contentieux émergeant de salariés qui revendiquent la paternité des œuvres et poursuivent leur employeur pour contrefaçon. Ainsi, le salarié d'une agence publicitaire a revendiqué avec succès des droits sur une brochure qu'il avait créée[9]. En revanche, un ex-créateur de Van Clef et Arpels n'a pu se voir attribuer la qualité d'auteur. Cette problématique du salarié titulaire des droits sur son œuvre est loin d'être anodine au regard des réflexions sur le secret des affaires. Comment, en effet, une entreprise peut-elle avoir un droit au secret sur ce qui appartient à son salarié ?

• La surveillance des salariés

La surveillance n'a pas forcément pour vocation de déceler d'éventuelles fraudes ou détournements. Elle peut avoir pour but d'améliorer la qualité des services (ce que l'on voit par exemple chez les opérateurs téléphoniques). Mais une telle surveillance peut être attentatoire à la vie privée et les limites qui lui ont été posées ne peuvent qu'être approuvées.

Pour être licite, la surveillance doit remplir trois conditions :

- Le moyen doit être proportionnel au but poursuivi (C. Trav, art. L.1121-1). Par exemple, il n'est pas possible d'organiser une fouille générale et systématique des salariés ou d'écouter ceux qui ne sont pas en contact avec la clientèle.
- Le salarié doit être averti des mesures de surveillance utilisées. C'est généralement la raison pour laquelle il est difficile pour une entreprise de recourir à des détectives privés.
- La mise en place d'un procédé de surveillance suppose l'information et la consultation préalables du comité d'entreprise (C. Trav, art. L.2323-32).

C'est sur la base de ces principes que seront rendues des décisions nombreuses et, au cas par cas, dans plusieurs domaines : surveillance des lignes téléphoniques des salariés, géolocalisation, vidéo-protection, accès aux mails des salariés. Les courriels sont considérés comme professionnels sauf si le salarié a apposé distinctement la mention « personnel ». L'employeur peut avoir accès, dans certaines conditions et sur autorisation de justice, à ces messages.

Définition réduite des bases de données

Lorsque la loi sur la protection des bases de données a été adoptée[10], beaucoup d'entreprises espéraient voir leur patrimoine informationnel protégé. Mais, à l'aune des décisions de jurisprudence, la protection s'avère assez restreinte. Les victimes peuvent toutefois se retrancher derrière d'autres fondements juridiques, comme la concurrence déloyale.

Selon l'article L.112-3, alinéa 2 du CPI, la base de données est « *un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen* ». Peut donc être protégé à ce titre, par exemple, un guide papier comparatif des fournisseurs de pièces automobiles. Mais toute base de données ne sera pas pour autant protégée.

Ce même code précise, en effet, que le contenu d'une base de données bénéficie d'une protection lorsque « *la constitution, la vérification ou la présentation de celui-ci attestent d'un investissement financier, matériel ou humain substantiel* » (art. L341-1 du CPI). Ainsi, la société Sarenza, qui vend des souliers et des chaussures en ligne grâce à un fichier de plusieurs millions d'adresses mail, n'a pas été considérée comme constituant une base de données ; la société Se loger n'a pas constitué de bases de données au sens légal du terme malgré ses dizaines de milliers d'annonces[11]; et la société M6 n'a pas créé de base de données au sens juridique du terme pour ses émissions en *replay*[12].

Le secret des affaires

L'Assemblée nationale a adopté le 23 janvier 2012 une proposition de loi sur le secret des affaires, à l'initiative du député Bernard Carayon. Ce texte a rencontré beaucoup de critiques, notamment parce qu'il n'apportait aucune protection supplémentaire par rapport à ce qu'avait défini la jurisprudence. Les tribunaux avaient été confrontés, en effet, à plusieurs hypothèses :

- l'information est donnée volontairement à une personne qui la détourne : la répression repose sur l'abus de confiance sanctionné par le Code pénal ;
- l'information est appréhendée contre la volonté de son détenteur, par exemple par *hacking*. La répression est alors fondée sur des textes réprimant l'intrusion informatique.

