place escange

Le think tank du risque immatériel
en entreprise

activités 2023|2024

www.place-escange.fr

: @place-escange : PlaceEscange

SOMMAIRE

ÉDITORIAL

Le patrimoine immatériel : risque n°1 des entreprises

Il y a un peu plus de 3 ans maintenant, lors de nos discussions avec les entrepreneurs et les pouvoirs publics, pour la création de Place Escange, think tank du risque immatériel en entreprise, nous étions loin d'imaginer que ce sujet deviendrait aujourd'hui la préoccupation numéro 1 des entreprises.

Certes, la succession de crises nous a donné raison de propulser ce think tank en partenariat avec les principaux acteurs du marché de l'immatériel ; et à ce stade, les « Conseil scientifique » et « Comité d'experts », composés d'universitaires, de praticiens, de chefs d'entreprises et de hauts fonctionnaires, anciens ministres… tous spécialistes du patrimoine immatériel sous toutes ses formes et de ses risques associés, ont déjà bien avancés dans leurs travaux.

Plusieurs membres d'honneur, que je salue chaleureusement, soutiennent officiellement nos travaux : Sonia ARROUAS, Marie-Christine OGHLY, Georges FENECH, Alain JUILLET, Thibault LANXADE, Corinne LEPAGE, Jean-Claude MAILLY et Michel SAPIN.

Nous n'en finirons jamais de définir ce risque immatériel tant il est mouvant et protéïforme : du risque sanitaire au risque politique, du cyberisque au risque des délais de paiements, du risque géo-politique au risque de e-réputation… Et il est certain que cette liste est loin d'être exhaustive et continuera à s'allonger, obligeant les chefs d'entreprise à rester en veille permanente.

C'est tout l'objectif de Place Escange.

Alerter, prévenir, informer, conseiller, sécuriser tous les entrepreneurs des risques auxquels ils seront confrontés un jour ou l'autre. A l'évidence, le risque immatériel est aujourd'hui le premier risque de toute entreprise.

Depuis des mois, les meilleurs experts se sont déjà exprimés sur notre plateforme ! Près de 90 tribunes ont été publiées avec le thème de l'immatériel comme fil rouge sur notre site www.place-escange.fr, relayées sur nos réseaux sociaux (LinkedIn et twitter) avec plus d'un million de vues au total : recrutement, deepfakes, droit de l'immatériel, e-réputation, RSE, publication des comptes, valorisation des actifs, information d'entreprise, système d'information, transition écologique, gestion du risque client, gouvernance, médiation financière, éthique et déontologie, données extra-financières…

Pour demain, notre feuille de route ne varie pas. Nous poursuivrons nos travaux en publiant des tribunes sur l'immatériel pour aider et accompagner les entreprises ; nous continuerons à réfléchir sur des notes de prospectives ; nous prendrons des positions pour valoriser ce patrimoine immatériel qui fait la richesse des entreprises et des organisations ; et nous organiserons des évènements, afin de diffuser au plus grand nombre des conseils sur cet enjeu d'aujourd'hui et de demain.

Charles Battista,
Président de Place Escange
Président de la FIGEC

L'ÉQUIPE DIRIGEANTE

Charles BATTISTA
Président

Sébastien BOUCHINDHOMME
Délégué général

Paola FABIANI
Conseillère

MEMBRES D'HONNEUR

Sonia ARROUAS
Présidente du Tribunal de commerce d'Evry

Alain JUILLET
Président d'honneur de l'Académie de l'intelligence économique

Thibault LANXADE
Entrepreneur, Président de Luminess

Corinne LEPAGE
Ancienne ministre de l'Environnement, ancienne eurodéputée et avocate associée fondatrice du cabinet Huglo Lepage Avocats

Jean-Claude MAILLY
Ancien Secrétaire général de Force Ouvrière

Michel SAPIN
Avocat, Ancien Ministre

Marie-Christine OGHLY
Présidente de Femmes Chefs d'Entreprises Mondiales et 1ère Vice-Présidente de ICC-World Chambers Federation

Georges FENECH
Ancien Magistrat. Député Honoraire

LE COMITÉ SCIENTIFIQUE

Jean-Luc BARAS
Président du Conseil National des Achats

Charles BATTISTA
Président de la FIGEC

Philippe BERNA
Médiateur national délégué à la Médiation des entreprises

Catherine CHAMBON
Conseiller stratégie numérique de l'IGPN

Jo-Michel DAHAN
Conseiller – Médiateur des entreprises

Carole CHRETIEN
Directrice relations entreprises CNRS

Frédéric DABI
Directeur Général Opinion IFOP

Michel DIETSCH
Professeur émérite à l'UNISTRA

Paola FABIANI
Présidente de WISECOM et Vice-Présidente du MEDEF

Denis FERRAND
Directeur Général de REXECODE

Jacky ISABELLO
Fondateur « Parlez-moi d'Impact »

Michel PHILIPPART
Expert « immatériel »

Louis-Rémy PINAULT
Expert développement stratégique

Numa RENGOT
Avocat associé Franklin

François PERRET
Directeur général de Pacte PME et professeur affilié à l'ESCP Business School

LE COMITÉ D'EXPERTS

Sofiane ABOUBEKER
Président d'ARECIA

Anthony BENHAMOU
Economiste – Enseignant à Sciences Po Paris

Valentin CLEMENT
Etudiant EDHEC

Marie-Anne DESNOULEZ-DELDIQUE
Co-fondateur WeTalk Group

David GRUSON
Directeur Programme Santé Jouve / Fondateur ETHIK-IA

Olivier LEDUC
Expert-comptable

Frédéric LEFRET
Président de l'Institut du Dialogue Civil

Philippe LOREC
Chargé de mission au Service du Haut Fonctionnaire de Défense et de Sécurité

Virginie MARTIN
Professeure à Kedge, Politiste, sociologue

Olivier REDOULES
Économiste

Stéphanie VERILHAC-MARZIN
SVM Consult

Mélanie PERCHERON
Arbitre international de judo

Myriam TRABELSI
Responsable Promotion économique – Grand Paris Grand Est

ESG et Immatériel, enjeux de la prise en compte des indicateurs de reporting pour les entreprises et les investisseurs

Stéphanie Verilhac Marzin

Directrice SVM Consult
Spécialisée en affaires publiques et réglementaires européennes et françaises dans les secteurs du digital, de la publicité, de l'information d'entreprise et de la gestion du risque

« ESG » : vous avez sûrement croisé ces trois lettres en vogue au sein de nombreux articles, webinaires, sessions ou conférences dernièrement, et ce n'est pas fini. Auparavant destinés et compréhensibles uniquement par un public de professionnels avertis, ces critères ne sont plus seulement l'apanage des grandes entreprises mais avec la mise en œuvre de la nouvelle directive européenne sur la publication d'informations en matière de durabilité par les entreprises (CSRD pour Corporate Sustainability Reporting Directive), le champ d'application va être élargi aux entreprises emplissant deux des trois critères suivants : avoir un bilan de 20 millions d'euros, réaliser 40 millions d'euros de chiffre d'affaires, employer au moins 250 salariés.

Quelle est donc la place de l'ESG dans la prise en compte de l'immatériel, à la fois en ce qui concerne l'évaluation du capital immatériel de l'entreprise mais aussi du risque immatériel lié à de mauvais indicateurs ou à une prise en compte insuffisante de leur impact ? Quelles sont les évolutions à attendre dans un futur proche, et quelles préparations les entreprises doivent-elles mettre en place pour assurer conformité et compliance ?

L'importance accrue accordée aux critères ESG que ce soit dans le débat public ou dans la prise en compte des indicateurs de reporting montre bien l'évolution du champ d'interprétation non seulement du risque mais plus largement du capital immatériel : une entreprise ne se définit plus uniquement par rapport à sa valeur financière, sa capitalisation ou son actionnariat, mais désormais également en fonction de ses actions et de sa redevabilité en matière environnementale, sociale ou sociétale et de gouvernance.

L'évolution règlementaire européenne récente place en effet les critères d'ESG au centre de l'adoption de la directive CSRD, laquelle est rapidement passée d'une directive uniquement normative à une directive plus politique incluant des mesures plus « fortes » que son ancêtre la directive NFRD : élargissement du champ et de l'assiette des assujettis, prise en compte de la chaine de valeur, importance des standards et de la mise en conformité avec de possibles sanctions si non-respect des règles… La CSRD met par ailleurs en place un principe-clé, celui de la double matérialité, conjonction de deux types de matérialité : la matérialité financière qui correspond à la vision « outside-in », et la matérialité d'impact qui, elle, prend en compte la vision « inside-out ». La matérialité financière (ou matérialité simple) ne prend en compte que les impacts positifs (opportunités) et négatifs (risques) générés par l'environnement économique, social et naturel sur le développement, la performance et les résultats de l'entreprise. Pour la matérialité d'impact (ou matérialité socio-environnementale), sont à prendre en compte les impacts négatifs ou positifs de l'entreprise sur son environnement économique, social et naturel. Ainsi au travers de la double matérialité sont évalués et rapportés à la fois les risques internes et externes de l'entreprise mais aussi son impact sur l'environnement extérieur, et il importe donc de bien mesurer les critères à prendre en compte et la façon de les retranscrire dans le rapport de gestion.

L'ESG s'inscrit également de manière plus large dans une nouvelle dimension d'évaluation du capital immatériel des entreprises ou des institutions qui témoigne de fortes attentes de la part des investisseurs. Le reporting extra-financier est ainsi scruté de manière beaucoup plus importante par les investisseurs, à tous les niveaux de développement de l'entreprise et quelle que soit sa taille. Les débats sur le Green Deal ou la Taxonomie Verte Européenne ont bien montré que les investissements dans les entreprises ou énergies vertes ou renouvelables sont préférés et favorisés. La prise en compte vient aussi des entreprises elles-mêmes qui réalisent l'importance réputationnelle d'un capital « ESG » comme en témoigne la mise en œuvre de la plateforme Impact en France avec déclaration volontaire. Les exemples sont multiples de grandes entreprises ou groupes vertueux cherchant à transmettre leurs valeurs mais aussi de l'importance de la redevabilité des allégations et prises de position, pouvant in fine mener à des actions de groupe contraires.

L'ESG passe donc d'une ancienne notion purement normative et règlementaire à la traduction d'un capital politique et réputationnel pour les entreprises et les investisseurs. En effet, le reporting ESG va participer de plus en plus à la définition du capital immatériel de l'entreprise, ne serait-ce que parce que la CSRD met en place non seulement des obligations de communication des critères ESG mais aussi une redevabilité à respecter ce qui est décrit et rapporté. Par ailleurs, le capital ESG s'inscrit également de plus en plus comme un avantage compétitif mais également comme l'empreinte d'une certaine souveraineté. C'est là tout le paradoxe auquel est confronté l'EFRAG (European Financial Reporting Advisory Group), l'instance européenne chargée de proposer les standards européens de la CSRD : il lui faut à la fois des standards universels compatibles avec d'autres métriques mais également respectueux d'une certaine spécificité pionnière européenne, un peu similaire à ce qu'a été la prise en compte du respect de la vie privée avec le RGPD. Les critères ESG jouent également de plus en plus dans le capital réputationnel de l'entreprise avec un système de « name and shame » qui risque de se développer avec les premières actions intentées contre des entreprises pour non-respect de leurs déclarations liées à l'ESG. Mettre en place en amont des indicateurs liés aux critères de reporting ESG avec des possibilités d'alertes sera donc un avantage ou un nouveau service qui sera sans nul doute développé par les sociétés d'information financière et extra-financière actives dans ce secteur. La prise en compte des normes, critères et du reporting ESG est donc à la fois nécessaire pour s'assurer du respect des impératifs légaux et de conformité engrangés par la CSRD mais aussi un atout si elle est vue comme composante d'un avantage compétitif en une sorte d'approche d'« ESG by design » qui intègre ces différents critères tout au long du cycle de l'entreprise. Nul doute que la transposition de la directive CSRD en droit français sera à suivre afin de cerner les attentes et évolutions du reporting en la matière et son impact sur le capital immatériel des entreprises.

Les fonds de Private Equity doivent mieux intégrer les intangibles

Michel Philippart, DBA

Professeur, Département Stratégie,
EDHEC Business School

Récemment, le manager d'une entreprise appartenant à un fonds d'investissement privé me partageait ses inquiétudes. Une troisième vente de l'entreprise, déjà passée d'un fonds américain à un fonds français, venait d'échouer. Pour tenter de réaliser la plus-value promise à ses actionnaires, le fonds propriétaire venait de lancer dans l'urgence un plan de doublement de l'EBITDA. Ce manager, obligé de lancer des initiatives autour de ce nouvel objectif de profitabilité à court terme me disait que c'était un jeu de mistigri dans lequel « la mariée devait être présentée sous ses plus beaux atours », alors que les difficultés intrinsèques restaient cachées au plus profond. Il prédisait avec amertume une issue peu enviable à moyen terme car les fondamentaux de son marché exigeaient des attentes plus réalistes, une vision à long terme, plutôt qu'un doublement de l'EBITDA à 18 mois. Cette remarque suggérait que l'approche du fonds d'investissement créait des risques intangibles ou des intangibles négatifs pour atteindre sa cible de résultat.

La tendance au rachat d'entreprises peu efficientes par des fonds d'investissement agressifs est apparue il y a quelques décennies, menée par des investisseurs comme Carl Icahn ou le fonds KKR entre autres. Les retours sur investissement obtenus par ces précurseurs ont encouragé l'apparition de fonds à l'affût d'opportunités de rendements plus attractifs que ceux offerts par les marchés classiques. Aujourd'hui, plutôt que des raids boursiers, ces fonds visent plus souvent des transactions hors marché. Ces fonds se fixent souvent un horizon court, de 3 à 10 ans, pour augmenter la valeur de leurs acquisitions. Leurs leviers de création de valeur sont, pour faire simple, de deux ordres, axées sur un changement des approches de management :

- Chasse aux coûts agressive en mettant en place une nouvelle culture opérationnelle. Le personnel et les fournisseurs sont les principaux « gisements de productivité » pour employer le langage des consultants. Ces gisements étaient nombreux car la culture précédant l'acquisition n'était pas aussi agressive que la moyenne du marché dans lequel opérait l'entreprise.
- Modification du périmètre de l'entreprise. Cela peut se réaliser en vendant des actifs pour lesquels une logique d'intégration au sein de l'entreprise n'existe plus, ou n'a jamais existé, ou qui ont plus de valeur en étant séparés de leur ancienne maison mère. Alternativement, l'acquisition d'entreprises similaires permet de mutualiser des dépenses communes, comme la R&D ou les frais de structure, tout en réduisant l'intensité concurrentielle en alignant les objectifs d'anciens concurrents pour augmenter les prix de vente.

Le ratio d'entreprises financées par des fonds privés par rapport aux fonds publics est en augmentation [1]. Cependant l'information économique récente regorge d'exemples d'acquisitions qui n'ont pas permis de réaliser les plus-values escomptées, ont abouti à la faillite, voire à la disparition de l'entreprise acquise. Des études récentes [2] montrent d'ailleurs que le rendement des investissements dans des fonds privés est en baisse, alors que de plus en plus d'argent est collecté par ces instruments. Pourquoi ? Les investisseurs n'avaient-ils pas une bonne perception des risques ? Ou avaient-ils une foi trop importante dans la capacité à répéter une approche qui a fonctionné par le passé, sans questionner les fondamentaux de ces gains historiques ?

Alors que les premières opérations de ce genre sur une entreprise permettent en général de générer de vrais gains de productivité, lorsque la cible est revendue à un autre fonds plutôt que remise sur le marché, ce fonds doit trouver de nouveaux leviers. En effet, le fonds vendeur a lancé les opérations d'amélioration de la productivité. Le suivant, en attaquant de plus en plus les coûts visibles, risque d'attaquer les intangibles de l'entreprise, sa relation avec son écosystème, les clients, les fournisseurs, le personnel, et sa réputation. L'EBITDA peut en général augmenter à court terme grâce à un management plus agressif encore des coûts, et par des investissements en marketing renforcés. Mais le gain marginal de ces leviers se dégrade de plus en plus. Les bénéfices que ces tactiques ont pu délivrer par le passé ne se réalisent pas. La quête de l'EBITDA à court terme se fait au dépend de la destruction du capital immatériel et crée des risques intangibles qui vont oblitérer le futur de l'entreprise. C'est le cœur du métier qui sera impacté à long terme.

Les fonds d'investissement sont essentiels à la croissance de l'économie en amenant du capital aux entreprises en croissance, à fort potentiel mais trop petites ou trop risquées pour les marchés publics. Lorsqu'ils deviennent des instruments de financement d'entreprises matures, ils doivent changer leurs méthodes de pilotage de leurs investissements, pour prendre en compte de manière plus structurée la gestion des intangibles, et des risques associés à cette gestion. En effet, une des caractéristiques de la valeur intangible est le risque de sa destruction rapide, alors que sa construction est un jeu de patience.

Pour continuer à jouer un rôle prépondérant, les fonds de « private equity » doivent capitaliser sur leurs avantages intrinsèques, c'est à dire la capacité à investir avec un horizon de temps flexible, à moyen et long terme. Les apporteurs de fonds sont de plus en plus discriminants, en plus d'être exigeants. Espérer faire des « coups » est devenu aléatoire et gaspille un des avantages intrinsèques du « private equity » : sa capacité à valoriser la valeur intangible à long terme sans tenir compte de l'effet de la publication des résultats trimestriels face aux analystes sur les marchés publics. Pour paraphraser Anthony Baldwin, CEO AIG UK [3], il faut changer la culture de l'investissement privé pour mieux prendre en compte les avoirs et les risques intangibles. Les fonds les plus performants ont déjà lancé cette mutation mais la culture du gain à court terme reste encore trop présente, alors que les prochaines opportunités seront dans la meilleure prise en compte des ressources immatérielles et la meilleure gestion des risques immatériels. Les leviers de création de valeur mentionnés ci-dessus doivent donc inclure de manière beaucoup plus structurée l'identification des gisements de valeur liée à l'exploitation du capital intangible et le renforcement de la protection contre les risques intangibles.

[1] Stulz, « Public versus Private Equity »; McKinsey, « McKinsey's Private Markets Annual Review | McKinsey ».
[2] Bain & Company, « Global Private Equity Report 2020 »
[3] « Tangible Solutions for Intangible Risks | AIG UK ».

Valentin CLEMENT
Membre du Comité d'Experts

Le risque humain en Cybersécurité

Transformer l'humain en maillon fort pour renforcer sa cybersécurité à moindre coût

La récente crise sanitaire et la démocratisation du télétravail ont posé de nouveaux challenges aux entreprises françaises. Si celles-ci ont rapidement su s'adapter du point de vue des infrastructures, les risques immatériels liés à de telles pratiques n'ont pas tous été pris en compte. La priorité a été essentiellement mise sur les aspects logiciels et matériels : renforcement des postes de télétravail, mise en place d'un VPN pour les connexions distantes au serveur de l'entreprise, chiffrement des emails… en oubliant souvent un élément essentiel au cœur de l'écosystème cyber : l'humain.

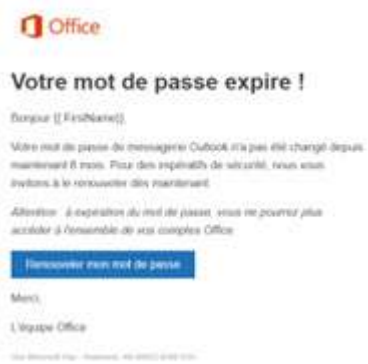
En effet, 63% des incidents de sécurité dont sont victimes les organisations proviennent d'un employé. L'humain reste donc aujourd'hui le maillon faible de la chaîne de la cybersécurité.

Ces incidents ont diverses origines et peuvent avoir des conséquences allant de la fuite de données confidentielles à la paralysie totale de l'entreprise, en voici quelques exemples en guise de rappel :

Le shoulder surfing : littéralement le fait de regarder par-dessus l'épaule d'une personne pour récupérer ses informations personnelles à son insu. Par exemple, lors d'un déplacement en train, un employé se connecte à ses mails sans se préoccuper d'éventuels regards indiscrets. Un opportuniste malveillant en profite alors pour mémoriser ses accès messagerie et récupérer de précieuses informations confidentielles sur les clients de l'entreprise qu'il pourra revendre à des concurrents.

Le phishing (ou hameçonnage) : il consiste à contacter la ou les victimes par courrier électronique en se faisant passer pour un tiers de confiance (banque, prestataire, client, etc…). L'objectif est de récupérer des données confidentielles (mots de passe, données bancaires, secret industriel) afin de les revendre ou de les utiliser à des fins malveillantes (dans le cadre d'une fraude au président par exemple). Une authentification à 2 facteurs (ex : mot de passe et authentification biométrique) permet de réduire les chances de succès d'une telle attaque.

Exemple de phishing au renouvellement de mot de passe Office :



La fraude au président : elle consiste à contacter un employé en se faisant passer pour le directeur de l'entreprise (parfois avec son adresse réelle récupérée via phishing) en demandant, par exemple, un virement bancaire urgent. Flattant d'abord son interlocuteur pour gagner sa confiance, le « président » va justifier un envoi de fonds vers l'étranger, évoquant alors une opération financière, une acquisition de société ou un redressement fiscal à régulariser. Les possibilités offertes par l'intelligence artificielle, et notamment la multiplication des deepfakes (vocaux ou vidéo), rendent ce genre d'attaque de plus en plus difficile à déceler.

Ci-dessous, capture d'écran d'un deepfake vidéo réalisé sur le président Emmanuel Macron :

Le ransomware : Probablement le plus gros risque pour une entreprise, un employé téléchargeant et/ou ouvrant une pièce jointe de provenance inconnue permet à un ransomware de chiffrer les données de son ordinateur et de les rendre inaccessible à quiconque n'en possède pas la clé. Le virus se propage ensuite au reste du réseau. Dans la plupart des cas, le créateur du ransomware exigera une rançon en cryptomonnaie pour déchiffrer les données (qu'il ne faut surtout pas payer car aucune garantie n'est apportée sur la récupération des données). Si rien n'est fait pour contenir l'attaque, la totalité des serveurs de l'entreprise peut être infecté et les données seront irrécupérables. Il faudra des semaines à votre entreprise pour se rétablir et votre business peut être directement et durablement impacté.

Actuellement, l'humain en cybersécurité est considéré comme un problème qu'il faut contrôler, et soumettre à des règles strictes de sécurité. **C'est oublier que l'écosystème cyber est en constant changement et que les attaquants disposent souvent d'un coup d'avance au regard des techniques d'attaque à leur disposition**. Se baser sur des politiques de sécurité pour contrôler les comportements humains n'est donc pas une méthode suffisamment flexible pour faire face à la complexité des attaques futures et il est temps de changer de paradigme en ne considérant plus l'humain comme un problème mais comme une solution.

Comment faire du « problème humain » une « solution humaine » ? **La sensibilisation !**

En formant vos collaborateurs aux bonnes pratiques et aux différents risques, vous transformez ceux-ci en de véritables acteurs de la cyberdéfense de votre entreprise.

Il est possible pour un directeur des systèmes d'information de sensibiliser sois même ses collaborateurs, la tâche est cependant chronophage ! De nombreux organismes proposent de prendre en charge la formation de vos employés et les contenus sont divers : e-learning, mise en situation avec intervenants qualifiés, simulations de phishing. Ces dernières sont de bons indicateurs du niveau de sensibilisation et permettent de mesurer les progrès de vos équipes de façon régulière.

En effet, pour que la sensibilisation soit efficace, elle se doit d'être continue, ludique et prévue sur le long terme. Plutôt que de sanctionner les erreurs, il ne faut pas hésiter à mettre en valeur les bons comportements et à les récompenser. Cela participera à créer une relation de confiance entre les responsables du système d'information et les collaborateurs et augmentera le taux de signalement en cas d'attaque réelle.

Pour reprendre l'exemple de la simulation de phishing, un employé sensibilisé chaque mois finira par analyser instinctivement chaque mail reçu et signalera ceux qui lui semblent suspects. Ce réflexe pourra s'avérer salvateur le jour où un mail de phishing réel atterrira dans sa boite mail. De plus, vos collaborateurs sensibilisés participeront eux aussi à sensibiliser leurs proches par rebond et ainsi, à diminuer l'impact des attaques cyber et ce, même en dehors de la sphère professionnelle.

De plus, le coût de cette sensibilisation sera souvent inférieur au coût de mesures logicielles et matérielles et il sera dans tous les cas inférieur au coût réel d'une attaque qui paralyserait votre chaine de production. L'État met en place des aides via les Opérateurs de compétence (OPCO) pour financer ces formations. L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) propose même une formation gratuite (disponible ici) et des kits de sensibilisation à imprimer pour commencer à entrainer vos collaborateurs.

Enfin, la sensibilisation deviendra une bonne pratique obligatoire pour travailler avec des partenaires désignés opérateurs de services essentiels, notamment avec l'arrivée de la directive NIS 2 (qui touchera 150 000 entreprises en France) et le renforcement des exigences des entreprises vis-à-vis de leurs sous-traitants pour se prémunir des attaques par supply chain (où un attaquant accède au système d'information d'une entreprise via son fournisseur).

Pour conclure, interrogez-vous sur vos pratiques personnelles, quel que soit votre rôle dans l'entreprise :

- Avez-vous déjà transmis un message suspect à votre support informatique ? Etes-vous capable de passer de la vigilance au rôle de sentinelle ?
- Avez-vous utilisé le mot de passe de votre système d'entreprise ailleurs que sur ce système ? Par exemple sur une base de données professionnelle externe ?
- Avez-vous activé une authentification plus forte qu'un simple mot de passe ?

Si vous êtes responsable de la sécurité, ou responsable financier :

- Comment avez-vous sensibilisé vos collaborateurs ? Un email ? Un support de communication ? Ou une session de formation active obligatoire ?
- Faites-vous des audits réguliers ? Avec des experts internes/externes ?

Pour pallier ce risque immatériel, il ne vous reste plus qu'à devenir un maillon fort de la cybersécurité de votre entreprise ou à transformer vos collaborateurs en solution à vos problèmes cyber !

Sébastien Bouchindhomme
Délégué Général de la FIGEC & de Place Escange

Le portefeuille clients, un risque immatériel à canaliser

La gestion du risque client dans l'entreprise est du ressort du crédit manager, une fonction présente dans la plupart des ETI et des grands comptes. Dans les PME et les structures plus réduites, la direction financière, l'éventuel trésorier, voire le directeur commercial ou le responsable de la comptabilité. Et bien sûr, le chef d'entreprise se doit de structurer la démarche.

Le danger encouru à cause d'un retard ou d'un défaut de paiement n'est pas, loin s'en faut, la priorité de l'entrepreneur au lancement de son activité. Il pense naturellement à se structurer rapidement avec une direction commerciale pour organiser le développement du business et la conquête, et avec une comptabilité – éventuellement externalisée – pour éditer les factures et effectuer les relances. Mais ces trois entités ont de telles autres urgences opérationnelles qu'elles abordent rarement, et encore moins en les partageant, les problématiques de risque client. Et pourtant…

Les besoins apparaissent donc lors d'un premier incident. La découverte des conséquences éventuelles d'un retard, voire d'un défaut de paiement se vit généralement dans la douleur. Force est aussi de constater que la surprise est d'autant plus grande que les habituels conseillers des créateurs d'entreprise (banquiers, chambres consulaires, cabinets d'expertise-comptable) ont d'autres priorités.

Et pourtant, ce sujet est important. Surtout quand on sait que 25 % des quelques 50 000 défaillances d'entreprises annuelles en France (en moyenne) ont pour origine, chaque année, des factures impayées. Mais parfois, les retards de paiement qui s'accumulent ont aussi un effet désastreux sur la trésorerie de l'entreprise, même en croissance, ce qui peut l'amener à demander des facilités de trésorerie à son banquier et à devoir en payer les frais afférents.

Créateur d'entreprise, le premier de cordée

Sur le chemin de la structuration d'une véritable stratégie de gestion du risque client, c'est bien sûr le chef d'entreprise qui agira le premier, chronologiquement. Parce qu'il est sur tous les fronts, souvent seul au début. Concentré sur le développement de son chiffre d'affaires, il ne met en place que progressivement son service comptable, préférant même l'externaliser au départ ou utiliser des logiciels de gestion en mode SAAS. C'est lui qui gère les retards de paiement de ses clients, parfois en se rapprochant de son expert-comptable, qui peut lui conseiller d'utiliser les services de sociétés spécialisées en recouvrement de créances. Son banquier lui proposera des solutions de type « Factor », qui permettent le rachat de créances mais avec un impact finalement assez limité : ces rachats ne concernent que les clients déjà connus, acceptés par la banque qui de toute façon se retourne vers le créancier si elle ne parvient pas à recouvrer la créance.

La comptabilité, le début de la structuration

C'est avec la création d'un service comptable interne qu'apparaissent les premières briques d'une gestion structurée du risque client. Le professionnel va vouloir mettre en place des outils de suivi des factures en cours, puis de relance automatique. Il peut également établir des indicateurs et des statistiques qui lui permettront d'anticiper sur les dérives. Avec l'aide de l'expert-comptable qui travaille pour la société, il commence également à organiser une veille – légère – sur les événements affectant la vie des sociétés clientes – suivi des procédures de dépôt de bilan par exemple.

Une responsabilité qui se partage

En grandissant, l'entreprise structure ses forces commerciales et nomme à leur tête une direction. Il en va de même pour la direction financière qui va, peut-être, se doter aussi d'une fonction trésorerie, au fur et à mesure que s'éclaire le BFR, ainsi que les besoins en cash management entre entités du groupe.

Dans cette étape de la vie de l'entreprise, la gestion du risque client devient une préoccupation partagée, à la fois par les équipes de ventes qui peuvent dans certains cas être intéressées sur le paiement final de leurs clients, la direction financière qui souhaite limiter les recours aux prêts bancaires, et le trésorier qui apprécie de disposer de fonds à faire travailler.

En même temps, cette responsabilité reste diluée tant qu'un credit manager n'est pas nommé. Son rattachement hiérarchique se fait généralement à la direction financière, mais le parcours du candidat, ou l'histoire de l'entreprise peuvent aussi amener à un positionnement plus intermédiaire, entre la DAF et la direction commerciale.

Le credit manager, une femme ou un homme de projet à plus d'un titre

Dans tous les cas, le credit manager est une femme ou un homme de projet. D'abord parce qu'il lui revient la responsabilité de structurer, avec les différents métiers concernés, la chaîne complète qui va de la recherche du client jusqu'à l'encaissement d'une facture, en passant par les étapes d'analyse du risque, de dématérialisation des chaînes de facturation, de relances automatiques ou encore de recouvrement. Aujourd'hui largement dématérialisés, ces processus s'appuient par exemple sur des partenariats avec les sociétés membres de la FIGEC, (Fédération Nationale de l'Information d'Entreprise, de la Gestion de Créances et de l'Enquête Civile – https://www.figec.com/) qui fournissent des scorings élaborés sur les clients potentiels, remontent des alertes sur les incidents les affectant, organise la médiation financière et peuvent aller jusqu'à gérer les contentieux.

Le credit manager suit également l'actualité réglementaire, qui a été riche ces dernières années sur le front des conditions de règlement des factures.

Mais surtout il est, au quotidien, amené à prendre des décisions, une fois le risque connu, sur des affaires qui engagent l'entreprise auprès de ses clients. Ce faisant il est directement contributeur au développement de l'activité, y compris à l'international avec l'aide là-aussi des entreprises de la FIGEC qui disposent des bases de données adéquates.

Un sujet éminemment transversal

La constitution et l'animation d'un comité de crédit concrétise la transversalité du sujet – en même temps que la maturité de l'entreprise -, qui continue d'impliquer aussi bien la direction commerciale que la direction financière et la direction générale. Le crédit manager en est le pivot : il est alors amené à éclairer les décisions de l'ensemble de ces acteurs de la réussite de l'entreprise, en exposant les risques, mais en sachant également en prendre.

La crise révélatrice de la nécessité d'une approche intégrée des immatériels

Stéphane TREBUCQ

Professeur des Universités en Sciences de Gestion

Louis-Remy PINAULT

Expert développement stratégique chez GENERALI

Alors que l'Europe a commencé à réglementer d'une manière croissante l'industrie de la banque assurance, avec sa taxonomie verte, les récents projets du gouvernement français via la plateforme Impact illustrent l'importance d'une donnée publique sur les performances sociale, environnementale et économique des entreprises. Toutefois, aucune de ces initiatives n'arrive encore à traiter d'une manière satisfaisante la question d'une mesure des immatériels, et plus particulièrement le capital organisationnel, le capital humain, le capital relationnel et social, ou encore le capital intellectuel. Peut-on toutefois s'en tenir seulement aux seuls immatériels comme clé de lecture prédictive de la performance de l'entreprise ? C'est à ce niveau que la crise sanitaire mondiale de la Covid a permis de révéler les défaillances béantes des outils de gestion précédemment mis en place. En effet, dans quelles cartographies des risques figuraient ce risque de pandémie ? Dans quelles cartographies des risques figuraient les risques de rupture d'approvisionnement de certains composants électroniques ? Cette crise nous aura au moins appris à prendre conscience de l'obsolescence de nos technologies de gestion. Dès lors, à la question d'une meilleure compréhension des immatériels, s'ajoute l'enjeu d'une sophistication du management des risques. Un nouveau terme a d'ailleurs vu le jour, avec le concept de résilience. L'idée sous-jacente est alors de renforcer la capacité de performer dans un état de la nature, par une capacité de résister dans toute une série d'autres états de la nature. Comment alors relier la notion d'immatériel avec la notion de résilience ?

De nombreux travaux académiques montrent justement que le capital humain est un facteur majeur de résilience. Pourquoi ? Tout simplement parce le capital humain renvoie au fonctionnement des individus, mais aussi des équipes, qui peuvent alors savoir faire preuve d'adaptation et d'agilité, et ce d'autant qu'ils adhèrent au projet de l'entreprise. Citons aussi l'importance d'un système d'information, autrement dit un capital informationnel, permettant d'organiser cette résilience. Les cartographies des risques, pour défaillantes qu'elles aient été, sont effectivement à compléter par des cartographies de processus, des cartographies stratégiques, des cartographies d'enjeux de matérialité, ou encore des cartographies de parties prenantes. Si ces cartographies sont mises en place, le système d'information permet-il pour autant d'en comprendre les liaisons ? Est-il possible de comprendre et d'anticiper via les systèmes en place les conséquences d'un scénario-type choisi par l'équipe dirigeante pour se préparer à une future situation de crise ? Sur ce plan, on ne pourra que constater la faiblesse des bases de données disponibles, le manque de structuration de l'information par l'éco-système des structures accompagnant les entreprises. Si la robustesse des capitaux immatériels est un facteur de résilience, et que l'on souhaite dépasser le stade du discours, il serait alors temps de structurer les observations d'une manière plus scientifique, rigoureuse, systématique.

A l'opposé de la robustesse, nous trouvons la situation des immatériels en position de fragilité. D'où cette dernière peut-elle provenir ? L'hypothèse que nous avançons repose sur la théorie des systèmes. De cette approche, nous retenons l'idée que la mauvaise compréhension des interactions entre risques, processus, objectifs stratégiques, immatériels finit par empêcher une prise de décision pertinente dans l'entreprise. Le recours à la théorie socio-économique des organisations, développée à Lyon par les professeurs Savall, Zardet et Bonnet, permet d'ajouter une brique complémentaire à ces interactions incomprises, en avançant la notion de dysfonctionnements. Or ces derniers ont été listés et référencés par leur institut de recherche. Il ne tient alors aux entreprises et à leurs dirigeants qu'à développer une mise en relation de leurs outils de gestion, afin de mieux appréhender l'ensemble des chaînages de causalité. Cette propriété est qualifiée de « connectivité », et représente au-delà un enjeu organisationnel plus large, puisqu'il s'agit de mettre en connexion les instances de gouvernance, le traitement des risques et des opportunités, les composantes du modèle d'affaires, ainsi que l'ensemble des analyses prospectives.

Face à une telle complexité, l'évaluation externe des risques de l'entreprise semble bien démunie, et de moins en moins pertinente. L'assureur est donc appelé à évoluer du statut d'expert des risques à celui d'accompagnateur des dispositifs permettant de sécuriser et développer l'entreprise. Ce nouveau positionnement nécessite d'être en capacité d'identifier les faiblesses de l'entreprise, souvent situées dans la difficulté à se remettre en question, à formuler un projet stratégique clair, à développer des actions cohérentes et coordonnées. La création de valeur produite par l'assureur consiste alors à permettre aux dirigeants d'opérer une transformation de l'entreprise, en facilitant les contacts avec des experts dans les domaines stratégiques, informationnels, communicationnels, opérationnels.

Si la formulation claire de la stratégie est un préalable, et un élément fondamental, pour espérer entraîner et engager l'ensemble des salariés, le recours à la RSE (responsabilité sociétale des entreprises) peut constituer un apport non négligeable. Cette dernière repose principalement sur les préconisations d'écoute et de satisfaction des parties prenantes. Reste à savoir si les parties prenantes ont été bien choisies, et si ces dernières, satisfaites, s'avèreront loyales et fiables en temps de crise. Il est donc important que compléter l'approche classique de la RSE, par une approche des risques et des scénarios, où les immatériels peuvent eux-mêmes devenir des facteurs d'empêchement de la réalisation des objectifs stratégiques de l'entreprise.

De ces différentes réflexions, nous tirons plusieurs enseignements. En premier lieu, l'environnement cognitif du management nous apparaît mouvant. Il importe par conséquent d'en intégrer les nouvelles notions, telles que la résilience. En second lieu, l'espoir d'une compréhension du système de l'entreprise passe par une connaissance et un suivi des interactions entre un ensemble d'objets clés : dysfonctionnements, processus, objectifs, capitaux. En troisième lieu, les partenaires de l'entreprise, comme les assureurs, sont appelés à raisonner en termes de co-construction, d'éco-système et d'expertises complémentaires, afin de sécuriser la trajectoire de performance globale de leurs clients. En quatrième lieu, la RSE est un levier incontournable pour opérer une formulation stratégique pertinente. On doit toutefois en percevoir les limites. Plus que jamais, il nous semble dès lors essentiel de développer une compréhension systémique de l'entreprise. Les progrès en la matière ne pourront être cependant constatés sans un grand plan national de collecte de données pertinentes, ne relevant pas seulement d'une logique de résultats, mais d'une analyse des déterminants fondamentaux de création de valeurs.

Risque immatériel, capital humain et opérations de haut de bilan

Carole GIORGI

Associée de Gouvernance et Valeurs

Il peut paraitre surprenant de lier ces trois termes mais l'historique associé à plusieurs opérations de haut de bilan met en évidence que le risque immatériel lié au capital humain est un élément déterminant dans le succès ou l'échec de ces opérations.

Il s'agit du capital immatériel le plus significatif et mesurable grâce à plusieurs critères :

- le coût de recrutement pour constituer l'équipe de travail,
- le temps de travail investi pour l'intégration et la transmission de la culture de l'entreprise
- les dépenses liées aux formations pour former l'équipe,
- La dextérité, la productivité et l'efficacité de l'équipe,
- La motivation, les compétences, le climat au sein de l'entreprise,

Ce capital reflète l'intelligence collective endogène et exogène de l'entreprise. Il tient donc compte du coût du travail, de l'efficience des équipes avec la taille et les compétences des équipes « support », de l'encadrement, de l'équipe commerciale. Il prend aussi en considération les dirigeants avec la stratégie de l'entreprise, les commerciaux, les gestionnaires et les meneurs d'équipes, la maîtrise du métier mais aussi l'efficacité avec les compétences des équipes, le climat et la motivation des équipes.

Aussi surprenant que cela puisse paraitre : le capital humain est un actif immatériel prégnant dans les opérations de haut de bilan.

En effet dans les opérations de fusion acquisition, ainsi que dans toutes opérations capitalistiques : il apparaît primordial qu'il n'y ait ni vainqueur ni vaincu, en l'occurrence le vainqueur étant la société absorbante et la vaincu la société absorbée.

Lorsque deux entreprises antérieurement concurrentes fusionnent : il est stratégique que les équipes commerciales autrefois rivales soient fédérées dans un même projet d'entreprise.

D'autres échecs d'opérations de fusions acquisitions peuvent être liées à des problèmes d'égo et de neutralisation réciproque des équipes concernées. Un cas d'école est la funeste fusion Alcatel-Lucent qui a été destructrice de valeur pour ces deux sociétés. Les deux dirigeants Pat Russo et Serge Tchuruk s'estimaient peu et n'ont jamais pu coopérer pour mener à bien un projet commun et fédérateur pour les équipes.

Dans le cadre des PME, qui sont rachetées suite à une cession, le facteur humain est un élément déterminant dans la continuité de la trajectoire de l'entreprise achetée et la valorisation des compétences et des savoirs-faire doivent faire l'objet d'une expertise indépendante dédiée.

Le capital humain représenté par le management et les équipes est donc un facteur clé sur lesquels les investisseurs vont prendre le risque de s'engager.

Ainsi il est d'usage que lors des opérations de transmission, de levées de fonds, soit annexé au projet, le CV de l'équipe dirigeante.

Aujourd'hui, une grande partie de projets de post-mergers intégration des PME échoue en raison notamment du facteur humain et de la mauvaise complémentarité entre les membres de l'équipe.

Cela implique qu'une entreprise qu'il s'agisse d'une PME ou d'une start up a besoin d'une belle collection de ressources: connaissances, talents, compétences, expérience, intelligence… pour y parvenir.

Concernant le capital humain, nous pouvons affirmer que la connaissance est un principe de base qui augmente considérablement les chances de réussite. Dans les nouvelles entreprises, le capital humain de l'entrepreneur peut être considéré comme une ressource clé.

Dans ce cas, il s'agit de savoirs difficilement appropriables et porteurs d'avantages compétitifs : valoriser devient fondamental afin de pérenniser ce dernier.

Lorsque des personnes souhaitent rejoindre une équipe en co-création, il existe un certain risque qu'elles puissent partir. Il n'y a aucune obligation formelle de les faire rester. Mais un environnement et une culture fédératrice diminuent ce risque.

Les employés des startups et de taille moyenne doivent souvent remplir plusieurs rôles avec compétence, ce qui nécessite une excellente gestion du temps, un dévouement et un niveau de compétence plus élevé que la plupart des emplois dans des entreprises plus grandes et mieux établies.

Les entreprises qui remplissent ces rôles divers et stimulant avec des employés expérimentés éviteront bon nombre des problèmes internes qui affligent traditionnellement ces typologies d'entreprises et libéreront plus de temps à l'entrepreneur pour se concentrer sur la croissance et d'autres facteurs. De plus, ces employés qualifiés seront mieux en mesure de former de nouveaux talents lorsque l'entreprise commencera à se développer, ce qui rendra les employés à moindre coût plus efficaces au fil du temps.

Qu'ils s'agissent de startup ou de PME : il est essentiel de fédérer et motiver les équipes pendant toute la durée de vie du projet en l'occurrence le succès de la levée de fond ou la période de post acquisition ou post merger…

Les désunions et mésententes entre associés, un turnover important des équipes ou une ruinerait la confiance des investisseurs et de l'ensemble des parties prenantes.

Capital immatériel, le risque de l'exposition sociétale

Frédéric Lefret

Président de l'Institut du Dialogue Civil

Depuis de nombreuses années, la Responsabilité Sociale d'Entreprise (RSE) est une des composantes majeures de la stratégie d'entreprise.

Nulle entreprise ne peut agir aujourd'hui sans prendre en compte les parties prenantes et les territoires où elle intervient.

Cette RSE qui se décline à travers des engagements et des réalisations contribue fortement au capital immatériel de l'entreprise.

Pour autant, ce qui devrait renforcer ce capital se traduit souvent par une extension du risque sociétal de l'entreprise.

Les engagements RSE passés au crible

En effet, le green trolling ou le rse trolling, est aujourd'hui devenu l'une des actions phares des mouvements contestataires et des ONG vis-à-vis de la crédibilité des stratégies RSE.

Scrutés, analysés, décortiqués… les engagements RSE sont passés sous les fourches caudines.

Le moindre écart entre engagements et réalisations est révélé, dénoncé et partagé au plus grand nombre pour tenter de lier le capital immatériel de l'entreprise au greenwhashing.

La promesse ne suffit plus, seule la preuve peut-être crédite autant faut-il qu'elle soit démontrable…

Soupçonné de démarches insincère, l'entreprise se trouve davantage exposée en raison de l'apparition d'un concept mouvant et protéiforme : le wokisme.

Cette nouvelle radicalité qui prend souvent pour cible l'entreprise comme fait générateur, a conquis une partie importante de la jeunesse et notamment la génération Z.

Plus de la moitié des 18-35 ans souhaitent désormais que les entreprises s'engagent dans leur communication marketing comme dans leur politique de ressources humaines à une meilleure prise en compte des revendications et des critères identitaires comme l'appartenance ethnique, l'identité de genre, ou la religion.

La marque devient politique

Aux yeux des Français, les institutions politiques traditionnelles (élus, mais aussi ONG) apparaissent de moins en moins comme des acteurs capables de changer la société et de répondre aux défis de notre époque. À la différence des entreprises qui, avec la montée en puissance de la RSE et du statut d'entreprise à mission, voient leurs rôles sociétales et politiques s'accroître.

Certaines thématiques rassemblent toutes les générations. La défense de l'environnement est un enjeu majeur pour 89 % des Français, 84% placent également le bien-être animal et la place des femmes parmi leurs priorités. Mais les 18-35 ans portent également des combats plus identitaires directement issus du mouvement Woke, comme la prise en compte par les entreprises des revendications liées à l'appartenance religieuse, ethnique ou de genre.

Sur ces nouvelles thématiques, une profonde fracture générationnelle s'est ouverte. Ainsi, le sondage Harris Interactive pour l'Institut du Dialogue civil révèle, par exemple, que si 78 % des moins de 35 ans souhaitent que la société réponde mieux « aux attentes des personnes en fonction de leur religion », ils ne sont que 29 % parmi les plus de 50 ans à soutenir cette proposition. Un écart de 49 points qui sera la source de difficultés pour trouver la bonne façon de parler de ces sujets à l'ensemble de la population.

Pour les générations Z et Y, l'entreprise est devenue le lieu naturel où doit s'exercer la nouvelle « justice sociale ». C'est en contraignant les entreprises à intervenir sur ces fournisseurs, ses clients, ses produits, ses actionnaires, ses collaborateurs… que cette génération souhaite changer les habitudes et transformer la société. Si, en tant que consommateurs, les plus de 50 ans continuent de placer en tête des critères qui les incitent à choisir une marque des aspects comme la qualité du produit, ou son prix et finalement s'intéressent assez peu aux aspects liés à la religion, le genre ou l'appartenance ethnique, ce n'est pas le cas des moins de 35 ans.

55 % des 18-35 ans considèrent, par exemple, que lorsqu'ils achètent un produit les critères liés à la « place accordée par l'entreprise qui commercialise ce produit aux attentes des personnes selon leur identité sexuelle » sont prioritaires, de même pour la religion ou l'appartenance ethnique.

Le marketing de l'entreprise est alors scruté à la loupe pour y détecter tous positionnements qui pourraient renforcer selon eux cette justice sociale.

Une e-génération prête aux actions radicales auprès des entreprises

Bien se préparer à ce défi est un enjeu vital pour les entreprises, car le risque de subir des attaques violentes se développe. En effet, pour défendre leurs idées, les moins de 35 ans sont bien plus nombreux que leurs aînés à envisager le recours à des méthodes radicales, comme d'occuper de force un site (32%), de dégrader des panneaux publicitaires, ou même de pratiquer des micro-sabotages auprès de l'entreprise.

C'est la conséquence de leur impatience face aux dangers qu'ils considèrent comme imminents et qui légitiment, selon eux, des actions radicales.

Ces aspirations à la radicalité sont soutenues et entretenues par de nombreuses publications militantes et universitaires et par des organisations d'activistes qui ces dernières années ont considérablement professionnalisé leurs méthodes (infiltration, retournement de salariés, maîtrise de la communication digitale…).

Désormais les attaques peuvent être globales, être menées par des activistes stratèges qui n'hésitent pas, par exemple, à utiliser le trouble suscité chez les salariés d'une entreprise par une polémique pour tenter de les recruter et d'infiltrer la société.

Face à ces potentielles attaques, les entreprises ne doivent ni sous-estimer la menace ni sur-réagir. Encore une question d'équilibre pour préserver l'atout du capital immatériel.

Comment mesurer l'immatériel ?

Abdoullah Lala

Expert-Comptable & Commissaire aux Comptes

Cette question métaphysique ou existentielle nous préoccupe parfois : comment donner de la valeur à ce qui n'a pas de substance physique, ni d'existence concrète, bref ce qui est invisible en somme ?

La réponse se traduit par l'espérance qui peut nous transcender, et nous faire croire en un lendemain meilleur, et sur le plan « matériel », par l'espoir que l'immatériel (ou plutôt l'exploitation économique de ces biens immatériels) nous réserve un avenir heureux et fructueux en raison du succès qui -nous l'espérons- nous permettra finalement de récolter les dividendes de nos efforts et/ou de notre talent.