Il n'existe que peu de trous dans la raquette.

C'est dans ces conditions que la Commission européenne a élaboré une proposition de directive destinée à protéger le secret des affaires[13], rendue publique le 28 novembre 2013. Ce texte, fortement inspiré des dispositions qui existent aux États-Unis, s'appuie

6. Code de la propriété intellectuelle, art. L111-1

7. Loi du 3 juillet 1985

8. Loi n° 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information

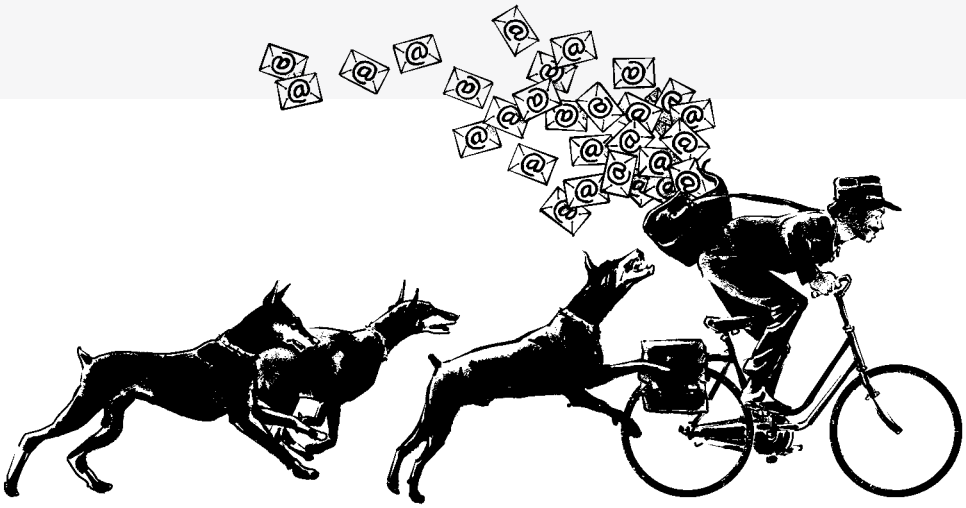
9. Cour d'appel d'Aix-en-Provence, 21 mars 2013, n° 2013/ 121

10. Loi n° 98-536 du 1er juillet 1998 concernant la protection juridique des bases de données.

11. Cour d'appel de Paris, arrêt du 15 novembre 2013

12. Cour de cassation, 31 octobre 2012, rejet n° 11-20.480

13. http://ec.europa.eu/internal_market/iprenforcement/trade_secrets/index_fr.htm



Éric NOSAL

sur le principe suivant : à partir du moment où l'entreprise prend des mesures de nature à assurer la protection de l'information, celle-ci a un caractère secret et toute personne qui en aurait connaissance sans l'accord du titulaire sera condamnée à réparer le préjudice résultant de cette appropriation.

La proposition de directive recourt ensuite à des mécanismes juridiques qui ont fait leurs preuves en matière de propriété intellectuelle, comme des procédures d'urgence et des mesures d'indemnisation.

Bien entendu, il existe des tempéraments à la protection du secret des affaires pour éviter que la presse ne soit bâillonnée ou que l'on ne puisse dénoncer un fait contraire à l'intérêt général.
Enfin, la justice est normalement publique et il suffit d'assister à certaines audiences pour capter des secrets. La proposition de directive envisage donc un « huis clos » pour protéger le secret des affaires.
Cette directive doit encore être adoptée, ce qui relève d'un long parcours. Dans d'autres pays européens, le sujet est moins sensible qu'en France.