Combien de jeunes entrepreneurs ou futurs entrepreneurs caressent l'espoir que leur start up -qui porte les fruits de leurs talents et de leurs efforts- soit demain à l'origine d'un succès économique et financier leur permettant de rejoindre au panthéon des grands entrepreneurs Larry Page (Google) ou Mark Zuckenberg (Facebook) dont les fortunes sont estimés à plusieurs milliards de Dollars.

Posée en ces termes, la question de la valeur de l'économie immatérielle peut se révéler iconoclaste mais elle rejoint les interrogations de certains analystes financiers dès lors qu'ils sont amenés à examiner la valeur des entreprises -qui font appel public à l'épargne ou non- dont l'actif du bilan laisse apparaitre ou non la valeur de leur patrimoine immatériel.

Comment définir la notion de biens immatériels ?

Les normes applicables en matière d'information financière (nous parlerons essentiellement de normalisation internationale plus communément connue sous le vocable d'IFRS et de ses avatars les IAS/IFRS) définissent dans certaines situations (pas toutes hélas) la notion d'actif immatériel ou plutôt d'immobilisation incorporelle, en donnant une acceptation plus restrictive à ce dernier concept, comme un actif non monétaire identifiable sans substance physique (Cf. IAS 38).

La définition d'une immobilisation incorporelle (terme que nous allons utiliser par la suite pour désigner un actif immatériel par simplicité) dans le référentiel IFRS impose que cette immobilisation soit identifiable, afin de la reconnaitre (la comptabiliser) comme un actif au bilan de l'entreprise.

Un actif satisfait au critère « d'identifiabilité » dans la définition d'une immobilisation incorporelle lorsqu'il est séparable, c'est-à-dire qu'il peut être séparé de l'entité et être vendu soit de façon individuelle, soit dans le cadre d'un contrat, avec un actif ou un passif lié.

Cette norme définit également la notion d'actif comme une ressource contrôlée par une entité du fait d'événements passés et à partir de laquelle on s'attend à ce que des avantages économiques futurs bénéficient à l'entreprise.

La notion de contrôle d'un actif suppose le pouvoir d'obtenir les avantages économiques futurs découlant de la ressource sous-jacente. Dans ces conditions, une immobilisation incorporelle doit être comptabilisée si, et seulement si, il est probable que les avantages économiques futurs attribuables à l'actif iront à l'entité et si le coût de cet actif peut être évalué de façon fiable.

Comment évaluer ces biens immatériels reconnus à l'actif des entités ?

Dans le cas d'immobilisations incorporelles acquises séparément, le coût peut généralement être évalué de façon fiable comme étant le coût d'acquisition tel que le définit la norme IAS 38 (§ 24 à 28).

Et lorsque de tels éléments sont acquis dans le cadre d'un regroupement d'entreprises (donc avec d'autres actifs et passifs), ils sont susceptibles de faire l'objet d'une comptabilisation séparée du goodwill dans certaines situations. Pour illustrer notre propos, la norme IFRS 3 reprend des exemples d'actifs immatériels tels que marques, nom de domaine, titres de journaux, carnets de commande, goodwill…

En revanche, les marques, titres de journaux et de magazines, listes de clients et autres éléments similaires en substance générés en interne ne doivent pas être comptabilisés en tant qu'immobilisations incorporelles. Les dépenses engagées pour générer ces éléments ne peuvent pas être distinguées du coût de développement de l'activité dans son ensemble.

Par conséquent, ces éléments ne sont pas comptabilisés en tant qu'immobilisations incorporelles et ne peuvent être donc évalués séparément.

Ce qui n'est pas le cas d'autres actifs incorporels à l'image des frais de développement ou des brevets voir des logiciels. Le coût de ces actifs immatériels générés en interne comprend tous les coûts directement attribuables nécessaires pour créer, produire et préparer l'immobilisation pour qu'elle puisse être exploitée.

Conclusion : tout le patrimoine n'est pas identifiable -donc mesurable- d'où la notion d'information extra-financière ?

Nous voyons à travers ce raisonnement que la question posée au préalable de la mesure des actifs immatériels est complexe et que les référentiels comptables (IFRS ou référentiel applicable en France) ont permis de dégager une pratique permettant d'identifier, de reconnaitre et de valoriser le patrimoine immatériel d'une entité.

Mais il existe du patrimoine immatériel qui ne peut être appréhendé voir reconnu, et nous pouvons citer comme exemple, le capital humain (personnel de l'entreprise), qui ne peut être comptabilisé et évalué à l'actif d'une entreprise. Parfois, il vaut mieux ne pas reconnaitre l'ensemble des actifs immatériels pour éviter les dérives de ce que l'on peut qualifier de « comptabilité créative » qui permettrait de tout évaluer, mesurer, comptabiliser.

D'où la nécessité d'une information extra comptable pour mesurer la performance des entreprises et leur empreinte « carbone », que nous pouvons plutôt traduire, par l'impact sur l'environnement de leurs activités mais aussi la façon dont l'entité respecte la cadre dans lequel elle intervient notamment dans les pays ou la notion de droits humains ou sociaux présente un caractère secondaire comparé à l'impératif de développement. C'est « l'entreprise à mission », notion mise en place récemment dans le cadre de la loi Pacte.

Nous évoquons ici pour finir la notion de RSE (responsabilité sociétale et environnementale de l'entreprise) qui ne lie pas forcément la réussite ou le succès à la croissance ou à la performance financière. Mais nous parlons ici d'une notion qui s'invite de manière régulière dans le débat public…. Il s'agit de la notion de décroissance.

Droit de l'immatériel : Focus sur le régime juridique des actifs numériques au regard de

Céline MOILLE

Avocate et Docteur en droit privé international

La loi du 22 mai 2019 (loi Pacte), instaure un régime juridique spécifique en matière d'actifs numériques, communément appelés les crypto-actifs, qui prévoit, en France, le statut de prestataire de services sur actifs numériques (PSAN), couvrant un grand nombre d'activités (10 au total).

Adoptant une approche fortement inspirée de la régulation du secteur financier, la loi identifie une liste d'activités qui, ayant pour objet un actif numérique, sont alors qualifiés de « service sur actif numérique » dont l'exercice est subordonné à un enregistrement préalable obligatoire auprès de l'AMF.

Ces services sont détaillés par le code monétaire et financier dont la lecture révèle un champ extensif.

C'est sous le titre des « autres prestataires de service » que les PSAN ont intégré le code monétaire et financier (art. L54-10-1 à L54-10-5).

Ce régime prévoit un enregistrement obligatoire auprès de l'AMF pour les acteurs offrant ces services ainsi qu'un agrément optionnel.

L'agrément impose au prestataire de respecter différentes exigences en matière d'organisation, de conduite de leur activité et de ressources financières. Il n'y a jusqu'alors pas eu de société agréée par l'AMF et seulement une vingtaine ont été enregistrés.

L'enregistrement auprès de l'AMF est obligatoire pour quatre types de services : l'achat/vente d'actifs numériques contre une monnaie ayant cours légal (par exemple, échanger des bitcoins ou des ethers contre des euros), la conservation d'actifs numériques pour le compte de tiers (à savoir la conservation des clés privées des clients et la capacité à les utiliser en leur nom), l'échange d'actifs numériques contre d'autres actifs numériques et l'exploitation d'une plateforme de négociation d'actifs numériques. L'AMF n'intervient pas seule, puisqu'elle ne rend sa décision qu'après avoir reçu un avis conforme de l'Autorité de contrôle prudentiel et de résolution (ACPR).

Ce régime juridique exigeant est mis en œuvre par le régulateur dont il faut d'ailleurs observer que ses attentes ont évolué au fil du temps, et ce en dépit de la « jeunesse » du dispositif.

Le régime des PSAN s'est consolidé, voire il s'est durci depuis quelques mois et les obligations imposées aux porteurs de projets ne cessent de croitre, ce qui a tendance à décourager certains acteurs du marché.

En outre, l'ordonnance n°2020-1544 du 9 décembre 2020 renforçant le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme applicable aux actifs numériques est venue encadrer spécifiquement les acteurs du marché « crypto ».

En toute hypothèse l'AMF vérifie que le prestataire qui souhaite être enregistré se conforme bien à la réglementation relative à la lutte contre le blanchiment et le financement du terrorisme (LCB/FT).

En la matière, et comme pour les opérateurs du secteur financier, l'organisation du dispositif de LCB-FT doit être adaptée à la taille, à la nature des activités et des services sur actifs numériques fournis, ainsi qu'aux risques identifiés par le prestataire.

Au vu des attentes du régulateur français et de la relative nouveauté de la matière, il faut donc porter une attention et une vigilance certaines aux exigences légales et aux processus organisationnels que le prestataire doit mettre en œuvre pour y satisfaire.

David Colon

Enseignant et chercheur à Sciences Po, où il enseigne l'histoire de la communication

La manipulation numérique de masse, un nouveau risque immatériel

Depuis le début du XXe siècle, la manipulation est devenue une science, en même temps qu'un art pratiqué des « ingénieurs des âmes humaines » issus pour la plupart du monde de la publicité, des relations publiques, de la communication politique ou du divertissement. Passés maîtres dans l'art d'influencer les masses à leur insu, en tirant profit des avancées des sciences et des techniques, ils ont bouleversé les règles du jeu politique tout en permettant le triomphe de la société de consommation. D'Ivy Lee à Ernest Dichter, en passant par Albert Lasker, Edward Bernays ou John Hill, ils ont contribué à façonner le consentement au service de leur clients politiques ou industriels, en s'appuyant sur les médias de masse. Ces « maîtres du faire croire » ont ainsi très souvent contribué, dans les démocraties occidentales, à réduire ou limiter les risques tant politiques que sociaux.

Or, depuis moins de trois décennies une nouvelle génération de manipulateurs de masse s'est appuyée sur Internet et le numérique pour produire de nouvelles techniques de manipulation qui ne visent plus tant à conformer les attitudes et fabriquer le consentement démocratique qu'à cloisonner les individus, de semer la discorde au sein des sociétés, de rendre impossible tout compromis, et de favoriser la défiance. Croyant servir le bien commun, le chercheur Brian Jeffrey Fogg a inventé la « technologie persuasive », en appliquant les principes de la psychologie sociale à l'interaction entre les humains et la machine. Ses découvertes ont permis à ses élèves de Stanford de rendre les interfaces numériques des réseaux sociaux à la fois addictives et manipulatrices. Fils de psychiatre et ancien étudiant en psychologie à Harvard, Mark Zuckerberg a conçu avec Facebook une arme de manipulation massive, capable de modéliser, de prédire et d'influencer les attitudes et les comportements de ses 2,8 milliards d'utilisateurs. Ses outils publicitaires combinent non seulement tous les acquis de la persuasion de masse depuis un siècle mais aussi les trois grandes approches de l'intelligence artificielle : l'approche inductive, par l'analyse prédictive des données des internautes, l'approche déductive, par les expériences menées sur ses utilisateurs, et l'apprentissage profond, qui permet par exemple d'identifier l'état émotionnel ou psychologique de ces derniers. Parmi les « ingénieurs du chaos », Steve Bannon, est celui qui a le plus tôt compris le potentiel de ces outils pour déstabiliser l'ordre politique, et y est concrètement parvenu, avec Cambridge Analytica. La manipulation numérique est donc devenue un risque immatériel majeur, dont la Commission européenne s'est récemment saisie en prévoyant dans son projet de Règlement sur l'intelligence artificielle l'interdiction des « systèmes ou applications d'Intelligence artificielle qui manipulent le comportement humain pour priver les utilisateurs de leur libre arbitre ». Il reste à savoir si ce n'est pas trop peu, ni trop tard.

L'immatérialité dans le recrutement

Dan Deville

Président de Deville Group Executive Recruitment and Training

Dans les cabinets de recrutement comme j'ai pu initier le mien il y a 13 ans, les aspects immatériels ont pris une place conséquente autant pour les sociétés du CAC 40 comme dans les PME. En 2021, l'immatériel est devenu le critère n°1 dans l'embauche des cadres. Enumérons et expliquons sans filtre et en toute transparence la place de l'immatériel dans le recrutement.

Chacun d'entre nous est le fruit apparent d'un bas de l'iceberg complexe et invisible basé sur nos passés, nos expériences, nos échecs et nos réussites. Cet immatériel invisible aux yeux des autres est la clef de l'ensemble de notre comportement matériel. Il n'y a en effet jamais de hasard dans notre apparence, dans notre habillement ou dans notre langage : Ils sont les résultantes de ce qui est caché et ne peut être relevé que dans des circonstances particulières ou à l'occasion d'entretiens approfondis.

Recruter, c'est d'abord comprendre l'immatériel qui se cache derrière le matériel. Nous, recruteurs expérimentés, connaissons quelques méthodes pour y arriver. L'écoute active est l'une d'entre elles, et savoir poser les bonnes questions sur les aspects matériels en est une autre. Ceci veut dire avoir un sens aigu de l'observation et savoir « décortiquer » chaque détail des apparences. C'est aussi prendre en compte l'ensemble des signes ouverts ou cachés !

Dans les trois niveaux de communication habituels il y a :

- Le verbal, qui représente 7 % de la communication
- Le paraverbal (le ton) qui représente 38 % et
- Le non verbal (l'attitude) qui représente 55 %

Lorsque le verbal et le non verbal ne sont pas compréhensibles, c'est le non verbal qui résume le message.

Quant au silence, immatériel s'il en est, il est essentiel dans la communication et sa compréhension. Une langue se parle autant avec des silences qu'avec des mots…. La parole est d'argent et le silence est d'or en recrutement et les candidats qui ne savent pas écouter sont des candidats qui ont perdu d'avance. Il en est de même pour les recruteurs !

Pour conclure il me suffit de rappeler qu'on ne sait jamais ce que quelqu'un pense vraiment et que sa matérialité reste une simple façade cachant un invisible toujours complexe.

Le risque immatériel créé par la mise en cause pénale de l'entreprise et de ses dirigeants

François Mazon

Avocat

Lors de mes formations aux dirigeants sur la prévention du risque pénal dans l'entreprise, j'ai l'habitude de dire qu'aux sanctions prévues par le code pénal, privation de liberté, amende et peines complémentaires, s'ajoute un risque immatériel souvent très lourd de conséquence mais non prévu par le code pénal, l'atteinte à la réputation. En effet, le mot pénal est immanquablement associé à la délinquance de droit commun voire à la prison.

Or tous les jours des entreprises et des dirigeants sont condamnés pénalement y compris de très grandes entreprises comme en juin 2021 IKEA et son directeur général pour avoir espionné leurs salariés, ou en 2019 France Telecom devenue Orange et plusieurs dirigeants pour harcèlement moral, et la banque UBS et ses dirigeants pour blanchiment de fraude fiscale et démarchage illicite. Ces deux dernières entreprises ont fait appel mais en termes de réputation le mal est fait : même si la cour d'appel infirme les décisions de première instance, ce sera plus de deux ans après et l'impact positif de l'arrêt d'appel souvent peu relayé médiatiquement s'avèrera insuffisant pour faire disparaître la mauvaise réputation créée par le jugement de première instance.

Même avant tout jugement, le mot pénal peut entacher la réputation des entreprises et de leurs dirigeants : il suffit qu'une information sur une perquisition au siège d'une entreprise ou le placement en garde à vue d'un dirigeant tourne en boucle sur les réseaux sociaux et les chaines d'information en continue pour que leur réputation soit durablement abimée. Or une perquisition ou une garde à vue sont des actes d'enquête qui ne présument pas de la culpabilité d'une personne physique ou morale et toutes les enquêtes ne se terminent pas par un renvoi devant un tribunal correctionnel mais peuvent se clôturer par un classement sans suite ou un non-lieu … ce qui intéresse beaucoup moins les médias !

Pour minimiser ce risque immatériel, il faut pouvoir agir avant, pendant et après sa survenance.

Avant, la priorité est la prévention qui passe par trois étapes : identifier d'abord les 3 ou 4 infractions pénales qui représentent 80% du risque pénal de l'entreprise en fonction de son activité et de son organisation et en déduire des plans de prévention adaptés, puis mettre en place des délégations de pouvoirs, et enfin former le personnel exposé aux principaux risques identifiés.

Si néanmoins le risque se produit et qu'une enquête ou un procès a lieu, ce sont des actions de communication de crise qui peuvent s'avérer nécessaires. Les avocats en pénal des affaires sont de bons conseils mais l'appui d'un cabinet de communication spécialisé dans ce domaine est souvent utile pendant l'enquête ou le procès.

Enfin, une fois l'enquête ou le procès terminé, il faut contre-attaquer après une décision de classement ou de relaxe en accentuant la communication de cette « bonne nouvelle » pour rétablir la réputation entachée. Et, si une faute lourde des services de la justice peut être caractérisée, la loi (1) permet d'assigner l'État pour demander réparation du préjudice subi. Jean-Michel Baylet, patron de presse et homme politique, a ainsi fait condamner l'État en janvier 2015 pour une procédure qui a duré près de 10 ans dans laquelle il a été successivement mis en examen, renvoyé devant un tribunal et finalement relaxé. Il s'est dit qu'il n'avait pas été nommé ministre à cause de cette mise en examen…

(1) Article 141-1 du code de l'organisation judiciaire : « L'État est tenu de réparer le dommage causé par le fonctionnement défectueux du service public de la justice. Sauf dispositions particulières, cette responsabilité n'est engagée que par une faute lourde ou par un déni de justice».

La redondance dans l'Immatériel

Michel Philippart, DBA

Professeur, Département Stratégie,
EDHEC Business School

Un capital redondant est un capital qui ne contribue pas à la bonne marche de l'entreprise au quotidien mais qui est conservé pour réagir à un impondérable, ou qui a perdu son utilité à la suite d'évolutions de l'entreprise.

Par extension, d'autres redondances ont été introduites en entreprise et dans la chaîne d'approvisionnement. Dès que la gestion du risque est apparue sur le radar des industriels, la première recommandation était la redondance, que ce soit la redondance d'équipements critiques, de pièces de rechanges, de stocks de sécurité, ou la duplication des sources d'approvisionnement.

Lorsque s'est développée l'hyper-concurrence à la fin du siècle dernier, la modélisation des coûts a pointé l'impact de ces politiques de redondance dans la chaîne d'approvisionnement : deux fois plus de coûts fixes, moins d'effets d'apprentissage, plus de ressources pour gérer plus de fournisseurs, en particulier pour les approvisionnements complexes demandant investissement en capacité, outillage, formation de la main d'œuvre : cela apparaissait comme des coûts faciles à mesurer et à réduire. Il est aussi quasiment impossible de faire du juste à temps en utilisant deux fournisseurs. L'argument de la meilleure négociation parfois proposée par les tenants de la double source ne tenait pas à l'analyse car même en cas d'approvisionnement à 100% chez le même fournisseur ou prestataire, la renégociation périodique crée la tension concurrentielle recherchée par les chasseurs de coût. De même, la redondance interne, la duplication d'équipements critiques, a souvent été remplacée par la fiabilisation technique. Ces initiatives généraient des gains financiers facilement mesurables, donc rapidement adoptés pour devenir des pratiques standard.

Cependant, ces gains n'ont pas été mis en parallèle du coût associé à tous les risques dont ils étaient censés prémunir les organisations. C'est en particulier vrai pour les risques les plus faibles, pour lesquels une approche statistique de l'équilibre coût / risque était impossible. Ces risques invisibles, les risques immatériels, sont au cœur des réflexions de Place Escange. Autant il est possible d'évaluer la matérialité d'un risque fréquent, comme les risques sur les stocks liés à la variabilité dans le temps de la demande ou du délai de livraison, autant il est difficile d'évaluer celle d'un risque rare comme un incident majeur chez un fournisseur, la faillite d'un partenaire. Ces risques rares sont donc peu quantifiés, immatériel. Ils existent, mais ne rentrent pas dans les modèles financiers classiques utilisés pour piloter les opérations industrielles.

Comment les intégrer ? La gestion du risque passe par plusieurs étapes structurées, initialement développées dans les industries les plus sensibles, comme l'aéronautique. Après l'identification et la priorisation des risques vient la phase d'action. Quatre familles d'initiatives permettent de développer une politique de gestion des risques efficaces : la suppression du risque par un changement de choix, la réduction de la probabilité ou de l'impact, le transfert du risque à une entité plus à même de le gérer, et la préparation de la réaction à un incident. A chaque étape ses coûts et ses renoncements. Quand il s'agit de redondances, destinées à réduire la probabilité d'une rupture, l'entreprise devra en analyser la valeur non pas par une approche de comptabilité analytique et d'approches probabilistes, mais par une approche qui identifie les conséquences d'événements rares mais possibles, catastrophes naturelles, accidents industriels, événements géopolitiques, et bien entendu pandémies.

Jo-Michel Dahan

administrateur général, conseiller chez le Médiateur des entreprises

Positiver le récit immatériel

Les dirigeants d'entreprise sont immergés, depuis une vingtaine d'années, dans le 21ème siècle, caractérisé notamment par un accroissement du décalage entre la valeur boursière des entreprises et leur valeur comptable couronné par la suprématie du numérique. Pourtant, les instruments d'évaluation de la valeur de leur organisation demeurent empreints du poids de la comptabilité du tangible et du patrimonial dans une version qui a peu varié depuis de nombreuses années. Il ne faudrait toutefois pas sombrer, a fortiori dans une période de crise mondiale comme celle que nous vivons actuellement, dans une strate supplémentaire de discours anxiogène fondé sur une approche du risque mal équilibrée par des contreparties immatérielles évanescentes.

Alain Supiot, dans un ouvrage paru en 2015, La gouvernance par les nombres, nous avait déjà mis en garde sur la transformation de l'imaginaire industriel vers une ère cybernétique qui répond au vieux rêve occidental d'une harmonie fondée sur le calcul. A l'heure où près de 80% de la valeur d'une entreprise est composée d'actifs immatériels, il devient impératif pour les entreprises de s'outiller afin d'intégrer cette démarche d'évaluation au cœur même de leur stratégie. Et y procéder dans un climat serein, sans contrainte, par une approche volontaire et transparente sera gage de diffusion au sein de l'organisation et participera d'une qualité accrue du dialogue avec ses partenaires.

Concrètement, le capital immatériel d'une entreprise est constitué de ses compétences et connaissances accumulées, mais aussi de ses procédures, de sa réputation, de ses marques, de la fiabilité de ses systèmes d'information, de sa capacité d'innovation, ou encore, de la qualité de ses relations avec ses clients et partenaires et, désormais, de son respect des engagements sociétaux et environnementaux. Mais avant de se lancer dans un travail exploratoire d'identification des actifs immatériels stratégiques, il convient de bien en connaître les limites. Par exemple leur existence, selon le degré de maturité du capital à prendre en compte, n'existe souvent à l'origine que de manière latente et il faut déployer des efforts particuliers pour les transformer en actifs valorisables. De plus, il existe un risque de dévalorisation brutale et inattendue de certains actifs qui contraint à une prudence dans ses choix. Enfin, il ne faut pas se laisser inquiéter par la conceptualisation du terme « immatériel » alors qu'en réalité il permet d'aboutir à des actions très concrètes. Ceci étant posé, les meilleures pratiques dans ce domaine ont été de coupler cette intégration de la donnée immatérielle à d'autres démarches stratégiques de l'entreprise. Il en est ainsi de la stratégie de marque, du renforcement de la protection cyber ou de la responsabilité sociétale de l'entreprise, par exemple.

Il faut ainsi encourager les chefs d'entreprise qui, en adoptant un nouvel axe de développement, intègrent de manière concomitante une identification, une mesure et enfin une valorisation de données immatérielles indispensables pour l'enrichissement (au sens premier) des différents leviers d'accomplissement. A titre d'illustration, et dans une période où le bien-être des collaborateurs devient un impératif et parfois un critère d'embauche à rebours sur lequel les jeunes générations sont très attentives, le récit que chaque dirigeant pourra bâtir sur ce thème deviendra un atout précieux. Loin des clichés et d'un discours artificiel, c'est sur de véritables informations parfois plus ou moins quantifiables mais toujours objectivables que le narratif peut devenir un nouvel outil de dialogue pour établir la confiance avec son écosystème. A cet égard, le capital humain, nous l'avons vécu dans la période récente, est l'un des éléments les plus précieux que l'entreprise ne peut bouder en se fondant uniquement sur des indicateurs financiers ou comptables. J'aime à citer ce bel aphorisme : « en immatériel, tout ne se compte pas mais tout se raconte ». Les dirigeants d'entreprise vont aussi devoir devenir des conteurs de l'immatériel car cela sera at-

Stéphanie Verilhac Marzin

Directrice SVM Consult
Spécialisée en affaires publiques et réglementaires européennes et françaises dans les secteurs du digital, de la publicité, de l'information d'entreprise et de la gestion du risque

Intelligence Artificielle et immatériel : impact du projet de règlement européen sur la gestion de l'immatériel

Fin avril 2021, la Commission Européenne a présenté son projet de règlement européen sur l'Intelligence Artificielle, qui vise à mettre en place un outil règlementaire de gestion de l'Intelligence Artificielle. La Commission souhaite ainsi développer un cadre large, horizontal, de manière un peu similaire à l'approche englobante faite par le RGPD pour la protection des données personnelles, tout en adoptant un système basé sur la classification des risques liés à l'utilisation de l'intelligence artificielle. Or la protection du capital immatériel de l'entreprise repose également sur une approche liée aux risques et à la gestion de ces risques. Le suivi legistialtif du projet de règlement lié à l'Intelligence Artificielle aura donc un impact sur la gestion de l'immatériel notamment sur trois points : la définition de l'intelligence artificielle et du champ d'application territoriale du règlement, la classification des IA suivant une approche liée aux risques et les problématiques de conformité préalable que devront respecter les fournisseurs de solutions basées sur l'IA et leurs utilisateurs.

Le champ d'application et la définition choisis sont en effet volontairement larges, afin de s'assurer que toute application utilisant l'intelligence artificielle qui produit des effets sur un utilisateur européen soit concernée, quel que soit le pays dans lequel est basé la société ou le fournisseur de solution d'intelligence artificielle. Le champ d'application territorial est donc vaste, tout comme celui du RGPD. La définition de l'intelligence artificielle ou plutôt des systèmes d'intelligence artificielle concernés est également large et technologiquement neutre, englobant tout « logiciel développé avec une ou plusieurs des techniques et approches énumérées à l'annexe I et qui peuvent, pour un ensemble donné d'objectifs définis par l'homme, générer des extrants tels que le contenu, les prédictions, des recommandations ou des décisions influençant les environnements avec lesquels ils interagissent »[1]. Ainsi de nombreux outils de gestion du risque immatériel, qu'il soit réputationnel, commercial (risque-client), sécuritaire ou lié à la propriété intellectuelle se verront concernés dès lors qu'ils utilisent une forme d'intelligence artificielle dans leurs process.

Le projet de règlement prévoit par ailleurs une classification des systèmes d'intelligence artificielle basée sur le risque, avec une approche pyramidale en quatre niveaux : IA à risque inacceptable, IA à haut risque, IA à risque modéré et IA à faible risque. Selon cette classification, les fournisseurs de solutions d'intelligence artificielle devront respecter des mesures plus ou moins contraignantes, jusqu'à l'interdiction pour les IA à risque inacceptable. La majorité des IA devrait appartenir aux niveaux à risque modéré ou faible qui dès lors nécessitera des mesures de transparence telles que la notification aux utilisateurs d'une interaction avec une IA. Pour les IA classées à haut risque, telles que par exemple le credit scoring pour les consommateurs ou la gestion RH ou encore les algorithmes d'affectation des étudiants, il faudra obtenir une certification CE basée sur une conformité préalable devant être accordée par l'autorité compétente nationale. Cinq critères principaux seront pris en compte dans la gestion de la conformité : l'utilisation de datasets à jour et de haute qualité, une documentation précise et à jour comprenant les informations sur les connexions (logs) permettant une meilleure traçabilité, des mesures de transparence et d'information aux utilisateurs, des mesures renforcées en matière de cybersécurité et enfin une supervision humaine incluse dans le système. Le projet prévoit également la mise en place d'un système de gouvernance duale avec un « Intelligence Artificial Board » européen agissant comme coordinateur des autorités nationales compétentes, lesquelles pourront émettre des sanctions allant jusqu'à 6% du chiffre d'affaires global en cas de non-respect des règles. Nul doute dès lors qu'il est important pour toutes les entreprises utilisant et interagissant avec des solutions basées sur l'intelligence artificielle de bien suivre l'évolution de la proposition législative européenne et de mesurer leurs risques et leur exposition afin d'intégrer également cette composante dans la gestion de leur patrimoine immatériel.

[1] Traduction de l'article 3-1 du projet de règlement de l'UE « Artificial Intelligence Act ».

Risques immatériels et diplomatie

Bernard Valéro

Ancien diplomate, Consul général à Barcelone, Ambassadeur à Skopje et à Bruxelles, et ancien Porte-Parole du Quai d'Orsay

Quelle que soit la taille d'une entreprise, s'engager à l'international est aujourd'hui une impérieuse obligation afin de ne pas rester encalminée, avant de finir dépassée puis déclassée, dans le grand bain de la compétition internationale.

Sortir du cocon national ou de la bulle de confort européenne n'est pas chose aisée. Les entreprises voient en effet s'élargir aussitôt leur champ de risques immatériels et donc celui de leur vulnérabilité. Qu'il s'agisse d'exporter des savons de Marseille aux Etats-Unis ou des avions Rafale en Egypte, d'investir dans un projet gazier au Mozambique ou de contracter avec un fabricant chinois de masques en pleine pandémie, d'attirer sur le territoire national un investisseur canadien ou une startup de Singapour, les ressorts du risque immatériel sont les mêmes : nouveaux interlocuteurs/partenaires, nouveau cadre juridique et judiciaire, nouvel environnement géopolitique, nouveau climat des affaires, nouvelles règles du jeu social, cinquante nuances de différences linguistiques et culturelles, autant de facteurs d'incertitude qui altèrent les habitudes acquises au sein des frontières nationales au-dedans desquelles les risques immatériels peuvent être davantage maitrisés.

Au fil de la montée en puissance de la mondialisation et de l'ampleur prise par l'économie des flux et par celle de l'innovation, les Etats se sont employés à s'adapter à cette nouvelle donne qui fonde ce qui est en train de devenir l'économie mondiale du XXIe Siècle. Dans ce contexte, la communauté internationale s'est efforcée de réguler cette évolution par une gouvernance de l'économie mondiale afin de ne pas laisser s'imposer la loi du plus fort d'une part, et de veiller au respect des grands équilibres internationaux d'autre part : mise sur pied d'organisations ad hoc (OCDE, OMC, OIT), construction d'ensembles économiques régionaux (ASEAN, ALENA, CEDEAO, MERCOSUR par exemple), mise sur pied d'institutions financières régionales (BAD, BID, BERD) en appui au FMI et à la Banque mondiale, développement d'un multilatéralisme à géométrie variable et à plusieurs vitesses (G7, G8, G20, BRICS, IBSA), sont autant d'illustrations (il y en a beaucoup d'autres), de cet effort collectif de la communauté internationale visant à ordonner, structurer, réguler la marche de l'économie du monde et des échanges internationaux.

Cela étant posé, lorsqu'une entreprise s'engage sur un pays étranger (pour y investir, y exporter, s'y approvisionner), elle sera immanquablement confrontée à de multiples risques immatériels qui peuvent aller, selon les destinations et les circonstances, de la sécurité de ses employés aux problèmes soulevés par la corruption, de l'apprentissage des règles du droit et des usages locaux à l'état de la conjoncture politique locale ou régionale, de la lutte contre les contrefaçons ou le pillage technologique à la protection des brevets.

C'est précisément pour accompagner et appuyer les acteurs économiques français à l'international que le Quai d'Orsay a mis en œuvre depuis une bonne vingtaine d'années une active diplomatie économique, dimension désormais centrale de la politique étrangère de la France. Aujourd'hui priorité politique affichée, cette diplomatie économique repose sur :

- Une mobilisation forte déclinée sur un large éventail d'engagements au service de toutes nos entreprises, en faveur du rayonnement économique de la France dans le Monde et au bénéfice de l'attractivité de la destination France et du « Made in France ».
- Une Direction de la Diplomatie économique au Quai d'Orsay, en quelque sorte le cœur du réacteur, qui mène ses missions en s'appuyant notamment sur un certain nombre de représentants spéciaux pour certains pays ou zones géographiques (Russie, Chine, Australie, Japon, Inde, Balkans, Asie centrale, ASEAN).
- Un engagement permanent de l'ensemble du réseau diplomatique et consulaire français (le 3ème au monde aux côtés des Américains et des Chinois), au premier rang duquel les ambassadeurs, mais aussi leurs équipes des chancelleries diplomatiques, des services économiques et des services de coopération culturelle et scientifique.

Le travail des réseaux locaux : les chambres de commerce et d'industrie françaises à l'étranger, les conseillers du commerce extérieur de la France, le réseau des établissements d'enseignement français à l'étranger, les élus des Français de l'étranger, autant de réseaux d'acteurs qui, sur le terrain, soutiennent nos entreprises et accompagnent l'expatriation de leurs employés.

- Un biotope de partenaires : l'opérateur Business France, BPIFrance, la Caisse des Dépôts, le Medef, la Cpme, les administrations économiques, les collectivités territoriales.
- Des négociations internationales menées en permanence sur tous les fronts, sur tous les sujets, sous tous les cieux, dans toutes les enceintes afin que le cadre juridique normatif, tant européen qu'international soit le plus favorable aux intérêts de la France et de ses acteurs économiques.

Cette boite à outils de notre diplomatie économique se nourrit de la spécificité de l'ADN et de la culture d'entreprise du Quai d'Orsay, familier des risques immatériels et des réponses à apporter à ceux-ci : data et intelligence économique, capacité d'identification d'aiguillage et d'accompagnement vers les bons interlocuteurs, conseils aux entreprises, promotion d'image et influence (« soft power »), négociations des cadres publics de régulation juridique et règlementaire, décryptage des réalités et des particularismes locaux, relai d'influence et d'accès aux décideurs, communication, appui au règlement des contentieux, etc…

Concilier une mondialisation plus juste et mieux maitrisée avec la défense légitime de nos entreprises telle est l'essence même de cette diplomatie économique de la France au service de laquelle le Quai d'Orsay met ses moyens, son expertise, et sa culture de la lutte contre les risques immatériels, celle-ci étant aujourd'hui une dimension essentielle de la diplomatie.

La valeur immatérielle de l'immeuble

Philippe Marin

Avocat au Barreau de Toulon (droit immobilier, droit des affaires)

L'immobilier de bureaux est le reflet de nos modes de vie et de travail. La question de ce qu'il apporte à l'entreprise est plus que jamais d'actualité. En effet, on savait la génération des millennials particulièrement sensible à la qualité de vie au travail ; on peut parier que la crise sanitaire que nous traversons sera un accélérateur majeur de la transformation des bureaux en espaces plus flexibles, plus conviviaux et porteurs de valeurs humaines et environnementales, moteurs de performance et d'attractivité. Les nouveaux bureaux consacrent déjà une place croissante à de nouveaux services, à la mobilité, aux lieux de vie et plus généralement à une meilleure prise en compte des éléments touchant au bien être des occupants.

Cette évolution consacre la notion de valeur d'usage des actifs immobiliers. En effet, de nombreux critères, parmi lesquels la qualité de l'air, les niveaux de bruit, de luminosité, l'ergonomie des aménagements ont un impact sur la santé des occupants et jouent un rôle essentiel dans la diminution des arrêts de travail et l'amélioration de leur productivité. De même la proximité de transports et le développement de services dans l'immeuble est un enjeu d'attractivité pour les entreprises. Ces critères immatériels donnent à l'immeuble une valeur de plus en plus immatérielle.

Comment calculer les avantages immatériels d'un immeuble pour l'entreprise ? Il parait au premier abord plus facile de mesurer les surcoûts engendrés par la prise en compte des exigences environnementales ou de responsabilité sociale du bâtiment, que le gain de productivité des salariés et l'impact sur le compte de résultat. Toutefois, toutes les études réalisées ont montré que l'amélioration du bien-être des salariés dans l'espace de bureaux est un levier d'optimisation, qui a des répercussions sur la performance de l'entreprise. Le gain de productivité qui en découle est alors quantifiable pour l'entreprise, ne serait-ce que par comparaison, et constitue un véritable goodwill.

Cette valeur d'usage est-elle pour autant intégrable dans les méthodes communes de valorisation immobilière ? Si les experts immobiliers prennent généralement en compte les caractéristiques des bâtiments et la qualité de ses aménagements dans la méthode par comparaison, il est plus difficile d'estimer le bien-être des occupants et l'usage qu'ils en font. En revanche, la part de valeur immatérielle de l'immeuble apportée par l'amélioration de performances économiques peut se retrouver dans la méthode d'évaluation par le rendement. En effet, les immeubles de bureaux intégrant le confort des espaces de travail et des services offerts à leurs occupants, voient leur valeur locative augmenter. Dès lors, si les loyers augmentent, la valorisation de l'actif immobilier augmente également.

Les actifs immobiliers, comme facteur de création de valeur immatérielle, peuvent donc rejoindre le capital immatériel de l'entreprise.

L'IA, l'avenir mondial – Pour une politique économique européenne du nouvel immatériel

Thomas Kerjean

CEO – Mailinblack

De toutes les formes d'activité humaine, la musique est de loin la plus intéressante à étudier pour anticiper l'évolution du monde. Petite musique de nuit avant l'aube, bruits précurseurs d'une révolution, immatériel privatisé par le concert annonçant l'avènement de la bourgeoise, propriété intellectuelle piratée par Napster, la musique permet d'entrevoir les organisations politiques, sociales et économiques en devenir. Jacques Attali l'a brillamment résumé dans Bruits, ouvrage publié l'année de ma naissance.

L'économie contemporaine fait beaucoup de bruits. Mais si on porte un regard attentif sur son épine dorsale, on y voit un squelette immatériel : La Data. Fuel de l'Intelligence Artificielle, elle aussi immatérielle, la Data est le moteur de tous les modèles économiques, toutes les innovations majeures des années à venir.

Enfant de la post-guerre froide, de l'essor libéral, de la fin de l'Histoire, j'ai été bercé aux sons des premiers modems, quand Internet a émergé en 1992, aux mélodies de Nevermind de Nirvana, groupe de grunge emblématique de Seattle. Seattle, c'est le berceau de Microsoft et d'Amazon, au nord de la Californie où bronzent les développeurs d'Apple, Google et Facebook.

Ces 5 entreprises, avec plus récemment les BATX, sont la moelle épinière de tous les modèles économiques à venir, qui reposeront sur l'une de leur plateforme cloud. Chez Microsoft, en écrivant mes lignes de codes, en vendant mes premiers contrats de licences, en écrivant mes premières spécifications fonctionnelles, un casque sur les oreilles, j'ai assisté au fil des années à une privatisation tout aussi étonnante que celle de la musique au fil des siècles : Celle des données personnelles, Big Data, tout aussi immatériels et précieux.

L'économie contemporaine se dessinait : Sur un fond mélodieux et jovial de services gratuits, j'ai vu chaque État mondial, dont le mien, devenir progressivement le pétrole de Google et Facebook, dont le modèle économique consiste à privatiser vos données personnelles pour entrainer des algorithmes, qui ont pour but de vous faire acheter plus, mieux ; de stimuler votre dopamine à cadence calculée ; d'orienter vos choix. On amalgame souvent à tort les GAFAMs : Amazon et Microsoft, en tout cas dans leurs activités Cloud, n'ont pas le même modèle économique : Le leur consiste à monétiser un service d'infrastructure (IaaS), de plateforme (PaaS) ou bien d'application (SaaS). Vous achetez le produit dans ce cas et n'êtes pas, comme avec Google et Facebook, le produit qui est vendu.

Qu'on se comprenne bien ici : Il ne s'agit pas seulement d'un secteur économique fortement valorisé : L'industrie de la Tech, au premier rang de laquelle Google (Search, Android, YouTube) et Facebook (Instagram, WhatsApp) figurent, sont les piliers de la nouvelle économie mondiale. Au sommet de la chaîne de valeur, leur stockage et calcul (Cloud d'infrastructure), leur cybersécurité (identité, applications, serveurs, etc.), leurs IA (auditives, visuelles, textuelles), les Big Data que nous leur offrons sans contrepartie, ces leaders mondiaux sont le cœur même de tout ce qui va suivre. L'innovation produit (connecté, intelligent), l'optimisation de processus (par le machine learning), les interfaces des objets eux-mêmes (IoT, Android, iOS) auront durablement pour socle les Clouds publics américains et progressivement chinois.

La bonne nouvelle est ici : La France est un pays de mathématiques. Un pays de recherche. Elle a pris conscience jusqu'aux sommets de l'État de l'importance vitale de créer une autonomie, une souveraineté numérique, en impulsant un projet de cloud souverain, en dynamisant un écosystème via les French Tech, via les grands défis technologiques impulsés par le rapport C. Villani notamment.

L'autonomie immatérielle, celle de la Data et des IA doit devenir un impératif européen. Cette autonomie se construira par le rapatriement de talents en data science, en développement, en management et innovation produit ; également par une politique de fonds d'investissement européennes plus coordonnées et focalisées, avec l'aide des instances européennes.

Nous avons toute latitude pour entrainer nos propres IA avec nos données business, santé, collectivités, cybersécurité colossales. Toute latitude pour réunir nos fonds d'investissement et créer les licornes d'un immatériel réinventé, plus éthique, plus mature, plus responsable. Les licornes qui seront les garantes de l'autonomie de tous les autres secteurs de l'économie : maison, bâtiment, voitures, écoles, hôpitaux, hôtels… connectés et intelligents. L'Europe est l'autre puissance mondiale en devenir, qui doit dès à présent affirmer et consolider sa volonté de faire émerger les prochains leaders numériques mondiaux.

L'immatérialité d'une procédure pénale

Armand Feste-Guidon

Avocat au Barreau de Marseille (droit pénal des affaires)

Le risque pénal fait désormais partie de la vie des affaires.

Qu'elles soient relatives à l'usage des biens de l'entreprise, aux comportements à l'égard des salariés, à l'atteinte potentielle à l'environnement, les incriminations ne manquent pas et se multiplient. C'est l'esprit du temps – peut-être d'un nouveau moralisme – qui veut enserrer l'entièreté des comportements des sociétés dans le carcan de la loi et offrir une réponse judiciaire à toute action imprévue.

Ces risques sont heureusement de mieux en mieux appréhendés par les chefs d'entreprise, qui ne sont aujourd'hui plus surpris par la perspective d'une perquisition, d'une garde à vue, ou du regard inquisiteur d'un juge. Rompus à la stratégie, aux négociations difficiles, à l'importance du secret des affaires, nos entrepreneurs sont particulièrement conscients de ce nouvel environnement et s'y sont adaptés en assimilant les ressorts et la logique parfois tortueuse du code de procédure pénale.

C'est néanmoins dans les interstices de ce code que vient se nicher un nouveau risque immatériel : celui de la communication dévoyée de l'information. Dans une procédure pénale, cette communication de l'information a l'inconvénient paradoxal d'être à la fois inexistante et débordante.

Ainsi, à l'heure où est exigée des acteurs économiques une transparence toujours plus grande, l'accès au contenu d'une procédure pénale est tout d'abord lacunaire. Dans le cadre d'une enquête préliminaire – cadre d'investigation ultra majoritaire –, les personnes soupçonnées n'ont pas accès au dossier de la procédure. Il est ainsi exigé des chefs d'entreprise des réponses exhaustives et techniques alors qu'ils ne peuvent pas même consulter les pièces au fondement des soupçons formés à leur endroit.

Inversement, l'accès à l'information autour d'une procédure pénale se révèle trop souvent sans contrôle et nauséabond. Rien n'attire plus les caméras que les nuques baissées sortant d'un commissariat ou d'une salle d'audience, rien ne fait davantage couler d'encre que les extraits soigneusement choisis d'une audition ou d'un interrogatoire d'une personnalité en vue.

Les dégâts de ces quelques propos ou images volés sont considérables : ils contaminent toute la physionomie d'une compagnie et entache sa réputation. Cette mauvaise réputation détourne les clients d'une marque car ils redoutent de voir leur propre nom associé à celui du pestiféré. Elle affecte également les équipes : le management voit son attention accaparée par la problématique pénale et les collaborateurs, quant à eux, se montrent inquiets, les meilleurs talents devenant plus difficiles à retenir ou à attirer.

Pour pallier cet accès contrarié à l'information, l'entreprise aura besoin d'un professionnel de la matière pénale afin de s'approprier le bon tempo. A l'immatérialité de la communication pervertie, il opposera l'immatérialité du contrôle de la temporalité. L'avocat spécialisé envisagera ainsi l'allongement du temps par l'exercice des voies de recours utiles ou au contraire son rétrécissement en s'emparant des mécanismes de justice négociée (CRPC, CJIP). Son expertise conduira alors l'entreprise à faire de nouveau sien le temps judiciaire.

Actifs incorporels ou immatériels et avantages fiscaux

Pierrick Babin

Avocat fiscaliste à la Cour de Paris

Depuis le 1er janvier 2019, le régime de l'« IP box » permet de bénéficier d'un taux préférentiel d'impôt sur les sociétés de 10 % sur les revenus tirés de l'exploitation de certains actifs incorporels tels que les brevets ou les logiciels protégés par le droit d'auteur.

Pourquoi avoir institué un tel régime préférentiel ?

Pour lutter contre les pratiques fiscales dommageables, l'OCDE puis l'Union européenne ont consacré l'approche du lien dite « nexus » explicitée dans le rapport sur l'action 5 du projet BEPS (« Base Erosion and Profit Shifting »), consistant à conditionner l'application d'un régime favorable d'imposition des profits tirés de l'exploitation et de la cession d'un brevet ou actif incorporel ou immatériel assimilé à la réalisation des dépenses de recherche et développement engagées par le contribuable lui-même pour développer cet actif.

En pratique, l'approche « nexus » est basée sur l'idée que l'avantage fiscal afférent aux revenus de la propriété industrielle doit être corrélé avec l'importance des dépenses de recherche et développement engagées en amont sur le territoire qui accorde cet avantage fiscal.

C'est pourquoi la Loi de Finances pour 2019 a mis en conformité le régime fiscal français avec cette approche « nexus » : les dispositions ainsi intégrées à l'article 238 du Code Général des Impôts (CGI) conditionnent désormais l'accès au régime préférentiel à la réalisation par le contribuable bénéficiaire de l'avantage fiscal des activités de recherche et développement (R&D) génératrices de revenus.

Ainsi, conformément aux dispositions de l'article 238 du CGI, le résultat net imposable selon le régime de faveur est déterminé en deux temps :

L'entreprise détermine d'abord le résultat net de la concession, sous-concession ou cession

Si ce résultat est positif, l'entreprise lui applique un ratio « nexus » correspondant au rapport entre les dépenses de recherche directement réalisées par l'entreprise ou des entreprises sans lien de dépendance et les dépenses de recherche totales.

Mais ce ratio « nexus » peut toutefois être écarté dans certaines circonstances exceptionnelles au profit d'un ratio de remplacement.

La possibilité d'obtenir un ratio de remplacement est subordonnée à l'obtention d'un agrément préalable, délivré sous réserve que les deux conditions suivantes soient réunies :

1- le ratio « nexus » doit être supérieur à 32,5 % ;

2- le ratio de remplacement doit être significativement supérieur au ratio « nexus » du fait de circonstances exceptionnelles indépendantes de la volonté du contribuable.

Le résultat net déterminé après application du ratio « nexus » ou du ratio de remplacement peut sous certaines conditions être soumis à une imposition au taux réduit de 10 %.

Ce nouveau régime d'imposition a un caractère optionnel. L'option pour ce régime préférentiel d'imposition est formulée pour chaque actif, bien ou service ou famille de biens ou services dans la déclaration de résultat de l'exercice au titre duquel elle est exercée.

En application du nouvel article L 13 BA du Livre des Procédures Fiscales (LPF), les entreprises ayant opté pour l'application du régime de faveur sont soumises à une obligation documentaire permettant de vérifier les modalités de détermination du résultat net soumis au taux réduit de 10 %.

Ainsi, ces entreprises doivent tenir à disposition de l'administration fiscale, à la date d'engagement d'une vérification de comptabilité, une documentation comprenant une description générale de l'organisation des activités de R&D de l'entreprise qui cède un ou plusieurs actifs mentionnés à l'article 238, I du CGI ou concède les licences d'exploitation de ces actifs, ainsi que des informations spécifiques concernant la détermination du résultat imposable.

Il y a lieu de noter que l'entreprise qui cesse d'appliquer le régime de faveur au titre d'un exercice donné en perd définitivement le bénéfice pour chaque actif, bien ou service ou famille de biens ou services concernés.

A titre d'exemple, tel serait le cas si l'entreprise ne procédait plus au suivi des dépenses de R&D.

Combiné au crédit d'impôt recherche (CIR), qui permet de financer une partie des dépenses éligibles au crédit d'impôt en phase de recherche, la taxation à 10 % des revenus en phase d'exploitation permet à la France de se placer au premier rang des pays européens en matière de fiscalité attractive pour les activités de recherche et d'innovation.