L'e-reputation

Le droit est fait de principes qui s'entrechoquent, se télescopent et se contredisent. Internet en est un bon exemple. Il y a d'un côté la liberté de s'exprimer à laquelle personne ne peut renoncer dans une société démocratique et, de l'autre, la protection de la vie privée que tout un chacun revendique. Difficile pour les juges et le législateur, qu'ils soient français ou européens, de trouver un bon équilibre et ce d'autant plus que nombre de réseaux sociaux sont situés outre-Atlantique où la législation est fort différente de la nôtre.

Comment réagir à une rumeur ?

Des entreprises comme des particuliers sont victimes de cyberharcèlement et de rumeurs dont la durée de vie est d'environ un mois, ce qui est bref au regard de la longueur d'une procédure judiciaire. Et chaque étape de la procédure peut réveiller une rumeur endormie. D'où le dilemme : si je réagis judiciairement, la rumeur risque de durer, voire de s'enfler, mais si je m'abstiens, ne vais-je pas l'accréditer ? Dès lors, la riposte à la rumeur va nécessiter une double compétence : celle du juriste ou de l'avocat et celle d'un communicant.

Il convient, tout d'abord, d'effectuer un constat d'huissier. L'acte de cet officier ministériel a pour but de figer la preuve mais également d'offrir un choix de compétence, puisque le tribunal saisi sera celui du lieu du constat. Ensuite, on peut engager une procédure de référé[14] pour faire retirer les éléments litigieux. Pour obtenir des dommages-intérêts, il faut introduire une procédure au fond, qui prend de 12 à 18 mois.

Dans la pratique, la principale difficulté est d'identifier les médias qui diffusent la « fausse » information. Le plus souvent, l'attaque se produit concomitamment sur plusieurs médias tels que YouTube, Facebook, des blogs, etc. Il faut alors saisir chacun des responsables de ces médias par voie de justice pour les obliger à donner les adresses IP des personnes ayant fait courir la rumeur. Quant aux fondements de retrait des informations, ils sont divers : loi Informatique et libertés, atteinte à la vie privée, diffamation, etc.

La publicité des décisions de justice

Les décisions de justice sont publiées, pour certaines, sur le site de Légifrance et, pour toutes les décisions des cours d'appel et de la Cour de Cassation, sur des sites spécialisés comme Lexis Nexis.
Elles sont anonymisées pour les particuliers, mais le nom des entreprises demeure. Et l'on y trouve une mine d'informations et de documentation, notamment pour les veilleurs. Mais peu d'entre eux ont une formation juridique. À l'inverse, les juristes ne sont pas formés à la collecte et à l'analyse d'informations.
Par ailleurs, les justiciables n'hésitent pas à mettre en ligne les décisions qui les concernent et ce comportement peut provoquer un ////

14. Le référé est une procédure d'urgence qui permet d'obtenir une décision en 15 jours ou un mois.

1 IDENTIFIER LES RISQUES

//// phénomène « boule de neige ». Un internaute prend connaissance d'une décision de justice et s'estime dans la même situation que le justiciable bénéficiaire de la décision ; il va alors saisir les tribunaux, ce qu'il n'aurait sans doute pas fait dans d'autres circonstances.

Le droit à l'oubli

Les règles établies en 1995 au niveau européen sur le respect de la vie privée sont totalement obsolètes. Comment en effet parler de vie privée alors que tout un chacun se répand dans les réseaux sociaux sur ses amis, ses activités, ses bonnes et mauvaises fortunes ? Quelle est la législation applicable à l'heure où sont dupliquées les données grâce au *cloud computing* ?

La directive actuellement en vigueur va être remplacée par un Règlement européen qui prévoit notamment un droit à l'oubli[15]. Il sera dès lors possible d'obtenir le retrait du Web d'informations gênantes.