Mais, si le régime d'imposition au taux préférentiel de 10 % est incontestablement un avantage significatif, la complexité de ce régime implique pour les entreprises de se faire assister par un avocat fiscaliste, afin de pouvoir bénéficier d'une parfaite sécurisation fiscale de ce régime de faveur.

Stéphane Fargette

Spécialiste du Management de Transition

Le recrutement d'un manager s'appuie aussi sur des valeurs immatérielles

Un manager, et spécialement lorsqu'il est recruté en mission de transition, doit savoir s'appuyer depuis toujours sur les valeurs classiques et traditionnelles de l'entreprise. Mais qu'en est-il aujourd'hui de la prise en compte des valeurs que l'on pourrait nommer « le capital immatériel » tels que la prise en compte des dirigeants et des collaborateurs de cette entreprise, de sa marque, des capacités de connaissances et de R&D, de sa capacité de transformation notamment dans le numérique et dans la data, de la qualité de ses relations avec ses partenaires comme avec ses clients, et de la maîtrise de son écosystème territorial par exemple ?

La recherche d'un dirigeant, d'un manager, se doit aujourd'hui d'intégrer l'ensemble de ces éléments, mais encore plus, de savoir identifier la compréhension et la prise en compte de ceux-ci chez la ou le manager qui vont être confrontés aux défis de l'entreprise. Il ne suffit plus d'être un bon gestionnaire, ni même un bon visionnaire.

Dans un processus de recrutement très ramassé sur quelques jours et très exigeant, aux qualités techniques et managériales du manager, au processus qui se doit de vérifier ses compétences, ses références et son adéquation avec le besoin au sein de l'entreprise, il faut encore plus prendre en compte aujourd'hui sa capacité à gérer l'ensemble de ce capital immatériel.

En effet, à quoi servirait un Directeur informatique s'il n'avait pas une approche appropriée du traitement de la data de son entreprise ou de l'apport d'une digitalisation adaptée pour les forces vives comme pour les clients ? A quoi servirait un Directeur financier si, au-delà des logiciels (actifs incorporels) il ne prenait pas en compte le capital humain qui est amené à les utiliser ? A quoi servirait un Directeur général si, dans sa vision et dans sa politique de l'entreprise, il ne pouvait intégrer l'ensemble de ces valeurs immatérielles au même titre que les autres ?

Recruter un manager de transition nécessite aujourd'hui de savoir déceler l'ensemble de ces capacités, et ces qualités à les mettre en musique. Une société est la somme d'éléments matériels et immatériels, qui ne peuvent être dissociées.

Dans le management de transition, comme dans toute forme de recrutement aujourd'hui, l'ensemble des acteurs (entreprises, candidats, cabinets) ont parfaitement intégrés ces valeurs immatérielles. L'engagement sociétal, les qualités du management, la vision de l'entreprise non seulement de ses perspectives mais également de son rôle dans les évolutions du monde que nous vivons, les notions telles que la bienveillance, l'éthique, la parité, sont aujourd'hui des sujets essentiels qui se doivent d'être traités.

Impossible aujourd'hui, et encore moins demain, de ne pas prendre en compte l'ensemble de ces valeurs. Et il ne fait aucun doute qu'elles sont déjà et vont être plus encore intégrées dans les critères d'évaluations.

En réalité, les valeurs immatérielles ont toujours été présentes dans chaque entreprise, dans chaque société. Mais elles commencent à peine à être valorisées à leur juste importance.

Eric Freysselinard

Directeur de l'Institut des hautes études du Ministère de l'Intérieur

Haro sur les deepfakes, potentiel risque pour les entreprises

Selon le milliardaire de la Silicon Valley Peter Thiel, qui a notamment fondé les entreprises PayPal ou Palantir, la pandémie de Covid-19 marque le vrai début du XXIème siècle, l'année où « la nouvelle économie a remplacé l'ancienne ». Difficile de lui donner tort, quand on constate le développement spectaculaire du télétravail, et de son corollaire la visioconférence. Même lorsque la crise sanitaire sera achevée, ces changements, cette dématérialisation accélérée des entreprises dans leurs méthodes de travail, leurs process, les relations humaines, ne s'achèvera pas et continuera de plus belle. L'adaptabilité extraordinaire des entreprises doit être soulignée, mais ce nouveau paradigme emporte par là même de nouveaux risques immatériels, qu'il convient d'étudier, et pour lesquelles les entreprises doivent se préparer.

Ces risques sont légion, mais j'aimerais en citer un en particulier. Les « deepfakes » sont des produits de l'intelligence artificielle et du machine learning : à partir de photos, vidéos ou audios préexistants, un algorithme générateur s'entraîne à créer des répliques jusqu'à ce qu'elles soient photoréalistes. Ainsi, il est possible avec cette technique de faire dire n'importe quoi à quelqu'un dans un audio ou une vidéo, pourvu qu'il y ait suffisamment de données sur la personne en question, et les logiciels développés pour créer des deepfakes sont de plus en plus performants. Il n'est évidemment pas certain que de telles méthodes soient utilisées dans un but malveillant : elles peuvent être utilisées dans un objectif de caricature notamment, ou pour simplifier la réalisation de vidéos ou films amateurs.

Mais les risques pour les entreprises sont réels : dans un monde où les communications importantes passent par visioconférence, quid d'une usurpation d'identité d'un participant, par des hackers, des escrocs ou des espions industriels ? Un exemple de 2019 est éloquent en la matière : le dirigeant d'une entreprise britannique a été berné, croyant entendre au téléphone la voix du PDG de sa société-mère. A sa « demande », c'est-à-dire celle de l'escroc, il a transféré 243 000 dollars à un faux fournisseur, avant de se rendre compte de la supercherie. Ce genre de manœuvres est amené à se développer, et sera peut-être le rançongiciel du futur. Les dangers liés aux deepfakes peuvent être bien sûr de tout autre nature : j'ai cité les possibles cas d'espionnages industriels, notamment par des prédateurs étrangers, mais un actif immatériel essentiel pour les entreprises est la réputation. Des deepfakes pourraient très bien être utilisés pour attenter à la réputation d'une entreprise, en faisant tenir des propos intolérables à un cadre dirigeant par exemple.

Si ce rapide tour d'horizon doit nous inciter à être prudent, il doit surtout nous inciter à appréhender ce genre de risques bien en amont afin d'y faire face efficacement. C'est tout le sens du travail de l'IHEMI que je dirige. Dans le cadre de notre Observatoire des crises, nous entamons des études prospectives sur ce type de dangers. Nos formations, en particulier la session nationale Protection des entreprises et intelligence économique, sont un atout majeur pour les cadres d'entreprise, afin que ces derniers soient préparés au mieux à ces enjeux. Enfin, le ministère de l'Intérieur s'implique pleinement dans ces enjeux, avec la présence dans chaque département d'un sous-préfet à l'intelligence économique, auquel les entreprises peuvent s'adresser.

Droit immatériel : nouvel obstacle à l'obtention d'identification sur internet sur requête

Chloé Legris-Dupeux

Avocat au Barreau de Paris, spécialisée en droit pénal sur internet : e-réputation, dénigrement, diffamation, injure, vol de données, intrusion dans des systèmes

Victime de tweets diffamatoires et injurieux, une société avait obtenu sur le fondement de l'article 145 du Code de procédure civile notamment, que le Président du Tribunal de grande instance de Paris ordonne à Twitter en sa qualité d'hébergeur de contenus de tiers de lui communiquer les données d'identification qu'elle détenait sur le titulaire du compte depuis lequel était émis les tweets litigieux.

Le 22 juillet 2020, la Cour d'appel de Paris a estimé que le requérant ne justifiait pas de la nécessité « pour l'efficacité de la mesure sollicitée d'agir par surprise ni surtout la raison pour laquelle la mesure n'aurait pas pu être obtenue par une assignation en référé alors qu'elle indique elle même que le litige potentiel ne concerne nullement la société Twitter ».

L'application de cette solution jurisprudentielle en matière d'identification sur internet risque cependant de priver les requérants de leur droit de recours effectif à la Justice.

La Cour d'appel de Paris juge habituellement que : « l'éviction du contradictoire, principe directeur du procès, nécessite que le requérant justifie de manière concrète, les motifs pour lesquels, dans le cas d'espèce, il est impossible de procéder autrement que par surprise ».

Si cette solution s'explique dans les affaires de concurrence déloyale, l'arrêt « Twitter » rendu du 22 juillet 2020 pose de nombreuses problématiques en matière d'identification sur internet, dans lesquelles le recours à une procédure non contradictoire a toujours été adopté comme la solution la plus efficace, en raison des éléments suivants :

- le requis n'est pas l'adversaire du requérant dans l'hypothèse dans laquelle un litige pourrait découler de l'exécution de l'ordonnance sur requête ;
- l'exécution de l'ordonnance sur requête afin d'identification auprès de l'hébergeur ou du fournisseur d'accès à internet ne suppose aucune atteinte à l'intégrité du domicile ou du siège social du requis ;
- le requis est tenu par la loi de détenir et de conserver pendant un an les données d'identification recherchées ;
- les hébergeurs et fournisseurs d'accès à internet ont l'obligation de transmettre les données d'identification qu'ils détiennent, sous peine de sanction pénale ;
- la LCEN prévoit le recours à la procédure sur requête dans le cadre de l'article 6-I-8° qui dispose que « l'autorité judiciaire peut prescrire en référé ou sur requête, à toute personne mentionnée au 2 (hébergeur) ou, à défaut, à toute personne mentionnée au 1 (FAI), toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne ».

Jean-Baptiste Hennequin

Administrateur de la Ville de Paris & Directeur Général chez Fondation Inria

L'immatériel, évanescent hégémonique

L'immatériel évanescent

L'immatériel semble se définir par opposition au monde des objets. Invisible et intouchable. Et pourtant, il désigne une réalité, créée par le langage et l'abstraction. L'homme donne vie aux choses, en les désignant par des signes.

La pensée, dite abstraite, se déroule cependant dans des machines cérébrales humaines, animées par la biochimie et les impulsions électriques, questionnant la distinction entre le corps et l'esprit.

L'immatériel relève par conséquent du mystère.

La physique quantique, que « personne ne peut comprendre » (Richard Feynman), nous dit qu'une particule peut se trouver à deux endroits différents au même moment, ou qu'un chat est vivant et mort à la fois (Schrödinger).

La distinction entre l'immatériel et le matériel reste donc inaccessible à l'esprit humain.

L'immatériel a cependant transformé nos vies. La toute-puissance du numérique illustre cette domination.

L'immatériel numérique en voie d'hégémonie

Turing et sa machine, Gordon Moore et sa loi éponyme, représentent les prodromes de la domination de l'homme par ses inventions numériques.

Turing a décodé Enigma. Il a écrit le premier programme informatique et conçu les fondements de l'ordinateur. Il subira cependant une castration chimique. Tirons les leçons de ce présage.

Gordon Moore et sa loi éponyme, à savoir le doublement de la puissance de calcul des ordinateurs chaque année, a prédit son extinction en 2020, en raison des limites liées à la taille des atomes. Nous y sommes. Que va-t-il se passer ? La capacité de calcul va continuer à croître grâce à la physique quantique, qui permettra de décupler la puissance des ordinateurs, et de casser toutes les clefs de cryptographie fondés sur les systèmes binaires.

Colonisation immatérielle ou sursaut de l'Europe ?

A l'heure où j'écris ces lignes, le numérique accapare le temps de cerveau humain, dans des proportions sans précédent. Le machine learning a donné à Google sa toute-puissance, grâce au « natural language processing », c'est-à-dire l'interprétation du langage pour devancer nos désirs. L'intelligence se joue de notre narcissisme à travers les réseaux sociaux (Bernard Stiegler).

Demain, l'apprentissage automatique révolutionnera la santé et les transports.

Mais notre bel esprit européen n'est pas préparé à ces révolutions.

Malgré quelques succès (Iliad, 3DS), la France se trouve en voie de colonisation numérique. La suprématie américaine et asiatique s'avère écrasante, sans égard pour l'éthique, ni la protection de la vie privée.

D'aucuns en accusent le manque d'argent et la complexité bureaucratique européenne.

Mais si Dataiku et Criteo, des fleurons de l'intelligence artificielle, sont allées se financer aux Etats-Unis, ce n'est pas seulement pour ces raisons…

Dans nombre de grandes entreprises, le globish de l'« open innovation » des « labs » et de la « data science » fleurit en proportion inverse de la réalité.

J'ai ainsi entendu des dirigeants de grandes banques ou d'assurances m'expliquer qu'ils trouveraient toutes les solutions à leurs problèmes chez Google. Ou encore m'affirmer, par inculture plus que par malveillance, que les institutions scientifiques nationales que je représentais, étaient des filiales d'Amazon. C'est ainsi que de grandes entreprises enfoncent les clous de leur cercueil, en étant persuadées de préserver leur avenir. Produire de la rentabilité de court terme, critère décisif de choix et d'évaluation des dirigeants, n'est pas compatible avec des stratégies de développement pérennes, où la technologie occupe une place majeure. L'inexistence d'un vaccin français en constitue la preuve flagrante.

Les Jobs, Musk, Thiel, Zuckerberg ont su s'épanouir pour une raison principale : leur intérêt pour la recherche. Et aussi, à la faveur d'une certaine décontraction américaine, qui facilite les rencontres et les échanges. L'idée de l'iphone est née sur un parking, après une rencontre entre Steve Jobs et un scientifique français du nom de Jean-Marie Hullot. De grandes entreprises européennes se trouvent engoncées dans des organisations où marketing et bureaucratie camouflent mal une relative terreur envers la science. Les rencontres y sont devenues presque impossibles.

Il est donc temps que nos dirigeants, actuels et futurs, investissent dans les idées nouvelles, issues de la recherche, plutôt que de se résigner à acheter celles de leurs concurrents.

Ne pas publier les comptes de son entreprise, un vrai risque immatériel !

Charles Battista

Président de Place Escange, Président de la FIGEC

Déjà de plus en plus pratiquée avant la pandémie, la non-publication des comptes auprès des greffes de tribunaux de commerce et la demande de confidentialité devraient tenter plus d'un patron de TPE-PME confronté à des situations financières dégradées. Une démarche pas toujours judicieuse, notamment en ces temps troublés…

Selon un premier bilan national dressé par les greffes des tribunaux de commerce et présenté en janvier dernier, 47 % des entreprises ont opté pour la confidentialité de leur compte de résultat en 2020, contre 41% en 2019 et 36 % en 2018. Auparavant limitée aux micro-entreprises pour les comptes annuels, la possibilité de ne pas publier le compte de résultat a en effet été étendue par la loi Macron de 2015 puis la Loi Pacte aux TPE et PME. Depuis, cette autorisation est élargie aux entreprises qui remplissent deux des trois critères suivants : réaliser un chiffre d'affaires inférieur à 12 millions d'euros net, avoir moins de 50 salariés et un total bilan de moins de 6 millions d'euros pour les TPE ; réaliser un chiffre d'affaires inférieur à 40 millions d'euros net, avoir moins de 250 salariés et un total bilan de moins de 20 millions d'euros pour les PME. « Rappelons que si ces entreprises peuvent demander que leur compte de résultat ne soit pas rendu public, elles ont néanmoins l'obligation de les déposer auprès du greffe du tribunal de commerce dont elles dépendent », précise Charles Battista, Président de Place Escange. Pourtant et malgré cette obligation, les tribunaux de commerce tendent à constater une diminution des dépôts de comptes.

Mieux vaut jouer la carte de la transparence

Une opacité d'autant plus risquée aujourd'hui. En effet, le taux de défaillances des entreprises, historiquement bas, cache des difficultés qui risquent d'exploser dès lors que les dispositifs d'aide de l'état prendront fin (PGE, chômage partiel…). Dans ce contexte, ne pas publier ses comptes, même de manière confidentielle, tend à brouiller les pistes. « 60 % des entreprises qui ne publient pas leurs comptes ont des difficultés financières, constate Charles Battista. Dès lors qu'une entreprise opte pour la non-publication de ses comptes ou la confidentialité de son compte de résultat, elle laisse la porte ouverte à des suppositions parfois infondées sur sa santé financière, ce qui peut lui être préjudiciable. Aujourd'hui et au regard du contexte actuel, mieux vaut publier des mauvais comptes que ne pas le faire sous prétexte du secret des affaires ! Nous conseillons donc aux entreprises de continuer à publier leur compte afin d'éviter toute réserve de la part notamment des sociétés d'information d'entreprises, banques et assureurs crédit qui accèdent à l'ensemble de ces données. D'autre part, en les publiant, elles s'engagent également dans une démarche de transparence qui contribue à instaurer un climat de confiance entre l'entreprise et ses différents partenaires commerciaux (donneurs d'ordres, fournisseurs…). Enfin, pour se valoriser auprès de l'ensemble de cet écosystème, les sociétés ont également tout intérêt à communiquer sur la santé et la gestion de leur patrimoine immatériel (gestion des risques humains, informatiques, des données, politique RSE…) ».

Risques immatériels et communication de crise

Carole GIORGI

Associée de Gouvernance et Valeurs

La communication en situation de crise revêt une dimension stratégique pour l'entreprise. Elle reflète le bon fonctionnement de la structure et rassure les investisseurs et les parties prenantes de l'entreprise : salariés, clients, fournisseurs, partenaires de son écosystème. Mais quelle dimension doit-elle incarner ? Comment la communication en situation de crise participe à sa réputation et à la création d'un nouvel actif immatériel primordial dans la valorisation de l'entreprise ?

Lors d'une crise, une entreprise est directement impactée tant sur les plans économiques qu'humains. Les différents facteurs liés à la crise influent sur le nombre de clients, leurs prises de commandes engendrant une baisse du chiffre d'affaires, dégradant ainsi leur rapport à l'entreprise : à son image et à sa raison d'être.

Cela génère des conséquences douloureuses tant sur le plan social que sociétal qui ainsi détériorent l'image de l'entreprise et sa marque employeur : chèrement acquises au cours de ces dernières années.

La communication sous toutes ses formes peut indéniablement être qualifiée d'actif immatériel stratégique (AIS) [1], prenant ainsi toute sa part dans une logique de valorisation d'entreprise.

En effet lors d'une valorisation d'entreprise : il convient de calculer, entre autres cet Actif Immatériel Stratégique (AIS) en lien à la fois avec le capital client et le capital partenarial de l'entreprise.

Sans communication de la part de l'entreprise : la croissance du portefeuille clients, la fidélité, la satisfaction ou encore la taille du carnet de commandes en seront directement impactées. La communication devient alors un actif en soi, essentiel au maintien de l'activité économique de l'entreprise.

Montrer que le fonctionnement interne de l'entreprise n'est pas altéré par une situation de crise ou qu'il s'adapte à celle-ci témoigne de sa transparence et de sa volonté de garder un lien puissant avec les acteurs économiques, avec lesquels elle noue des liens durables.

Sa réputation devient donc un enjeu vital : son activité et son capital client en dépendent. Communiquer en situation de crise est par conséquent indispensable afin de préserver et de renforcer l'image de l'entreprise durant la crise : sans hypothéquer son avenir et assurer ainsi la pérennité des actions stratégiques initiées.

Un plan de communication de crise érige donc un risque immatériel en opportunité.

[1] A.I.S : Actif Immatériel Stratégique : Concept défini, faisant référence aux travaux de Bernard ATTALI, Stéphane BELLANGER , Jacky OUZIEL et Gilles TRIGANO – « Valoriser le capital immatériel des entreprises innovantes » – Editions RB – Mars 2020.

Valoriser les actifs immatériels d'une entreprise dans l'évaluation d'entreprises

Sébastien Laye

Entrepreneur dans le secteur immobilier en Europe et aux USA, Sébastien Laye est aussi actif dans la sphère publique. Ancien d'HEC et de l'IEP, il est aussi diplômé du MIT et en Droit.

A regarder un manuel de finance d'entreprise de près, ou pire l'évolution des Bourses, une entreprise serait valorisée uniquement sur son compte de résultat, ou, dans le meilleur des cas, ses flux de trésorerie libre. Ainsi, en théorie financière, la valorisation d'une entreprise est la valeur nette actualisée de ses flux de trésorerie libres futurs.

Mais il y a aussi une autre manière d'analyser une entreprise, moins spéculative, à l'instant T, en regardant son bilan. Le problème est que les normes comptables prennent en compte (même si elles ne les valorisent souvent pas correctement) les actifs immobilisés, les terrains, les usines, les équipements, mais moins souvent les éléments intangibles ou immatériels ; quand il s'agit d'expliquer le prix payé pour une société au-delà des actifs tangibles, on se contente d'une catégorie fourre-tout, un concept un peu éthérique, internationalement connu comme le goodwill. Les dépenses liées aux actifs immatériels ou intangibles (marques, brevets, propriété intellectuelle, recherche, savoir-faire) impactent le compte de résultat (alors que les sociétés cotées par exemple cherchent à maximiser leur résultat net) : elles ont donc un effet négatif de court terme, même si la société espère en obtenir une amélioration future de ses revenus. A l'inverse, quand on dépense pour une usine ou créer un actif matériel, on crée au bilan comptable une immobilisation qui est ensuite dépréciée par le compte de résultat : mais on augmente son bilan, ses actifs, donc sa valorisation, et l'impact sur le résultat est plus graduel.

La véritable révolution des systèmes comptables serait de traiter de manière similaire les dépenses liées à l'immatériel. Ainsi, nous imaginons qu'une société de biotech par exemple, pourrait capitaliser au bilan cinq années de recherche (qui comptablement n'ont fait que des pertes) qui seraient ainsi valorisées au bilan, et ce montant serait déprécié chaque année. Nous aurions ainsi des valeurs comptables d'actif net qui intégreraient une forme (même imparfaite) de valorisation des actifs immatériels, et nous pourrions inventer une méthodologie similaire pour tout intangible. C'est en fait cette approche qui est utilisée à l'heure actuelle par les meilleurs analystes financiers, dans les fonds d'investissement : ils doivent souvent « redresser » le bilan des sociétés dans les secteurs de la technologie ou de la biotech.

La réputation, un actif immatériel à surveiller

Didier DAVITIAN

Conseiller en communication

Chaque année au mois d'Octobre, la société Interbrand délivre son classement des valeurs financières des principales marques mondiales. Depuis 2001, cette société suisse opère son classement suivant des critères extrêmement précis et le résultat est très attendu tant par les entreprises elles-mêmes que par la communauté des spécialistes des marques. Après Coca-Cola, c'est Apple qui depuis 2013 détient la 1ère place avec une valorisation de sa marque à plus de 300 milliards de dollars.

Pour l'entreprise, l'image de marque est un enjeu essentiel à surveiller. Mener une politique d'image nécessite du temps, du professionnalisme mais permet aussi d'enregistrer un retour sur investissement rapide. Après le logo dont on sait aujourd'hui qu'il doit être le plus épuré possible, place à la stratégie de marque avec le renfort de la publicité à base de storytelling rempli d'émotions afin de capter l'attention du client. Aujourd'hui, se bâtir une politique d'image c'est obtenir un capital confiance et un capital sympathie des collaborateurs internes de l'entreprise et des publics externes (clients, fournisseurs, banques…). Décathlon et Ikea arrivent à cumuler les 2 et font partie des marques préférées des français.

Avec l'information en continue (chaînes d'infos, réseaux sociaux…), tout ce qui est bâti minutieusement en plusieurs années peut se détruire en quelques instants. Les collaborateurs internes doivent avoir un sentiment de fierté et d'adhésion aux valeurs véhiculées par la marque. Certes, le « dieselgate » a coûté plus de 2 milliards d'euros à Volkswagen (frais d'avocats, retraits de véhicules, réparations des moteurs…) mais la baisse de la productivité induite par la chute de la motivation des salariés, actif immatériel difficilement quantifiable, pèse lourdement encore sur les comptes de l'entreprise.

En situation de crise, l'entreprise doit surveiller encore davantage sa réputation car la crise imprègne le cerveau collectif pour longtemps. En 2018, Starbucks réussit magistralement à retourner très vite ses accusations de racisme en fermant tous ses cafés pour former ses salariés à la lutte contre le racisme. Aujourd'hui, dans le cadre de la crise sanitaire, les assureurs, dont AXA, abondent profondément au sein de fonds de solidarité et à l'effort collectif. Et pourtant, pris dans la tourmente des pertes d'exploitation, la compagnie d'assurance a du mal à être audible sur ses autres communications.

Construire, maintenir et surveiller son image permet de garder une cohésion interne à l'entreprise et conquérir et fidéliser les clients. Face aux fakes news, une politique de préservation de sa réputation revêt à la fois une dimension de ressources humaines, de communication interne et commerciale. A l'ère du commerce phygital où les achats se font désormais pour une plus grande partie via le digital (Amazon…), construire et préserver sa réputation devient essentiel à la vie de toute entreprise.