Il ne faut donc pas voir le droit comme un outil utilisé seulement pour poursuivre des dérives. Il faut surtout le voir comme un outil qui joue de manière préventive un rôle organisateur et qui, à ce titre, diminue et prévient les risques. ■

15. Voir à ce sujet l'article « De nouvelles dispositions pour protéger les données personnelles » de la rubrique Droit, p. 23

Cloud, externalisation : quels risques pour la circulation des données hors de l'entreprise ?

Délégué général de European Outsourcing Association - France, **Georges COUVOIS** a été chairman de l'European Federation of Financial Executives Institutes (EFFEI) et banquier. Membre du Consultative Advisory Group (CAG) de l'International Auditing and Assurance Standards Board (IAASB, New York), de l'association Culture, économie, défense (CED), de l'Association nationale des directeurs financiers et de contrôle de gestion (DFCG), il fait partie du PressClub de France et a été membre d'honneur du Prix Turgot qui récompense les meilleurs livres d'économie financière. Il est aussi professeur et conférencier dans de grandes écoles de commerce et de gestion.

gcbm@wanadoo.fr

[transfert] L'externalisation est pratiquée par toutes les entreprises. Mais elle est parfois très risquée. Des solutions permettent de se préserver des dangers pouvant impacter l'activité, la rentabilité ou l'image de la firme.

L'externalisation (*outsourcing*) est devenue en quelques années un phénomène incontournable que toutes les entreprises ont envisagé ou ont mis en œuvre. Mais ces pratiques sont quelquefois très risquées, allant jusqu'à mettre en péril l'entreprise elle-même ou une branche de son activité. Elles doivent donc rechercher les solutions leur permettant de se préserver des risques pouvant impacter leur activité, leur rentabilité et leur image.

Les activités déployées sous la forme de l'externalisation sont fréquemment liées à la création de valeur et, surtout, s'accompagnent systématiquement d'un transfert d'information vers l'extérieur de l'entreprise, qu'il s'agisse de savoir-faire, de données informatiques ou de *process*. Aussi, l'externalisation ne peut être comprise comme de la simple sous-traitance. De fait, ces transferts importants de ressources que sont la technologie, le savoir-faire, une certaine image de l'entreprise ne peuvent pas être pris en défaut. La restitution et les travaux réalisés autour de toute externalisation ne doivent en aucun cas nuire à l'entreprise, si des irrégularités étaient commises ou si les travaux ne correspondaient pas à la conformité globale, voire étaient totalement décalés par rapport à la vision extérieure des marques de l'entreprise.

Au cœur de cette activité se trouve désormais une complexité qui intègre plusieurs prestations : les prestations techniques (*Information Technology Outsourcing* ou ITO) telles que l'informatique et les télécommunications, les prestations métiers (*Business Process Outsourcing* ou BPO) et les prestations à haute valeur ajoutée (*Knowledge Process Outsourcing* ou KPO). Les évolutions récentes ont vu aussi apparaître le *cloud computing*, une nouvelle forme de *sourcing* et de fourniture de services. Toutes ces pratiques mettent en œuvre des ensembles de moyens ou de services visant à améliorer sensiblement les coûts, à répondre aux évolutions technologiques et, avec le *cloud computing*, à intégrer l'utilisation des réseaux à la demande.

Parmi les nombreux secteurs qui font appel à l'externalisation, ceux de la banque et de l'assurance représentent près de 40 % du total. L'offre se traduit par des centres performants essentiellement localisés en Asie-Pacifique

Éric NOSAL

(Inde, Chine, Ceylan, Île Maurice, etc.) pour 55 % d'entre eux, en Europe de l'Est (Pologne, Hongrie, Slovaquie, Tchéquie, Roumanie, Estonie, etc.) pour 20 %, en Amérique latine (Brésil, Argentine, Mexique) pour 12 % et en Afrique (Maroc, Tunisie, Afrique du Sud, etc.) pour 8 %.

Pourquoi externaliser ?