La gestion du risque immatériel comme bonne pratique financière

Adrien Lehman

enseignant en économie à Sciences Po et research fellow « systèmes financiers » de l'institut Open Diplomacy

Derrière les risques financiers auxquels font face les entreprises se cachent bien souvent des risques immatériels, liés à des effets de réputation, à une mauvaise connaissance du marché ou à une mauvaise gouvernance interne. Bien prendre en charge ces risques immatériels sur le long terme est ainsi la meilleure manière d'éviter de gérer dans l'urgence des risques financiers qui conduisent presque toujours à des pertes. Mieux le risque est identifié en amont et plus les conséquences financières seront raisonnables et le passage en perte limité. Ainsi, les risques financiers ne sont en quelque sortes que la matérialisation d'un risque immatériel mal pris en charge.

Les risques financiers auxquels font face les entreprises sont bien connus. Les professionnels de risques les classent en quatre grandes catégories. Le plus évident est le risque de crédit, ou de contrepartie, c'est-à-dire le risque de pertes financières liée à l'insolvabilité d'un tiers. C'est aussi tout l'enjeu de la question des délais de paiement, qui se sont rallongés avec l'actuelle crise COVID-19. Le retard moyen est désormais de 13 jours. C'est treize de trop pour la trésorerie de beaucoup de petites structures. Dans ce cas précis, on parle de risque de liquidité. Par ailleurs, les plus grandes entreprises peuvent faire face à des risques de marché, notamment si elles sont exposées à l'international. A ces risques très techniques s'ajoutent les risques opérationnels ou de fraude qui s'accroissent avec la taille de l'entreprise.

Tous ces risques peuvent paraitre bien abstraits et donc réservés au public de spécialistes des directions financières et des cabinets de conseil. On pourrait se contenter de cette situation si leurs conséquences n'étaient si grave. En effet, ils peuvent mener à la disparition pure et simple de l'entreprise. Or, derrière une question financière d'apparence complexe se cache bien souvent un risque immatériel qui peut être identifié et neutralisé à la source par un manager vigilant. Il en va notamment ainsi des problèmes de trésorerie qui peuvent être limités grâce à une meilleure analyse de la réputation des agents économiques en présence sur un marché. Dans le sens inverse, un contrôle soigneux de son image de marque limite les risques de déséquilibre du bilan lié à une chute de revenus commerciaux sans rapport avec la qualité des produits proposés. La logique est la même en matière de cybersécurité et de protection de données ou de suivi de la réglementation. De même une prise en charge rapide des mauvais payeurs par une direction du recouvrement efficace évitera bien des problèmes financiers. Une protection de long terme contre ces risques immatériels évite ainsi à une entreprise de prendre en charge des risques qu'il faut souvent régler dans l'urgence et aboutissent nécessairement à des pertes directes. Mieux prendre en compte le risque immatériel, le plus en amont possible, est donc une excellente pratique financière.

Louis-Rémy Pinault

Expert développement stratégique chez GENERALI & Membre du Comité Scientifique «Place Escange»

Prévenir le risque pandémie, premier risque immatériel pour l'entreprise en 2020

La mondialisation heureuse enterrée

Dès la fin des années 90 la mondialisation a mis en évidence les impacts négatifs de la globalisation d'une économie low cost tant sur le plan social qu'environnemental. Elle a mis en perspective la vraisemblance de menaces de crises, financières, économiques, écologiques, sociales, politiques, géopolitiques pouvant dégénérer en crises systémiques dopées par la vitesse de circulation des informations, des données, des capitaux. Mais c'est une crise sanitaire, « à l'ancienne «, qui a frappé l'ensemble de la planète rappelant que les limites des scénarii improbables pouvaient toujours être franchies. Dans un contexte de profondes transformations, La crise de la Covid-19 impacte la perception des risques au sein de la société et de l'entreprise.

Le risque en 3D

Cette crise modifie sensiblement le rapport à l'incertitude. Les entreprises intègrent, en principe, en fonction de leur propre culture des risques, ceux qualifiés d'aléatoires et accidentels. Ils sont directement liés à leur activité et leur financement est en principe transféré à leur assureur, dans le cadre des règles techniques de l'assurance. Cependant, ils se trouvent confrontés de plus en plus à des risques d'origine externe aux conséquences dommageables importantes, parfois catastrophiques, pour leur performance, leur valeur, leur avenir :

- **Crise géo-politique avec un pays étranger et embargo les privant d'un marché,**
- **Décision politique, augmentation des droits de douane,**
- **Crise sociale,**
- **Accident industriel entraînant une rupture de la supply-chain,**
- **Impact du réchauffement climatique, météo sensibilité de l'activité, catastrophes naturelles,**
- **Cybercriminalité et attaque de serveurs stratégiques,**
- **Lock out électricité,**
- **Crises systémiques, financière, sanita**ire…

Dans cet environnement complexe, face à ces menaces qui s'additionnent aux risques « classiques », risques aléatoires et ceux relevant du risque d'entreprendre, l'enjeu pour la Direction de l'entreprise est de conserver le contrôle de la situation menaçante, tant dans le dispositif d'alerte que dans le traitement de la crise et la reprise d'activité.

Résilience et capital immatériel

La crise que nous traversons montre que la résilience des entreprises qui s'adaptent le mieux à la situation, s'appuie sur la robustesse de leur capital immatériel. Elles résistent en raison de la solidité du lien de confiance qu'elles entretiennent avec leurs parties prenantes et au premier rang, les collaborateurs. Cette robustesse du capital immatériel trouve sa source à la fois dans le développement de la culture du risque, de l'Excellence Opérationnelle et celui de l'intégration de la RSE à tous les niveaux de l'entreprise, au sein de son écosystème, sur son territoire. Le pilotage du capital immatériel, dans le cadre de l'approche de la résilience de l'entreprise, offre l'avantage de décloisonner le management des risques et la RSE. En effet, en mesurant la robustesse du capital immatériel, il est possible d'évaluer les impacts positifs sur la chaîne de valeur mais aussi les vulnérabilités source de risques et de destruction de valeur.

Ainsi, le système d'information pourra être un levier essentiel par exemple pour renforcer le capital client, organisationnel… mais aussi une source de vulnérabilité dans le cadre de cyber attaque aux effets dévastateurs.

Il en sera de même de la fidélité des fournisseurs de premier et second rang dont la prestation est essentielle en matière de qualité mais aussi de conseil dans le cadre de la conception et de l'absence de traçabilité de fournitures stratégiques venant d'Asie.

La situation inédite que nous vivons va devoir conduire à augmenter la solidarité au sein des écosystèmes et en direction des parties prenantes avec pour cible une meilleure protection du capital immatériel et stimuler l'innovation. Le premier enjeu est de repenser le projet de l'entreprise dans le cadre d'une transformation continue pour intégrer les nouvelles technologies, l'impression 3D, la cobotique, la robotique, l'intelligence artificielle… tout en limitant les impacts de son activité.

L'évaluation du capital immatériel et sa prise en compte comme élément moteur de la stratégie de l'entreprise doit conduire à développer des outils de prévention spécifiques. Un capital immatériel évalué, piloté, intégré au management des risques doit permettre d'agir à la fois sur l'efficience et sur la résilience de l'entreprise.

Damien Barthélémy

Directeur général de Creditsafe France & Belux

L'information d'entreprise, actif immatériel à maintenir, à sécuriser et surtout à reconnaitre

Les actifs immatériels occupent une part croissante dans notre économie, ils représentaient 17% de la valeur des entreprises en 1975, aujourd'hui 84% (Source : Ocean Tomo). Ils se développent de façon considérable pour les entreprises numériques mais pas seulement, c'est 75% de la valeur des Entreprises du CAC 40.

Depuis plusieurs années déjà nous assistons au développement de l'Economie Immatérielle qui est basée sur la connaissance, le savoir, et où la donnée, qu'elle soit collectée ou produite par l'entreprise, ainsi que la technologie pour la sécuriser et l'exploiter occupent une place centrale – contribuant largement à la performance et la compétitivité de l'entreprise.

Sans données ou informations, la connaissance n'existe pas et il devient difficile voire compliqué (pour ne pas dire impossible ou risqué) pour les dirigeants de se construire une vision 360° des ressources de l'entreprise – Ils ne peuvent pas non plus ajuster leur plan stratégique, prendre les bonnes décisions au bon moment, valoriser à sa juste valeur leur entreprise et par conséquent, ils réduisent leurs chances d'accéder au financement – condition de survie pour de nombreuses entreprises, en particulier les petites et moyennes entreprises (PME).

Nul besoin de rappeler que la data est non seulement créatrice de valeur mais qu'elle permet aussi d'anticiper et réduire les risques pour l'entreprise notamment dans les relations d'affaires avec les Tiers : Impayés, Défaillance, Contentieux, Privilèges, Réputation, Conformité Légale, Juridique et réglementaire. C'est encore plus vrai dans le contexte si particulier de 2020 où la situation économique impose aux entreprises de repenser leur Business Model, de s'organiser, de s'équiper pour être connectées au niveau des collaborateurs mais également des parties tierces. Elles doivent impérativement au risque de mourir, s'adapter à l'économie immatérielle car selon Bercy, tous les ans en France, le poids des investissements dans l'immatériel représente 2/3 des investissements totaux, et selon la Banque Mondiale, l'économie française est immatérielle à 86%.

Pourtant la plupart des tableaux de bord, data comprise, élaborés pour piloter la performance des entreprises ignorent encore le suivi de leurs valeurs immatérielles. Et bien que la Data respecte les règles en matière de pertinence, de fiabilité, de transparence, ainsi que les Systèmes d'informations, ne sont pas reconnus donc pas comptabilisés comme investissement au bilan mais considérés comme une charge.

Et si la data en plus de son rôle opérationnel pouvait apporter une solution comptable à la sortie de crise ? Et si cette initiative complétait le dispositif d'aides financières aux entreprises et était vu comme un levier supplémentaire qui interviendrait à la clôture du bilan ?

Aujourd'hui cela pourrait faire la différence dans la relance de l'économie.

Mais il faut garder à l'esprit que ces actifs s'altèrent, perdent de leur valeur s'ils ne sont pas structurés, agrégés et maintenus. Les fournisseurs de données d'entreprise au niveau mondial tentent de démocratiser l'accès à l'information en la rendant accessible par son prix et son exploitation. Ils analysent et enrichissent les référentiels Tiers (clients, fournisseurs, partenaires…) de données à plat (financières, légales, juridiques, réglementaires) ou agrégées (scores et indicateurs). Ils réalisent une photographie à l'instant T du niveau et de la nature du risque présent dans les référentiels. Ils mettent à disposition des systèmes de Surveillance, Screening Compliance, et proposent de connecter ces données aux données clients pour une mise à jour en temps réel rendue possible par les API. Les seuls objectifs de ROI qui en découlent pour les entreprises sont la performance, le développement commercial et stratégique.

Enfin, ils aident les entreprises à maintenir, sécuriser leur capital immatériel et à construire cette vue 360° dont ont besoin les dirigeants pour surtout ne pas piloter à vue.

Le risque politique, un risque immatériel pour l'entreprise ?

Virginie Martin

Professeure, Chercheure, Politiste, sociologue. KEDGE Business SchoolSciences Po

« Mad Men » série mythique, saison 1 épisode 1 : les publicitaires de Madison Avenue savourent une à une leur réussite en tirant sur des Lucky strike et en vidant des verres de whisky. Ils sont ceux qui voient l'avenir, ceux qui savent séduire via des visuels accrocheurs, ceux qui trouvent des slogans, ceux qui croient à la consommation.

« Mad Men » une saison plus tard : les médecins commencent à alerter sur les dangers du tabac et les campagnes de publicité pour les cigarettes seront bientôt interdites. Les « mad men » perdent des marchés publicitaires et les cigarettiers, des consommateurs.

Voilà, illustré rapidement le risque politique. Un jour, la loi passe, le décret décrète et l'environnement se modifie.

Et pourtant… « l'entreprise » se voit parfois comme assez éloignée de la chose publique et politique. Les entrepreneurs, forts de leurs innovations, de leur envie de perpétuer une business family, de créer une firme à partir d'une bonne idée, ces entrepreneurs peuvent parfois négliger le risque politique.

De même, en sciences de gestion, la question politique est peu abordée, sauf chez certains auteurs qui sont dans une tradition appelée « Critical management studies » ou approche « critique et politique » tel David Courpasson en France ou Mats Alvesson et Hugh Willmott en Grande-Bretagne par exemple. Dans cette tradition académique c'est souvent la neutralité de l'économie et / ou de la gestion qui est interrogée et il est considéré ici que le politique est à tous les niveaux de l'entreprise.

Dans tous les cas, il faut considérer que l'entreprise est encastrée dans le politique ; partant, elle peut en avoir les opportunités, comme en subir les menaces.

L'environnement politique de l'organisation est donc à apprendre, à comprendre, à analyser, à anticiper. Mais cet environnement est complexe pour deux raisons majeures :

D'une part car il se déploie sur les niveaux national-local, européen et international.

D'autre part car il est mouvant, changeant au grès d'élections, de décisions, d'intérêts croisés.

Le politique est donc une partie prenante qu'on ne peut pas connaître parfaitement, et l'entreprise doit agir dans ce contexte de connaissance limitée et donc de « rationalité limitée », comme le rappelle Simon March dans ses travaux.

Le risque politique, un risque majeur

Le risque politique est d'ailleurs aujourd'hui, selon la Coface, un des risques majeurs pour l'entreprise. Un risque politique, qui se déploie d'ailleurs sur plusieurs champs, social, médiatique… nous y reviendrons.

Finalement, c'est du côté des risques non économiques que l'organisation doit aujourd'hui regarder. L'économique est une donnée nécessaire, mais totalement insuffisante.

Brexit, replis protectionnistes de la Chine ou des Etats-Unis, contexte iranien, gilets jaunes, gestion de la Covid-19, normes anti-pollution sont autant d'exemples qui rendent extrêmement tangible le risque politique.

On le voit dans cette brève énumération, il existe des risques domestiques, des externalités négatives, et enfin des risques exogènes dépendants des contextes internationaux.

Mais, les entreprises ne sont pas toutes égales face à ces divers risques politiques. Pas toutes égales au regard de leur capacité à connaître et bien maitriser ces risques et ces parties prenantes politiques. Les TPE ne sont pas dotés de service de gestion du risque, de service de veille… les très grandes entreprises, voire multinationales sont, elles, aguerries à ce type de connaissances.

De même, les plus petites entités n'ont pas souvent la possibilité de peser sur la décision politique ; les autres peuvent adopter des stratégies de lobbying et autres jeux d'influence.

Une profession bien organisée peut essayer de contrer la décision politique ; nous l'avons vu récemment en France avec les avocats sur la réforme des retraites. C'est toute une profession libérale qui s'est dressée contre cette réforme.

Le secteur de l'immobilier, quant à lui, n'a pas pu contrer la réforme de l'ISF qui a favorisé les produits financiers et pénalisé les biens immobiles via l'IFI.

Tout changement politique / électoral / gouvernemental est donc toujours un risque ou un bouleversement potentiel pour l'entreprise. C'est assez évident ; les 35 heures resteront à ce titre dans les annales.

Du côté du lobbying

Le plus souvent ce sont les très gros secteurs, représentés par de très grands groupes qui parviennent à s'imposer face aux états et à leur décision.

Les groupes de lobbyistes sont par exemple pléthores du côté de Bruxelles et tentent de maîtriser justement le risque politique, voire empêcher des décisions politiques à leur désavantage.

L'activité de lobbyiste ne cesse de croître aussi bien à Washington qu'à Bruxelles. La capitale européenne compterait plus de 50 000 lobbyistes et personnes impliquées dans ces activités. Ces lobbyistes dépensent des millions chaque année pour peser sur les décisions de l'UE. De l'industrie chimique à Google en passant par le bien nommé « Europatat », les groupes d'intérêts privés ne ménagent pas leurs efforts pour influencer et gérer le potentiel « risque » politique pour leur secteur.

Pour être efficace, les lobbystes doivent « capturer le régulateur », c'est à dire intervenir suffisamment en amont et auprès de la bonne cible au sein des fonctionnaires de la Commission européenne. Cette dernière édictant la loi, c'est à ce stade que les influences peuvent être plus efficaces afin d'amender une loi, de la diluer, de la retarder ou même de la supprimer.

On voit bien comment, dans ce cas, essayer de contenir le risque politique, contient un autre risque politique : celui d'une trop grande in-

fluence d'intérêts privés au détriment de l'intérêt général… ce qui a terme peut faire courir un risque politico-social non négligeable. L'affaire Monsanto, la 5G, les dérives environnementales… un risque politique régulé pour un secteur ou pour une entreprise, peut revenir en boomerang à terme contre ladite entreprise, via l'opinion publique par exemple.

Le risque politique ou plutôt géopolitique

N'oublions pas de même que, dans un monde ultra globalisé, le risque politique est aussi un risque géopolitique. Suite à la chute du mur de Berlin, le monde ne s'est pas apaisé ; les tensions ont juste pris d'autres formes que celle d'un affrontement entre l'Est et l'Ouest. Les printemps arabes, les soulèvements au Brésil, les zones de terrorisme en Irak, en Syrie dans le Sahel, les attentats en Tunisie, le bras de fer entre Grèce et Turquie, tous ces affrontements sont autant de risques politiques pour n'importe quelle entreprise qui veut jouer sa partition dans le monde entier ou dans une zone géographique du monde. La stratégie d'internationalisation de l'entreprise est en soi un risque. Elle peut se heurter à des volontés de repli ou de sanction commerciales comme le fait aujourd'hui l'Amérique de Donald Trump contre les pays qui osent continuer à avoir des actifs en Iran. Dans le même ordre d'idée, LVMH est en train de renoncer au rachat de Tiffany, compte tenu des possibles représailles étasuniennes.

Prévenir les risques géopolitiques demande une grande connaissance des enjeux, des gouvernants, de l'opinion publique du pays concerné. C'est un travail en amont important et c'est une actualisation incessante via des outils nécessairement diversifiés : juridiques, politiques, sociaux, économiques, diplomatiques…. et une aide aussi de l'Etat. L'Etat – français ou autre – doit accompagner ses entreprises à l'international et les protéger du mieux possible.

Le risque politique ou plutôt mediatico-sociétal

Si ce sujet nous amène classiquement à évoquer le risque géopolitique, nous ne pouvons plus aujourd'hui ne pas évoquer d'autres risques, à mon sens, contenu dans le risque politique. Il s'agit du risque sociétal et médiatique.

Prenons le cas tout récent de la mort de George Floyd aux Etats-Unis et des mouvements anti-racistes qui ont suivi, notamment avec le #BlackLivesMatter. Les opinions publiques se sont soulevées principalement en mémoire à George Floyd mettant au premier plan de l'agenda politico-sociétal-médiatique la question du racisme. Subitement, des entreprises qui n'avaient pas correctement anticipé ces mouvements de fond – au-delà du cas de G. Floyd – ont dû réagir et promettre de revoir leurs visuels. C'est le cas typique d'Uncle Bens qui, interpellé de toutes parts lors de cet épisode, décide en juin 2020 de changer ces imageries car trop stéréotypées. On peut penser que la marque aurait pu mieux anticiper ce type de mouvements et de demandes de la communauté afro-américaine et faire évoluer au fil des années ces visuels autour de Aunt Jemima et de Uncle Bens.

La question sociale ou sociétale prend de l'ampleur via l'amplificateur médiatique et devient un risque majeur pour l'entreprise.

Dans ce même cadre, certaines entreprises ont vu leur campagne de publicité réduite à néant et / ou ont dû faire face à un bad buzz pour cause de sexisme. Les images hyper stéréotypées des femmes ou hyper-sexualisées représentent aujourd'hui un coût très élevé pour la firme. La marque Le Temps Des Cerises en a fait les frais, tout comme le groupe Accor. Ce dernier avait en effet vanté les mérites d'AccordHotels Arena à grand renfort de slogans plutôt douteux : « le seul lieu où l'on peut peloter des stars sans se soucier des conséquences » ou encore « le seul lieu ou les femmes sont à vos pieds » accompagné d'un visuel montrant une tenniswoman à genou, visage enfoui dans les mains après, ce que l'on peut deviner, comme étant un point décisif. La campagne a été retirée des murs de Paris.

Le coût sociétal existe bel en bien ; même si nous pouvons rester surpris que de telles campagnes en 2020 soient encore acceptées, sachant la chaîne de décision complexe nécessaire pour adouber de telles publicités…

Pour contrer cela et éviter ce type d'erreurs, il faut compter sur les services dits RSE de l'entreprise – quand elles peuvent en avoir un – ou au moins avoir en tête les 17 Objectifs du développement Durable (ODD) de l'ONU.

Dans ces ODD de nombreux items concernent des questions sociétales telles que l'égalité entre les sexes, la réduction des inégalités, l'accès à la santé et à l'éducation. D'autres concernent des questions plus environnementales.

Aujourd'hui, aucune entreprise ne peut se risquer d'ignorer ces bombes médiatiques potentielles au niveau des opinions publiques pouvant s'embraser à tout moment.

Les risques politiques sont aussi aujourd'hui largement sociétaux, ne l'oublions pas.

Le risque politique ou socio-économique

Le risque social est à mon sens abrité au cœur du risque politique. Il concerne le climat délétère pouvant régner au sein d'une organisation ou dans son environnement.

De façon endogène il s'agit de prévenir les risques sociaux et psycho-sociaux, de veiller au bien-être des salariés (Burn-out, suicides…), d'éviter un trop fort turn-over, de ménager les équipes, de prévenir les dérives de harcèlement moral / sexuel : c'est tout le capital immatériel de l'entreprise qui doit être préservé. Ayant la main, la firme peut, peu ou prou, maitriser ces dérives éventuelles.

Mais les risques sociaux peuvent être plus exogènes et donc plus difficiles à gérer. Il s'agit du climat social qui règne dans le pays où les activités de l'entreprise sont développées. Nous pouvons penser aux manifestations au Venezuela, au Chili, en Argentine ou dans divers pays d'Amérique latine. Ces mouvements rythment la vie dans cette zone du monde, et représentent un risque politico-social quasi structurel.

Dans ces contextes, le politique, les gouvernants, les corps intermédiaires – dans les zones de type européen – ont des cartes à jouer afin que ledit pays soit vivable, sécurisé, qu'il ne soit pas traversé de grèves / manifestations toutes les semaines… le cas des gilets jaunes étant de ce point de vue, emblématique. La France n'a jamais connu dans son époque récente une telle récurrence de rassemblements et d'oppositions au système en place.

Ce qui reste étonnant c'est l'incapacité de l'exécutif, qui est – par définition – celui qui est en charge de la paix sociale, à trouver une issue à ce refrain hebdomadaire. Le pouvoir en place joue avec un risque politico-social majeur à ne pas tout mettre en place pour trouver une issue à ce bras de fer. Résignation, inexpérience du pouvoir, travail sur les opinions publiques, pourrissement de l'affrontement… ?

Ce qui est sûr, c'est que, quelle que soit la complexité des problèmes sociaux/politiques/géopolitiques/économiques, rares sont les gouvernements passés qui ont laissé le pays sous le joug de ce trouble politico-socio-économique de premier ordre. Les risques politiques majeurs qu'ont été les crises de 2008 – financière – ou celle de 2014-2015 – terroriste – ont été gérés par les pouvoirs en place. Comment croire qu'un gouvernement ne peut pas dialoguer, apaiser, trouver une issue à ce mouvement des GJ ?

On le voit le risque social ici dépasse largement ce que l'entreprise peut espérer maîtriser ; en revanche, peu d'entreprises ont pu penser de façon réaliste que ce mouvement social s'enliserait et deviendrait une antienne de la vie en France. Et là, se pose la question de la confiance à l'égard de ceux et celles qui nous gouvernent. Une confiance perdue peut aussi représenter d'autres risques politiques notamment à coup de radicalismes en tout genre…

Derrière chaque risque une opportunité ?

Nous l'aurons compris, derrière le risque politique se cachent plusieurs types de sous-risques : politico-électoral, sociétal, médiatique, géopolitique, social… tout cela peut être mis sous l'ombrelle du Politique. La complexité est à l'œuvre, c'est évident.

Mais ne nous y trompons pas, dans tout risque, une opportunité sommeille : il ne faut donc pas que l'entreprise craigne le risque, mais l'anticipe, le contrôle du mieux possible voire le retourne en sa faveur. Des entreprises comme Dove ou Renault ont saisi assez tôt l'opportunité que représente de s'adresser aux femmes de manière non sexuée /non sexiste.

De façon un peu différente, un risque politique peut mettre en fragilité un secteur, mais peut constituer une opportunité pour un autre secteur. Les normes environnementales peuvent gêner le secteur de l'automobile mais font naître d'autres possibilités pour les éoliennes, les vélos, les sites de co-voiturage de même que pour les nouvelles industries automobiles elles-mêmes…

C'est un équilibre entre menaces et opportunités que l'entreprise doit trouver. Au niveau micro, l'entreprise peut être inquiète, au niveau macro, les secteurs finissent par trouver une sorte de régulation aidée soit par les états, soit par d'autres marchés qui s'ouvrent quand d'autres se ferment…

Le risque sera néanmoins toujours atténué, amorti via l'anticipation, la diversification, la réactivité. Ces conditions peuvent en revanche mettre à mal les hommes et les femmes de l'entreprise, qui sont les amortisseurs de crises et de risques. Le risque politique pèse in fine sur des hommes et sur des femmes. Le risque politique finit par être un risque humain.

L'enjeu de demain, les Actifs Immatériels

Bernard Attali

Président du cabinet de conseil en stratégie « Gouvernance et Valeurs »

co-auteur de « Comment valoriser le capital immatériel des entreprises innovantes » Editions de la Revue Banque - Mars 2020

Les actifs immatériels sont au cœur de réflexions structurantes. Ils sont bien plus qu'une ligne à ajouter au bilan. Ils représentent la valeur cachée d'une firme. À première vue, la notion d'immatériel, d'incorporel ou d'intangible semble antinomique avec celle de mesure et d'objectivation. Mesurer les actifs immatériels et se doter ainsi d'un référentiel représente donc un enjeu de taille… d'autant plus que, selon plusieurs études récentes (Ernst & Young, Eurosearch…), 85 % de la valeur des entreprises cotées seraient constituées par des actifs immatériels.

Les actifs immatériels sont au cœur de la stratégie des entreprises : près de la moitié des groupes ou des sociétés n'appartenant pas à un groupe ont mis en place une gestion d'au moins une composante immatérielle de leur activité :

la communication publicitaire est la politique la plus fréquemment mise en œuvre ;

dans les autres domaines, la taille de l'entreprise joue un rôle plus important ;

très logiquement, les entreprises commerciales possèdent une ou plusieurs marques, alors que les entreprises industrielles déposent davantage de brevets.

Aussi l'investissement dans l'humain est plus que jamais indispensable dans une économie dénommée « économie de l'immatériel ».

Les pouvoirs publics ont pris la mesure de l'importance de la place des actifs immatériels dans nos économies contemporaines dès 2010, via un groupe de travail (1) puis sous la forme de deux rapports (2).

Le rapport Thesaurus – Bercy identifie les actifs suivants :

Le Capital Client: il recouvre la capacité à développer les flux d'affaire ; d'acquérir de nouveaux clients ; de fidéliser les clients existants.

Le Capital Humain : il intègre certes les ressources internes et externes valorisées par la masse salariale et les honoraires ; mais également les dépenses de formation ; le coût des dépenses de recrutement et d'intégration des nouveaux collaborateurs.

Le Capital Organisationnel : celui-ci se compose des 4 éléments suivants : la culture d'entreprise ; le leadership, le travail d'équipe ; l'alignement entre l'atteinte des objectifs, les récompenses individuelles ou collectives accordées.

Le Capital des Systèmes d'Information : c'est à dire la capacité pour une organisation de disposer d'informations ; fiables, utiles et pertinentes.

Le Capital de Savoir : il s'agit de valoriser et de rendre visible le capital des connaissances (Knowledge Management) dont bénéficie l'entreprise. Il se traduit pour l'entreprise par la détention de brevets, de « secrets de fabrication »….

Le Capital de Marques : il est la résultante de plusieurs facteurs tels que : notoriété , fidélité, logo, image, réputation et signaux sociaux qui concourent à « l'image de marque ».

Le Capital Actionnariat : il permet d'extérioriser la confiance des investisseurs qui ont fait confiance à la firme.

Le Capital Partenariat : il s'agit de valoriser la capacité de l'entreprise à nouer des alliances et de constituer avec ses partenaires un écosystème propice à l'innovation.

Le Capital Sociétal : il mesure la qualité des relations et l'impact de l'entreprise avec les « parties prenantes ».

Le Capital Naturel : il rassemble ce qui a trait à l'environnement et à l'impact de l'entreprise sur son environnement.

Le capital immatériel peut représenter jusqu'à 85 % des actifs des Sociétés inter-

venant dans le champ de l'Economie Numérique. Investir dans le capital humain, et plus particulièrement dans les domaines de la formation, du Knowledge Management, dans la mise en valeur des « Soft Skills » dans les pratiques managériales, dans le partage d'une intelligence collective au sein de l'entreprise sera un vecteur privilégié de croissance dans la nouvelle Economie Numérique

La publicité fait exister et valorise des marques. Selon Maurice Lévy (ex-PDG de Publicis), elle est l'art, à la fois de dématérialiser la matière en la transformant en idée, en impression, en référence et de matérialiser l'immatériel en faisant de cette idée, de cette impression, la source directe d'un revenu.

La valeur comptable : indice de mesure ?

Dès octobre 1993, Rich Karlgaard, rédacteur en chef de Forbes ASAP, déclarait dans un éditorial : « En tant qu'indice, la valeur comptable est définitivement morte, ce reliquat de l'ère industrielle. Nous vivons à l'âge de l'information, bien sûr (…). Ne pas comprendre le peu de pertinence qu'a aujourd'hui la valeur de l'entreprise – et les actifs qui la déterminent – en est la preuve. Ce sont l'intelligence humaine et les ressources immatérielles qui constituent aujourd'hui les actifs les facteurs plus précieux de toute entreprise. L'économiste qui voudra proposer une meilleure mesure de la valeur d'une entreprise devra prendre en compte ces nouveaux actifs incorporels si importants aujourd'hui… [À ce jour], l'étalon de mesure nécessaire pour apprécier cette nouvelle source de richesse fait cruellement défaut »

Aussi valoriser le capital immatériel c'est apprécier la valeur d'actifs qui ne sont pas représentés de manière apparente et visible dans les états financiers.

Malheureusement les dirigeants d'entreprise appréhendent difficilement ce « trésor caché » et les Investisseurs et Institutions financières se fondant principalement sur les états financiers, les minore dans leur appréciation de la valeur des entreprises.

Ainsi les méthodes d'évaluation classique sont difficilement applicables aux entreprises innovantes.

Or la valeur d'une Start up ne repose-t-elle pas essentiellement sur son Capital Humain et son Capital Savoir ?

La qualité de la politique et de la démarche RSE ne repose-t-elle pas sur ses actifs immatériels ?

Les référentiels comptables traditionnels ne prennent pas par exemple en compte ce que les économistes dénomment « externalités positives » et qui constituent les fondements du Capital Sociétal et du Capital Immatériel.

Aussi la question des méthodes d'évaluation des actifs immatériels dépasse très largement le champ de la technique comptable.

Aussi la prise en compte des actifs immatériels est pour les entreprises et ses dirigeants un impératif stratégique et pour l'Etat un enjeu de politique publique.

****

(1) Un groupe de travail Thesaurus – Bercy a été initié en 2010 sous l'impulsion de Madame Christine Lagarde Ministre de l 'Economie et des Finances.

(2) Les conclusions se présentent sous la forme de deux rapports : Thesaurus V1 publié le 7 Octobre 2011 et Thesaurus V2 publié le 15 Octobre 2015

Numa Rengot

Avocat associé Cabinet Franklin & Jean Dizabeau, Juriste stagiaire Cabinet Franklin

Gestion du risque de faillite et confiance dans l'entreprise

La confiance est un élément clé de la pérennité d'une entreprise. Dans un environnement économique concurrentiel et parfois très instable, une entreprise ne peut pas survivre sans la confiance que lui accordent ses interlocuteurs et ce, à tous les niveaux.

A cet égard, on ne saurait rappeler la nécessité d'obtenir des garanties suffisantes de confiance de la part des financeurs mais également de ceux qui font vivre l'entreprise.

Alors, les choix de gestion des dirigeants doivent être orientés vers un objectif de maintien et d'amélioration de cette confiance en l'entreprise.

La confiance des parties prenantes dans l'entreprise est ainsi une composante essentielle du capital immatériel de ces dernières.

Or, le choix de se protéger des risques de faillite par le biais des procédures collectives peut fragiliser cette confiance de certains des partenaires de l'entreprise. Qu'ils soient banquiers, fournisseurs, clients voire collaborateurs, l'ouverture d'une procédure collective peut les faire douter de la viabilité du projet social et de ce fait remettre en cause la confiance dont l'entreprise a besoin pour avancer.

En appréciation des difficultés que les entreprises peuvent rencontrer, le choix de recourir à une procédure collective peut néanmoins constituer une décision adéquate.

La passivité d'un dirigeant face au risque de faillite ne saurait être pardonnée du seul fait de la crainte d'une baisse de confiance envers l'entreprise et peut s'apparenter à une faute de gestion.

Juridiquement, le risque est un événement dommageable dont la survenance est incertaine, quant à sa réalisation ou à la date de sa réalisation. Si le risque est un concept qui ne mérite d'appréciation positive que dans sa non-réalisation, le risque de faillite n'échappe pas à la règle et doit être constamment anticipé.

L'acceptation des difficultés de l'entreprise et leur anticipation par l'usage des procédures collectives demeurent donc primordiales face au risque de faillite. Une conciliation avec la confiance des parties prenantes et des collaborateurs doit aussi être pensée.

| Le cas de la reprise de l'entreprise par son dirigeant dans le cadre d'un plan de cession

Lorsqu'une entreprise ne peut plus prétendre au bénéfice d'une procédure amiable, anticipatrice du risque, et qu'un plan de sauvegarde ou de redressement n'est plus crédible, un plan de cession permet d'envisager le sauvetage de l'activité.

La cession judiciaire obéit alors à une triple finalité : le maintien d'activités susceptibles d'exploitation autonome, la préservation de l'emploi et l'apurement du passif. Ce sont ces trois éléments qui motivent l'appréciation du bien fondé d'un tel plan.

Toutefois, le législateur a fait le choix d'ajouter un critère organique dans la recevabilité d'un plan de cession. L'article L. 642-3 du Code de commerce interdit au dirigeant de droit (mais aussi de fait) d'une société en procédure collective de présenter une offre de reprise de tout ou partie des actifs de sa société. Le dirigeant se voit par ailleurs interdire d'acquérir, dans les cinq années suivant la cession, tout ou partie des biens compris dans la cession.

Pourquoi le Covid-19 signe la fin de l'hyperspécialisation et réduit les conséquences du risque immatériel pour l'entreprise ?

Paola Fabiani

Présidente-fondatrice de Wisecom, Présidente du Comex40 du MEDEF, élue à la CCI de Paris

La crise sanitaire et ses répercussions économiques vont nécessairement engendrer une transformation dans les rapports commerciaux et de façon générale dans l'entreprise. S'il ne s'agit pas d'une révolution copernicienne ou de l'avènement d'un quelconque « monde d'après », force est de reconnaître cependant que certaines certitudes qui prévalaient il y a encore quelques mois se délitent face aux réalités économiques.

Parmi elles, la théorie ricardienne des avantages comparatifs, selon laquelle chaque pays a intérêt à se spécialiser dans la production des biens pour lesquels son avantage comparatif est le plus élevé, c'est-à-dire dont les coûts relatifs sont les plus bas. Si la seconde partie du XXème siècle a vu le développement de nombreux pays grâce à un modèle de croissance basé en premier lieu sur l'hyperspécialisation, la dépendance des entreprises – tant en termes d'approvisionnements que de débouchés – mais aussi leur spécialisation en termes d'offres de biens et services, placent aujourd'hui la plupart d'entre elles dans une zone de turbulence.

Ce constat est d'autant plus vérifiable à la lumière de la crise économique que nous traversons. L'exemple de l'industrie médicale européenne qui a subi de plein fouet le confinement chinois du fait de sa dépendance aux importations est ici un cas éloquent qui n'est pas sans rappeler plusieurs précédents. En 2011, suite au tremblement de terre et au tsunami qui avaient frappé le Japon, c'est tout le secteur automobile mondial qui avait été impacté, entraînant une chute de la production internationale. Cette rigidité des chaînes de valeur mondiales relève l'exposition des entreprises à des perturbations exogènes et met en lumière les conséquences indirectes induites par cette situation.

Ceci est d'autant plus vrai que la logique d'enfermement partiel conduit inévitablement à une plus forte exposition aux risques immatériels. Outre le risque sanitaire ou environnemental, l'entreprise centrée sur son cœur de métier s'expose plus facilement aux déstabilisations que peuvent engendrer plusieurs facteurs extérieurs comme un changement de réglementation, une cyberattaque ou encore une fuite des talents difficilement remplaçables du fait de leur spécialisation dans un savoir-faire particulier.

A contrario, la diversification maîtrisée facilite la répartition des risques eu égard aux activités exercées, une maîtrise des coûts et naturellement une augmentation sensible du chiffre d'affaires.

Lorsque David Ricardo rédige au début du XIXème siècle ses Principes de l'économie politique et de l'impôt, l'environnement géopolitique, économique et social est à la fois beaucoup moins riche et complexe qu'aujourd'hui. Pour autant, l'accélération des crises, qu'elles soient économiques, sanitaires, écologiques, géopolitiques ou numériques, engendre une complexité obligeant les entreprises à mieux les anticiper et de ce fait, à devenir plus agiles, plus flexibles, et par conséquent, à s'orienter vers une diversification de leurs ressources et de leurs débouchés.

Deux leviers sont ici particulièrement probants pour éclairer la façon dont la diversification permet d'éviter les risques immatériels : une trop grande dépendance à l'extérieur, notamment en ce qui concerne la possession ou la gestion de ses données, et la concentration dans un domaine d'activité étroitement lié à une réglementation et/ou une législation susceptible d'évoluer de façon négative pour l'entreprise concernée.

En effet, la place stratégique des GAFA, dans toutes les technologies et infrastructures digitales utilisées par nos entreprises, les rend aujourd'hui quasi-incontournables pour notre économie nationale. A titre d'exemple, Facebook et Google se partageaient en 2019 51,3 % du marché mondial de la publicité en ligne.

En mars 2018, l'agence indépendante My Media lançait le « Search Dependence Index » (SDI), un indice qui permet de mesurer la dépendance des sites internet aux moteurs de recherche, et, en particulier, à Google. En France, Blablacar.fr est l'un des 2 sites internet notés comme le moins dépendant des recherches via le moteur de Google, avec un score de 1,5/100. Pour mémoire, une note de 1 signifie que le site évalué est proche d'une « autonomie totale » tandis que la note 100 traduit une « dépendance totale » à Google dans l'acquisition de son trafic.

La très bonne note de Blablacar s'explique par sa place de pionner sur le marché, puisque le site – initialement baptisé covoiturage.fr – a été la première plateforme de mise en relation entre covoitureurs. Elle témoigne également d'une forte affinité des internautes à l'égard d'une marque dont le développement de sa notoriété différemment a permis de s'affranchir d'une dépendance au GAFA. Et développer ses services avec une application plus qu'un moteur de recherche. Avec plus de dix millions de membres, une croissance de 200% par an et 95% de parts de marché selon les statistiques données par le site, Blablacar est donc l'acteur français positionné sur le secteur des mobilités avec le plus faible SDI. A

titre de comparaison, le score moyen pour les entreprises du secteur est de 23. A titre de point de comparaison, une note qui est largement meilleure que celle attribuée à nos médias nationaux puisque l'indice moyen de la presse quotidienne française s'élève à 42. Seul L'Equipe, dont le contenu sportif est associé à une réelle expertise particulière, obtient un indice sensiblement inférieur (15).

Autre point soulignant la « GAFA dépendance » des entreprises françaises, les géants du web hébergent aujourd'hui la vaste majorité de leurs sites internet via les GAFA. Amazon Web Services (AWS), la solution de « cloud computing » de la firme de Seattle, est la plus utilisée dans le monde, et possédait presque 40 % des parts du marché mondial mi-2018, selon Synergy Research Group. Or, si les géants de la tech détiennent d'énormes quantités de données, y compris des entreprises françaises, l'adage selon lequel « de grands pouvoirs impliquent de grandes responsabilités » n'a jamais autant été d'actualité. Cette concentration du marché et de l'infrastructure d'Internet entre les mains d'un nombre réduit de leader mondiaux fait en effet naître de nombreuses inquiétudes et commande une réflexion sur le pouvoir de ces entreprises vis-à-vis des économies de chaque pays.

Si la crise sanitaire et économique actuelle doit engendrer une réflexion quant à la nécessaire diversification des chaînes d'approvisionnement et des offres de l'entreprise, ces dernières ne peuvent, dans le même temps, faire l'économie d'une réflexion quant à la gestion de leurs données. Comme le relève Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), il est urgent de « favoriser l'éclosion d'un écosystème français susceptible de protéger efficacement les entreprises privées et de nous consacrer à la protection des acteurs sensibles pour garantir leur indépendance et, de facto, préserver notre souveraineté dans le monde virtuel ».

Le risque de dépendance technologique revêtant dans les domaines particulièrement sensibles, une dimension vitale.

Les données constituent le (nouveau ?) capital de nos industries et relèvent d'enjeux économiques majeurs. Utilisées sans consentement, elles deviennent des armes en termes d'intelligence économique susceptibles d'avoir des impacts stratégiques majeurs pour nos entreprises.

C'est d'ailleurs cette prise de conscience de la nécessaire protection des données qui a engendré l'avènement de la Réglementation générale de protection des données (RGPD) au niveau européen.

Ainsi selon un sondage OpinionWay en date du mois de mai 2018, 8 Français sur 10 indiquent être prêts à boycotter une entreprise qui ne respecterait pas le RGPD et porterait atteinte à leur vie privée. A travers cette analyse, on prend la mesure des nouvelles attentes des consommateurs et des enjeux que portent la donnée et son traitement.

Ce qui nous amène à notre second levier qui est l'évolution de la réglementation. Ce changement a en effet un impact conséquent pour les entreprises utilisant massivement les outils de communication digitale, impliquant pour elles des transformations dans leur façon de travailler tout en engendrant des coûts importants.

Ce constat est d'autant plus vrai que la nouvelle réglementation européenne contraint désormais les entreprises et leurs prestataires à démontrer que le destinataire d'une campagne d'emailing par exemple, a bien donné son consentement. Une obligation rétroactive qui implique que les données collectées avant l'application du RGPD ne pourront être utilisées que si l'utilisateur se montre favorable pour être destinataire de la campagne. Pour pouvoir utiliser des données personnelles de clients, les entreprises doivent ainsi mettre en œuvre des dispositifs permettant d'obtenir leur consentement explicite.

Ainsi les entreprises n'ayant pas ou peu diversifié leur stratégie d'acquisition, se sont vues fortement impactées par cette nouvelle réglementation, parfois même au regard de concurrents d'autres continents ne disposant pas de cette réglementation dans une économie mondiale.

En diversifiant les stratégies, les biens ou prestations commercialisés et même les zones de distribution, ces effets sont moindres grâce à une meilleure possibilité de rebond face aux changements. A ce sujet, l'exemple des jardineries durant la période de confinement est intéressant. Imposées de fermer administrativement alors que débutait le printemps, une période clé pour la réalisation leur chiffre d'affaires annuel, elles ont réussi à rester ouvertes en vendant de la nourriture animale, un produit de première nécessité. Ne pas fermer était un impératif pour que le client le constate de visu lorsqu'il sortait de son domicile. Ou via Internet. Et revienne début avril quand l'autorisation d'ouvrir pour vendre des semences potagères a été possible. Et derrière des fleurs, arbres etc… toutes ne sauveront pas leur saison, mais elle ont limité la casse.

On ne reviendra pas sur l'uberisation de différents secteurs d'activités souvent à l'origine, précédé ou accompagné de changement de réglementation mettant de ce fait en cause de nombreux modèles souverains.

Dans cette même logique, le décret de « patriotisme économique », permettant à l'Etat de bloquer le rachat d'entreprises françaises par des investisseurs étrangers, est un exemple éloquent sur la façon dont la réglementation peut protéger les secteurs stratégiques nationaux. Concrètement, ce décret vise à élargir à cinq nouveaux secteurs le décret, adopté le 30 décembre 2005 par Dominique de Villepin, qui soumet un certain nombre d'investissements étrangers en France à l'autorisation du Gouvernement. Ceux-ci concernent l'approvisionnement en électricité, gaz, hydrocarbures ou autre source énergétique, à l'exploitation des réseaux et des services de transport, à l'approvisionnement en eau, aux communications électroniques et à la protection de la santé publique.

Publié consécutivement à la révélation des négociations entamées par l'américain General Electric pour racheter les activités énergie d'Alstom, ce texte a pour vocation de protéger les entreprises stratégiques nationales contre des formes indésirables de dépeçage et des risques de disparition. Il s'agissait alors de rééquilibrer le rapport de force entre les intérêts des entreprises multinationales et les intérêts des États.

Dans la mesure où notre avenir économique et notre souveraineté passera dans les années à venir par la défense des intérêts de l'Union européenne (UE) sur la scène internationale, la mise en place d'un « Buy European Act » – sur le même modèle que le Patriot Act américain – visant à protéger le tissu économique et industriel européen et à valoriser la production continentale dans les marchés publics, pourrait avoir du sens. Il s'agirait de réserver l'accès aux marchés publics européens aux entreprises dont les produits sont confectionnés à 50% sur le continent, avec des exceptions envisageables pour certaines gammes de produits ou technologies. L'ensemble de ces mesures pourrait être mise en place de façon parallèle au mécanisme financier européen voté en 1996. Ce dernier aurait pour objectif de contrer l'extraterritorialité américaine à travers une aide au financement des PME souhaitant contourner le FCPA. Les entreprises travaillant dans le secteur de l'environnement, de l'aménagement urbain, des infrastructures ou des transports, bénéficieraient ainsi de subventions en cas d'atteintes graves à leurs intérêts.

La mutation, et l'agilité à se transformer, à se diversifier, apparaissent donc bien comme un prérequis nécessaire à toute prévention de risque immatériel. En étant contraintes de suivre ces préceptes depuis le début de la crise liée au covid-19, les entreprises réduisent dans le même temps leur exposition aux risques immatériels. Face à l'accélération des crises, leur capacité à offrir une large gamme de produits, de prestations et donc des typologies de clients – que ce soit au niveau social ou au niveau territorial – ainsi que des zones d'approvisionnement et de commercialisation, doit renforcer la sécurisation de leur business.

Nicolas Arpagian

VP Stratégie et Affaires publiques, Orange Cyberdefense

Au-delà des systèmes d'information, la cybersécurité doit prendre en compte le capital immatériel des entreprises

Avant de se concrétiser par la fabrication de nouveaux produits ou la commercialisation de nouveaux services, la chaine industrielle a été précédée de nombreux échanges numériques entre les bureaux d'études, les équipes commerciales, les juristes, la direction financière, et le réseau de partenaires. Sans oublier l'implication de la direction générale. Les flux de données qui ont été générés, ont circulé et été régulièrement enrichis par les contributions successives de toutes les parties prenantes.

A ce stade, la question de la confidentialité et de l'intégrité des informations ainsi partagées est cruciale. Les décisions prises, les investissements envisagés et les ruptures technologiques proposées ne le sont précisément que parce que chaque contributeur a confiance dans la protection de cet actif immatériel à fort potentiel en cours d'élaboration. C'est la combinaison de la sécurisation juridique des informations et leur inaccessibilité à des tiers non autorisés qui donne confiance aux co-auteurs. Il est donc primordial que les équipes en charge de la cybersécurité conçoivent leur choix techniques en adéquation avec les métiers qui utiliseront ensuite les systèmes d'information. Cette co-construction en amont fera en sorte que les outils finalement choisis pour sécuriser le dispositif seront effectivement utilisés au-delà de la seule communauté des experts ès-informatique.

De leur côté les juristes et les communicants auront intérêt à intégrer cette exigence de protection des actifs numériques : profils suspects sur les réseaux sociaux, supervision des éventuels sites Internet parasites, repérage de campagnes de dénigrement en ligne, fraudes à l'identité, usages abusifs des attributs de la marque, ou du nom de ses dirigeants… Cette dimension sociale, qui mêle les obligations légales aux enjeux de communication, est désormais au cœur des stratégies de cyberattaques conduites par des pirates qui utilisent toutes les fonctionnalités de la société de l'information. Celle-ci s'appuie sur des infrastructures techniques qui doivent demeurer opérationnelles et également sur un patrimoine immatériel qui – si il n'est pas préservé – peut affecter gravement la réputation, l'activité, les ventes et donc les résultats financiers de la plus établie des sociétés commerciales. C'est aussi le rôle des équipes de supervision d'un CERT (Computer Emergency Reponse Team) d'effectuer cette veille dans le maximum d'environnements possibles (réseaux sociaux, Internet sombre…) en détectant les usages malveillants qui sont faits des actifs immatériels. Cela concerne également les fuites de données avec le repérage d'éventuels documents internes qui seraient accessibles en ligne ou sur des plateformes d'échanges.