Externaliser est une décision stratégique. Dans un projet de *sourcing* traditionnel, différentes directions de l'entreprise se trouvent impliquées, en particulier la Direction des systèmes d'information et, à ses côtés, la Direction générale, la Direction juridique et la Direction financière. D'autres sont parties prenantes de fait, comme la Direction des ressources humaines et la Direction des achats.

Dans un projet de *cloud*, la prise de décision n'est plus forcément collégiale, chaque direction s'émancipant des autres, conduisant son propre projet, créant de fait des risques souvent importants (voir ci après). L'externalisation est un processus assez complexe, donc consommateur de temps pour les directions générales. Ce type de projet sera donc réservé aux fonctions pour lesquelles le gain potentiel est important.

Le recours à l'externalisation est fondé sur trois points essentiels : une rentabilité accrue liée principalement à la réduction des coûts (de 20 à 50 %) ; le recentrage sur le cœur de métier de l'entreprise (activités stratégiques, capacité à innover, adaptation au changement et au management interactif) ; une réduction des délais opérationnels, des processus de fabrication, de la chaîne de livraison (sans aucun temps mort).

Il ne faut pas négliger l'importance des risques face à des bénéfices immédiats, des anticipations de gains parfois balayées par des surcoûts dont les conséquences les plus saillantes sont une facturation qui dérape, mettant ainsi en péril le projet dans sa totalité. Ce sont de nombreuses questions qu'il faut à l'évidence se poser pour rendre pérenne un modèle économique qui n'est pas le modèle traditionnel de l'entreprise : Quel est mon besoin ? Qui fait quoi ? Quels sont les différents aspects, social, industriel, économique ? Qui sont et qui seront les acteurs ? Suis-je en phase avec mon prestataire ?

C'est avant de décider d'externaliser qu'il faut se pencher sur la cartographie des risques pour pouvoir les anticiper (voir encadré). ////

La cartographie des risques de l'externalisation

- Manque de préparation dans la construction du projet (alors qu'une équipe projet structurée à cet effet s'impose).
- Manque de coordination des expertises en corrélation avec la refonte du modèle opérationnel.
- Défaut dans la prestation délivrée (implications internes et externes, emploi local, normes).
- Non-respect des engagements.
- Perte de contrôle de l'activité due à la distance géographique et culturelle.
- Défaut dans les choix techniques et humains du prestataire et dans la pérennité du service.
- Risques industriels à moyen ou long terme.
- Risques liés à la mutualisation (un prestataire peut utiliser son personnel et éventuellement ses infrastructures pour plusieurs entreprises).
- Moyens de traçabilité des produits et des données.
- Transfert des données (dépossession, divulgation, sensibilité des données transférées à l'étranger).
- Réglementation renforcée concernant notamment les données clients (obligations légales).
- Risques juridiques liés aux contrats de travail, aux transferts de savoir-faire.
- Risque accru de fraude.
- Risques sociaux liés à la délocalisation d'emplois.
- Risques d'assurances : pertes, contamination des données, piratage.
- Risques liés à la propriété intellectuelle des logiciels et des brevets.
- Risques de gouvernance et déconnexion par rapport aux habitudes de l'entreprise.

1 IDENTIFIER LES RISQUES

Réversibilité d'une externalisation et autres précautions

Dans un projet de *cloud*, d'autres risques apparaissent puisque les données migrent, sont copiées, sont échangées, sont accessibles dans le monde entier. En juin 2012, la Commission nationale de l'informatique et des libertés (Cnil) a publié des recommandations concrètes sur le *cloud* qui consistent à prêter attention aux points suivants :

- Qualifications et agréments du prestataire
- Adaptation des interfaces et évolution des plateformes de *cloud*
- Performance et interopérabilité des systèmes.
- Homogénéité de la sécurité et de la confidentialité des données.
- Adaptabilité des outils du prestataire (ordonnancement, monitoring).

Les derniers risques importants sont, en dehors de la viabilité du projet, les conséquences à terme non seulement sur le plan humain mais aussi sur le plan de l'organisation et des processus de l'entreprise elle-même. Il faut donc aussi intégrer la possibilité de la réversibilité d'une externalisation et anticiper cette éventualité.

Ces risques évoluent en regard des principales tendances du marché définies par les pays donneurs d'ordres ou les pays offreurs de prestations. De multiples environnements législatifs et réglementaires viennent en outre complexifier les montages à réaliser pour bénéficier des effets de levier liés à de telles opérations. Des mesures émergentes, plus protectionnistes, telles que la loi Durbin-Grassley aux États-Unis[2], peuvent avoir un impact dans le futur. En France, une première jurisprudence a mis l'accent sur la récupération des données et les obligations du prestataire qualifiant le contrat de *cloud* de contrat d'intérêt commun[1]. On voit que des évolutions telles que le *cloud computing* affectent les modèles d'externalisation, la gestion des postes de travail, la gestion des centres de données, etc.

intégrer la possibilité de la réversibilité d'une externalisation et anticiper cette éventualité.

1. Affaire Oracle-Union pour un mouvement populaire. Ordonnance de référé TGI de Nanterre, 30 novembre 2012, www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3794

2. Cette loi restreint la délivrance de visas pour les travailleurs indiens qui viennent pour un ou deux ans aux États-Unis, et dont le coût de travail est plus faible que certains homologues américains. La loi imposerait aussi les revenus de ces expatriés temporaires.

Externalisation et sécurité des systèmes d'information : un guide de l'ANSSI pour maîtriser les risques

Parce qu'il est indispensable, dans toute opération d'externalisation, de faire appel à des prestataires qui s'engagent sur la sécurité, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié un guide de l'externalisation qui aide à maîtriser les aspects de sécurité dans les marchés d'infogérance. Elle souligne en particulier les risques spécifiques à l'informatique en nuage (*cloud*).

http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides

L'externalisation au service du développement de l'entreprise

Les cadres dirigeants doivent acquérir l'expérience nécessaire à l'accomplissement de leur métier dans un contexte de plus en plus évolutif, transfrontalier et multiculturel. Prendre des risques, c'est l'apanage de tout dirigeant. Encore faut-il que cela se fasse après une véritable réflexion stratégique, une évaluation correcte de l'ensemble des risques, et la prise en compte de nouveaux risques potentiels. Il faut aussi harmoniser les fonctions transverses (DSI, DRH, Direction juridique) et y intégrer les compétences nécessaires. Le potentiel de création de valeur de l'externalisation ne doit, quant à lui, jamais occulter les véritables capacités de l'entreprise. Les modèles d'externalisation ne sont plus fondés sur un simple transfert de ressources et de responsabilités. L'externalisation signifie désormais moins un arbitrage de coûts de main-d'œuvre que l'accès à un univers de compétences à l'échelle planétaire. L'externalisation est désormais au service de la mondialisation du marché et du développement des entreprises et on assiste à une plus grande spécialisation de marché et des niveaux d'échanges intra-entreprises, de plus en plus sophistiqués, fondés sur l'essor fantastique et le développement des nouvelles technologies d'information et de la communication. ■

Le risk manager, de suiveur à stratège

[métier] Avec les scandales financiers et les lois qui ont suivi, le rôle du *risk manager* a considérablement évolué vers la préservation de la valeur créée et la sécurisation de la prise de décision.

Déléguée générale de l'Association Management des risques et des assurances de l'entreprise (AMRAE), **Bénédicte DE LUZE**, expert-comptable de formation, a commencé sa carrière à la Société générale avant de rejoindre KPMG où elle a créé le département de gestion des risques, de contrôle et audit internes. Titulaire de l'Associate in Risk Management, elle pilote les activités d'AMRAE Formation et du congrès annuel de l'association.

benedicte.deluze@amrae.fr

Le rôle du *risk manager* a bien évolué depuis ces dernières années. Dans les années 1980-90, la gestion des risques était souvent limitée à celle des assurances, en particulier aux risques assurables, et au domaine de la sécurité des infrastructures et de personnels. La vision globale des risques n'avait de sens que pour les mandataires sociaux dont le patrimoine personnel était engagé.

À partir de l'an 2000, les scandales financiers américains et européens ont mis en lumière la défaillance certaine des systèmes de contrôle interne et de gouvernance alors que des enjeux planétaires se profilaient. Le législateur s'est alors emparé de ces questions et a commencé à organiser les systèmes de gestion des risques et de contrôle interne. En 2003, en France, la Loi de sécurité financière traite pour la première fois de gouvernance et de contrôle interne. En 2008 lui est adjointe la gestion des risques.

Deux documents essentiels

Les objectifs de la gestion des risques sont simples et précisés dans le cadre de référence de l'Autorité des marchés financiers (AMF)[1] : créer et préserver la valeur, les actifs et la réputation de l'entreprise ; sécuriser la prise de décision et les processus de la société pour soutenir l'atteinte des objectifs ; favoriser la cohérence des actions avec les valeurs de la société ; et, enfin, mobiliser les collaborateurs de l'entreprise autour d'une vision commune des principaux risques.

Le rôle du *risk manager* est de définir et de déployer un dispositif correspondant à ces objectifs. Il s'appuie sur deux documents essentiels : le référentiel métier du *risk manager*[2] et un référentiel de gestion des risques[3]. Les neuf activités répertoriées dans le référentiel métier (voir encadré) le définissent à la fois comme le coordinateur de la gestion des risques et l'acteur de son financement. Le *risk manager* joue donc un rôle pivot dans le dispositif de gestion des risques. À travers sa mission - arrêtée par la Direction générale et entérinée par le conseil d'administration - le *risk manager* recense, hiérarchise et coordonne la cartographie des risques de l'entreprise. À partir d'entretiens individuels ou d'ateliers collectifs, il parcourt l'entreprise, du *corporate* aux filiales, s'informe sur toutes les activités pour révéler et comprendre les menaces actuelles et futures susceptibles d'empêcher la stratégie de se réaliser. À l'aide d'une échelle qualitative (conséquences, probabilité, maîtrise interne), d'analyses comparatives et de retour d'expériences, il rend fiable les évaluations des risques identifiés et cherche à donner à la Direction générale une hiérarchisation des risques la plus objective possible.

Un précieux stratège

Plans opérationnels, plan de continuité d'activités préparé et testé, programme d'assurances adapté, toutes ces analyses seront construites par le « propriétaire » de risques avec le soutien du *risk manager*. La connaissance transverse de l'entreprise que ce dernier possède, alliée à sa forte technicité des programmes de financement des risques en font le partenaire indispensable à la prévention des risques et des crises.

Demain, le *risk manager* contribuera à l'analyse de certaines décisions stratégiques, dans tous les grands projets d'investissement, dans la stratégie de prise de risques et de leur financement à court, moyen et long terme. ■

1. www.amf-france.org

2. *Référentiel métier du* risk manager, AMRAE

3. Référentiels existants : *Cadre de référence : dispositifs de gestion des risques et de contrôle interne* de l'Autorité des marchés financiers (AMF) ; *Iso 31000-2009 : Management du risque - Principes et lignes directrices* ; COSO 2 (Committee of Sponsoring Organizations), etc.

9

Les 9 activités du référentiel métier

- Définition des missions et de la structure du dispositif
- Appréciation du risque (identification, analyse, évaluation du risque)
- Maîtrise des risques (au niveau acceptable en fonction des critères de risques retenus)
- Diffusion de la culture du risque
- Financement des risques en accord avec la politique de management des risques
- Gestion des événements non assurés/non assurables
- Gestion des sinistres
- Gestion de crise
- Pilotage et reporting