L'intensification numérique des organisations s'accélère dans une période où le travail à distance et les interactions avec des partenaires disséminés sur la planète se systématisent. Outre les sécurisations des connexions et des équipements, il convient donc d'investir le champ de la protection des informations stratégiques. Une occasion supplémentaire d'accroître la collaboration entre les différentes équipes de l'entreprise : les métiers, les fonctions support et l'IT. Une hybridation des activités à l'image des approches transverses qui caractérisent désormais les organisations les plus efficaces.

Renforcer la résilience face aux risques immatériels dans le domaine de la transition écologique

Antoine-Tristan Mocilnikar

Ingénieur général des mines au Service du Haut fonctionnaire de défense et de sécurité

Les questions écologiques ont progressivement été intégrées d'une manière ou d'une autre par toutes les parties de la société. Elles ont constamment représenté autant de défis que d'opportunités. Les aléas climatiques apportent une dimension très nette de crise avec ce qu'elle comporte de préventions, de gestion de crise et d'actions post-crise. Le risque immatériel induit croit donc à mesure de cette prise en compte. Nous l'illustrons par trois moment clés : la décennie 1970, 2007 et nos jours.

La très forte croissance d'après-guerre avait vu apparaître des alertes comme celle exprimée par le club de Rome qui avait financé le rapport Meadows publié en 1972 et intitulé les limites à la croissance. Des mouvements politiques ou associatifs prenaient corps et existent toujours et se renforcent. Des conférences internationales se multiplient et déclinent les concepts et les ambitions. En même temps, la commission sociale du CNPF rejetait sèchement la volonté du Centre des Jeunes Dirigeants (CJD) de définir une notion nouvelle : l'« entreprise citoyenne ».

L'année 2007, marque un tournant dans la prise de conscience. Jacques Chirac nous alerte : « la planète brûle ». Les médias s'emparent définitivement et fortement du sujet. Puis à leur tour, les politiques de tous les bords, non les seuls spécialisés, s'engagent sur des actions fortes. La plupart des candidats à la présidentielle de 2007 signeront le Pacte écologique de Nicolas Hulot.

Dans le cadre du Grenelle de l'environnement qui suit l'élection, les pouvoirs publics, les associations, les experts et les entreprises décident ensemble de centaines de mesures environnementales sur un champ très vaste dans une culture du développement durable. Cette culture très positive, tout à fait à l'opposé de l'écologie punitive, cherche à ne pas opposer croissance et environnement, écologie et développement social. Au-delà des mesures sectorielles décidées et très substantielles, le cadre général, pour les entreprises, est la notion de responsabilité sociale des entreprises, la RSE, qui sort fortement renforcé. Les entreprises et plus généralement les acteurs ont compris que les lignes avaient bougés.

Depuis, les entreprises ont progressé considérablement. De nombreuses mesures les concernent toutes directement ou indirectement : recyclage, écoconception, ISO 14001, Taxonomie verte, compensation carbone. Dans le cadre de la RSE, encore renforcé en 2019 par la loi Pacte (Plan d'Action pour la Croissance et la Transformation des Entreprises), le « comment » et le « avec qui » pèse autant que le « quoi ». L'exercice de transparence extra-financière s'est renforcé. Toutes les parties concernées savent l'essentiel de l'action des acteurs économiques.

En parallèle, hélas et presque paradoxalement, la situation politique autour de la transition écologique s'est plutôt dégradée ou au minimum s'est complexifiée. D'un côté, tous les partis politiques ont des propositions, des projets, des actions locales très concrètes concernant l'environnement. Mais de l'autre, des extrémistes politiques discréditent certaines actions aussi bien dans l'arène politique traditionnelle que dans le cadre contestataire. Par ailleurs, les questions d'acceptabilité sociale ont pris une dimension accrue du fait de la montée en puissance des effets économiques et sociaux des politiques environnementales. Une trop faible prise en compte de l'acceptabilité fait rejeter par une partie de la population des mesures. C'est le cas de la fiscalité environnementale par les bonnets rouges puis les gilets jaunes.

Un autre phénomène a pris une ampleur particulière ; ce sont les dynamiques directes de consommateurs et de citoyens. Elles prennent des formes diverses. On peut penser au comparateur de qualité de nourriture Yuka, aux différents labels Bio, Max Havelaar pour le commerce équitable. On peut penser aux associations intéressés par le climat qui vérifie les affirmations de neutralité carbone des entreprises.

Une affirmation imprudemment émise peut-être qualifié de greenwashing. Il existe des « guides anti greenwashing », des « manuels pour déceler le vert du faux ». Un calcul trop simpliste sur son bilan carbone peut valoir une polémique. Une politique de gestion de déchet d'une entreprise peut être un sujet de débat et une cause d'appel à boycott. Ce sont autant des risques immatériels pour l'ensemble des acteurs. Ils peuvent, en outre, présenter des effets dominos. Un problème d'abord localisé peut ensuite migrer dans la chaîne de la valeur ou dans la société.

A plus long terme, le pivotement des organisations internationales, des institutions, des états, des collectivités locales vers la transition écologique constitue autant de risques immatériels très réels pour ceux qui n'anticipent pas ces changements. Prenons quatre exemples. En décembre 2019, un accord a été conclu entre le Parlement européen et le Conseil sur la création de la toute première « liste verte » du monde — un système de classification des activités économiques durables ou taxonomie. Cela contribuera à renforcer les investissements publics et privés pour financer la transition vers une économie verte et neutre pour le climat, en réorientant les capitaux vers des activités économiques et des projets réellement durables. Rater ce train peut être une tragédie pour de nombreux secteurs. C'est d'autant plus dommageable que des mesures d'accompagnement existent.

Autre exemple, « Un euro sur deux du budget de l'Ile-de-France sera dédié à l'écologie ». « Plutôt que d'interdire et de contraindre, on veut faciliter et inciter les comportements écologiques », argue le vice-président en charge de l'écologie et du développement durable du conseil régional d'Ile-de-France. Ce sont de réelles évolutions globales. Deux derniers exemples : 30 milliards d'euros dans le plan de relance d'un montant de 100 concernent la transition écologique. Finalement, notons que les propositions intitulée COVID-19: La Grande Réinitialisation, du World Economic Forum, qui organise Davos, place l'environnement au centre du village : « Une seule voie nous mènera vers un monde meilleur : plus inclusif, plus équitable et plus respectueux de Mère Nature. »

Le sujet de risque immatériel existe donc sur plusieurs angles. Le premier concerne la protection de sa réputation : il est devenu impossible de ne pas se positionner par rapport à la transition écologique. Le deuxième est lié à la très vaste complexité induite par le cadre des politiques publiques environnementales. Ce sont autant de risque de non-conformité. Le troisième est lié aux ressources humaines : la génération qui vient est attirée par les valeurs de l'entreprise. Pour attirer les talents et les garder, dans un monde concurrentiel, il faut donc évoluer pour séduire les jeunes et leur montrer que l'entreprise défend leurs valeurs. La dernière raison, moins tangible, vise à créer une valeur partagée. Autrement dit, l'entreprise, qui existe dans une société et un écosystème, peut difficilement éviter les évolutions structurelles. Cela limiterait sa prospérité.

Charles Battista

Président de Place Escange, Président de la FIGEC

Le risque immatériel aujourd'hui ?

Depuis 15 ans, on s'intéresse davantage à l'économie immatérielle grâce à l'intrusion croissante du numérique et d'internet chez les particuliers, comme dans les entreprises. Actuellement, ce sont ces GAFA qui gouvernent notre quotidien grâce à leurs moyens techniques surpuissants mais aussi par l'idéologie qu'ils véhiculent : abolition des frontières, facilité et rapidité d'action…

Aujourd'hui l'économie immatérielle s'est étoffée et revêt plusieurs dimensions : les flux financiers internationaux, la e-réputation, la e-sécurité de l'entreprise, le e-commerce, la responsabilité sociétale, l'environnement, l'éthique…

Mais la crise sanitaire de la COVID-19 a transformé les risques immatériels maîtrisés en des risques mortels pour l'entreprise : les risques de santé sur lequel notre think-tank travaille actuellement, les rallongements des délais de paiement, l'augmentation des créances impayées qui points de tension que la FIGEC (Fédération Nationale de l'Information d'Entreprise, de la Gestion des Créances et de l'Enquête Civile) porte devant les institutions publiques et privées pour les sensibiliser sur l'enjeu vital qu'ils représentent pour les relations interentreprises.

La FIGEC est l'Organisation Professionnelle qui rassemble les entreprises – start-up, PME, ETI, filiales de banques, grands groupes – de la gestion du risque client, au service de l'économie française. Les entreprises membres de la FIGEC travaillent quotidiennement pour sécuriser les 672 milliards d'euros de crédit interentreprises, diminuer les 56 milliards d'euros de perte pour créances impayées et préserver les 300 000 emplois menacés chaque année. Ainsi, face à la dégradation accélérée de la trésorerie des entreprises, ces dernières doivent mettre de côté leurs intérêts propres pour instaurer un échange d'expérience décloisonné, un partage généralisé des bonnes pratiques et une réflexion commune entre toutes les parties prenantes de l'économie française. Les adhérents de la FIGEC, sont avant tout de véritables médiateurs financiers dont l'objectif principal est de rapprocher créanciers et débiteurs.

De nos jours 80% du risque d'entreprise est immatériel. C'est parce que l'entreprise a évolué que ses risques ont changé. Que ce soit par la place croissante d'internet, du pillage des données et de la data, de la digitalisation, de l'instauration du télétravail au risque santé… l'entreprise est soumise à des risques qu'elle ne connaissait pas il y a 5 ans à peine.

C'est tout le travail de Place ESCANGE de diagnostiquer ces risques, de les mettre en valeur, puis d'y apporter les solutions par les meilleurs experts (professeurs, praticiens, membres d'administration publique…) sous forme de publications, de notes et d'événements à venir.

Avec cette crise de la Covid-19, typiquement la crise immatérielle la plus terrible de notre histoire, nos économies devront être repensées ou repansées à l'aune de l'immatériel. Ce qui pouvait être considéré comme accessoire il y a 10 ans devient primordial aujourd'hui. C'est pourquoi assureurs, prospectivistes, experts santé… planchent sur ces sujets afin d'éclairer les décideurs pour qu'une seconde crise immatérielle puisse au moins être anticipé.

Place ESCANGE doit ainsi devenir un lanceur d'alertes au profit des entreprises !

Jean-Michel Aspro

Président Ascent France

Les actifs immatériels au service de la performance de l'entreprise

Les actifs immatériels d'une entreprise représentent les actifs qui ne sont ni financiers, ni matériels. Souvent exclus du bilan, ils sont pourtant créateurs de valeur et constituent un levier de compétitivité, notamment pour les PME. Le b.a.-ba dans cet article.

| Appréhender l'immatériel

Dès 2006, Alan Fustec (R 82, GoodwillManagement), développe le sujet dans son ouvrage « Valoriser le capital immatériel ». Il décrit alors 4 groupes d'actifs immatériels qui représentent jusqu'aux 2/3 de la valeur d'une PME : humain, clients, produits, organisation. Le concept évolue et en 2013, la Direction Générale des Entreprises élabore un thésaurus proposant une approche de valorisation de 10 actifs immatériels : client (richesse, satisfaction), humain (savoir-faire des salariés), organisation (écosystème de management), système d'information (sécurité, robustesse, efficacité), savoir & brevets (avantage concurrentiel, activités R&D), marques (notoriété, réputation, protection), partenaires (fournisseurs, alliés commerciaux), actionnaires, sociétal (bassin d'emplois, infrastructures) et naturel (environnement physique). Ce thésaurus définit pour chaque actif ses critères et indicateurs de mesure de performance. Il propose également une évaluation. La solution web AddValue® d'ASCENT France capitalise sur ce modèle et l'enrichit de l'analyse des actifs marchés, produits & services, gouvernance et dirigeant.

| Pourquoi les actifs immatériels sont-ils si importants ?

Les bilans comptables mesurent les richesses accumulées mais passent sous silence des sujets essentiels au processus de création de valeur : sans collaborateurs, sans clients, l'entreprise meurt. L'immatériel décrit tout ce qui contribue à la singularité de l'organisation. Différenciants, expérientiels, pérennes, les actifs immatériels interagissent entre eux et conditionnent l'avenir de l'entreprise. Pour le dirigeant, ils constituent un tableau de bord utile au management et à l'amélioration de la performance, en complément des indicateurs financiers. Pour les assureurs et les banquiers, ils permettent de mesurer plus finement les risques opérationnels. Dès lors, ils deviennent stratégiques.

Dans quels contextes ?

> **Transmission**

> **Entrée d'associés**

> **Recherche de financements**

> **Fusion**

> **Redressement**

> **Cession ou reprise**

David Gruson

Ethik-IA Directeur Programme Santé JouveChaire Santé ScPo Paris

Intelligence artificielle en santé et risques immatériels éthiques

La gestion de crise COVID-19 a marqué un tournant majeur d'accélération de la transformation numérique et de la diffusion de l'intelligence artificielle en santé. Il convient, tout d'abord, de rappeler que la collecte massive de données – ce que l'on a pris l'habitude d'appeler un peu vite aujourd'hui « big data » – constitue une condition sine qua non au déploiement de l'intelligence artificielle. Celle-ci s'appuie, en effet, sur des algorithmes qui nécessitent la mobilisation de données fiables et en nombre suffisant pour dégager des calculs robustes de probabilités permettant d'appuyer les orientations de l'intelligence artificielle.

Une « course aux données de santé » s'est engagée au niveau mondial. Pour pouvoir approvisionner les algorithmes, ces données doivent être médicalement et techniquement fiables mais également en volume suffisant pour permettre à l'IA de s'appuyer sur des régularités statistiques robustes. Cette compétition internationale pour les données de santé est naturellement marquée par un facteur temps.

Dans l'Union européenne, le besoin de protection de ces données personnelles a été à l'origine du règlement général sur la protection des données (RGPD) qui place notre continent à l'avant-scène mondiale en terme de protection des données de santé.

Il est également essentiel de bien avoir à l'esprit que la diffusion de l'intelligence artificielle et de la robotisation en santé est tout sauf un processus récent. S'agissant de l'évolution de la médecine elle-même, la « part humaine » dans la décision médicale n'a cessé de se réduire depuis plusieurs décennies, avec un développement exponentiel de la robotisation médico-technique (singulièrement en biologie et en pharmacie) et, plus récemment, des logiciels d'aide à la prescription voire à la décision médicale.

L'approche par les algorithmes face aux risques pandémiques constitue un prolongement naturel des fondements de la santé publique. L'intelligence artificielle produira, à partir de ses paramètres initiaux de programmation et de sa pratique de traitement massif de données, des orientations d'aide à la décision ou des décisions directes visant à la santé du plus grand nombre. Les perspectives de déploiement de solutions d'IA dans l'aide à la gestion de risques épidémiques s'inscrivent directement dans cette logique.

Si la réponse au COVID-19 est d'abord et principalement humaine, il faut aussi relever que l'IA est également assez largement utilisée en réalité dans la pratique de la réponse à la pandémie : repérage des foyers épidémiques, apprentissage machine par reconnaissance d'image sur les clichés pulmonaires, mobilisation de robots pour faire respecter des mesures de confinement pour des millions de personnes… Avec Jouve, nous développons des outils d'IA susceptibles d'aider à la gestion du back-office en contexte épidémique : nous avons, ainsi, mis au point la solution Know Your Patient, IA d'assistance à l'admission à distance des patients pour éviter les concentrations inutiles de patients dans les halls hospitaliers à des fins purement administratives.

Nous avions proposé avec Ethik IA, voici deux ans et demi, l'introduction d'un principe de garantie humaine de l'intelligence artificielle en santé. S'ouvrir résolument à l'innovation et essayer d'en réguler les enjeux éthiques au fil de son application : c'est le sens de cette « Garantie Humaine » de l'IA désormais insérée dans la révision de la loi de bioéthique. En retenant ce principe, la France fait le choix d'une approche enfin plus ouverte de l'innovation, dans un cadre législatif et réglementaire qui est déjà, il est vrai, le plus protecteur au monde.

Pourquoi les grands acheteurs préfèrent les retards de paiement aux concessions tarifaires ?

Michel Dietsch

Professeur Emérite à l'Université de Strasbourg, en poste à Sciences Po Strasbourg

Les grandes entreprises paient moins ponctuellement leurs fournisseurs. Selon la Banque de France, 70% des PME respectent la norme de 60 jours, mais ce chiffre n'est que de 53% dans les ETI et de 46% dans les GE. Cette situation n'est pas propre à la France. Selon D&B, seules 14% des GE payent à date en France, 33% au Royaume-Uni et 42% en Allemagne. Il s'opère ainsi un transfert vers les grands acheteurs qui resserre la trésorerie des PME et pénalise leur croissance.

L'intérêt pour les retards tient sans doute aux sommes en jeu. Les dettes fournisseurs représentent 645 milliards d'euros en 2018 selon l'INSEE. Les ETI et les GE en détiennent au moins les deux tiers, dont plus de la moitié correspond à des délais supérieurs à 60 jours. Le non-respect des 60 jours par les entreprises les plus grandes leur procure donc près de 100 milliards d'euros. Mais, pour les grands clients, les retards ne peuvent être justifiés par l'existence de besoins de trésorerie. Ils relèvent plutôt de l'intention stratégique, motivée par l'état de la concurrence. A l'évidence, les retards des grands clients augmentent positivement avec leur pouvoir de négociation. Mais alors pourquoi préfèrent-ils les retards aux concessions tarifaires ?

Le crédit fournisseur n'est pas un crédit comme les autres. C'est un crédit bon marché, de sorte que les retards équivalent à une concession tarifaire, la valeur du temps diminuant le coût effectif des achats. Ainsi, le crédit fournisseur modifie directement le partage du profit dans la chaîne, sans toucher aux tarifs. De plus, il peut être différencié entre les acheteurs, alors que la loi interdit de leur appliquer des prix différents.

C'est pourquoi les retards dépendent du pouvoir de négociation. Or la concentration des acheteurs a augmenté ces dernières décennies, limitant la capacité des fournisseurs à diversifier leur clientèle. Cela les conduit à accepter les retards, qu'ils aient ou non un pouvoir de négociation. S'ils n'ont pas ce pouvoir, l'allongement des délais transfère une partie du surplus à leurs grands clients sans que ces derniers changent les prix, ce qui maintient le profit total de la chaîne. Seule sa répartition change. S'ils ont ce pouvoir et forment de fait un oligopole, la concurrence par les délais est préférée et les délais clients sont les plus élevés lorsque la concentration des fournisseurs est élevée. En somme, les vendeurs valident un comportement opportuniste des grands acheteurs.

Deux moyens peuvent limiter cet opportunisme. Le premier est l'application effective de la norme prévue par la LME. Aujourd'hui encore, les GE demeurent moins ponctuelles. Les sanctions de la DGCCRF pour infraction à la norme les touchent fréquemment. Pourtant, le respect de la norme est capable de limiter les transferts et de transformer la structure du marché amont, comme dans les transports. Le deuxième est la discipline de marché. A l'évidence, le respect des délais prévus procure des rendements boursiers supérieurs à la normale. La redistribution des liquidités ne saurait donc nuire à l'intérêt des grands groupes. Elle contribuerait de manière évidente à l'intérêt général.

NB : Une version complète est disponible auprès de michel.dietsch@unistra.fr

Le risque numérique pour les entreprises : tous concernés par ce risque immatériel

Catherine Chambon

Présidente d'Interpole Cybersécurité et Responsable Cybersécurité au Ministère de l'Intérieur

Aujourd'hui, les entreprises sont la principale cible d'attaques informatiques et ce, quelle que soit leur taille. Pour les entreprises de moins de 50 salariés, 4 sur 10[1] ont été victimes d'attaques informatiques par rançongiciel[2]. Les grandes entreprises ne sont pas plus épargnées. En 2019, la société Altran a vu tout son système d'information paralysé juste avant la publication de ses résultats sur les marchés financiers.

Les préjudices liés à la cybercriminalité : atteintes à l'e-réputation, vol de données personnelles, d'informations couvertes par le secret des affaires, pertes financières, sont des risques majeurs qui nécessitent la mise en œuvre de mesures de protection technique mais également humaine et d'anticiper la gestion de crise.

Les entreprises doivent, avant tout, mettre en place un plan d'action afin de protéger leurs patrimoines immatériels et relever leur niveau de sécurité. Ce plan doit être anticipé et prendre en compte tous les volets de l'entreprise qu'il s'agisse des infrastructures physiques et techniques, du personnel ou des processus organisationnels.

Lutter contre les cyberattaques passe indéniablement par la sensibilisation et la formation du personnel, premier acteur de la protection des données de l'entreprise. Tous les professionnels doivent pour cela acquérir des « réflexes sûreté cyber » tels que ne pas laisser sans surveillance leurs ordinateurs ou téléphones professionnels, ne pas procéder à des opérations sensibles lorsqu'ils sont sur des wifi publics ou encore de crypter leurs supports numériques, protection indispensable en cas de vol. De même, l'organisation régulière d'audits et de tests sont autant de mesures permettant à l'entreprise de s'assurer que son dispositif est adapté et qu'elle dispose des ressources indispensables à sa protection.

Enfin, en cas de cyberattaques, il est important, concomitamment, de porter plainte et de geler les systèmes dès la compromission enclenchée ou détectée. Il est essentiel que les entreprises qui subissent de telles attaques se rapprochent des services de police et veillent à la préservation de la preuve en isolant les machines compromises et en les tenant à disposition des enquêteurs pour analyse.

Pour conclure, il est primordial aujourd'hui d'inclure les risques numériques dans la gestion de crise au même titre que les risques juridiques, financiers ou opérationnels. Chaque dirigeant d'entreprise, chaque personne personnellement comme professionnellement doit prendre conscience que les données sont un patrimoine qu'il faut sécuriser voire assurer.

La participation de la sous-direction de la lutte contre la cybercriminalité (SDLC) aux réflexions prospectives de Place Escange a vocation à éclairer d'une vision singulière les débats et les axes de propositions. Au cœur de la lutte contre ce phénomène depuis 2001, l'OCLCTIC et depuis 2014 pour la SDLC contribuent aux travaux nationaux, européens et internationaux pour améliorer l'identification des groupes criminels organisés et à la prévention.

Souhaitons une belle réussite à Place Escange, à son souhait d'associer la SDLC de la direction centrale de la police judiciaire à un panel d'experts et qu'une impulsion, une dynamique commune accompagne les entreprises françaises dans leur épanouissement économique et leur sécurité cyber.

[1] Source : https://www.cpme.fr/positions/numerique/16-chiffres-cles-sur-la-cybersecurite-des-entreprises-50-salaries

[2] Logiciel malveillant qui chiffre les données ou rend les systèmes inutilisables et affiche une page indiquant une demande de rançon (à vérifier mais la note de rançon peut arriver après – il n'y a pas forcément une page qui s'affiche)

Directives européennes et gestion du risque immatériel

Stéphanie Verilhac Marzin

Directrice SVM Consult
Spécialisée en affaires publiques et réglementaires européennes et françaises dans les secteurs du digital, de la publicité, de l'information d'entreprise et de la gestion du risque

A l'aune de l'évolution de la crise sanitaire majeure que nous vivons, l'impact économique pour les entreprises françaises frappées de plein fouet par la baisse ou l'arrêt complet d'activité ou par les mesures drastiques de fermeture imposées par le confinement est lui aussi sans précédent. Pour les entreprises françaises, un enjeu essentiel se profile : tenter de juguler au maximum les retards ou défauts de paiement pour ainsi éviter les faillites ou liquidations en cascade.

Le socle sur lequel se basent les politiques de soutien aux entreprises et d'aménagement des échéances sociales ou fiscales repose pour partie sur les mesures exceptionnelles décidées en temps de crise mais également sur des directives européennes impactant la gestion du risque et de l'immatériel. Ainsi la directive européenne sur les délais de paiement, adoptée en 2011, prévoit que les Etats Membres adoptent des lois nationales pour réduire les délais de paiement contractuels inter-entreprises à 60 jours ouvrés maximum. Cette mesure a déjà été intégrée dans la LME française de 2008 qui établit des plafonds pour les délais de paiement contractuels à 45 jours fin de mois ou 60 jours à compter de la facture. La directive prévoit également des délais de paiement à 30 jours à réception de facture ou des marchandises entre pouvoirs publics et entreprises privées et la possibilité pour toute entreprise sujette à un défaut de paiement de réclamer des intérêts compensatoires. Cette mesure est cependant peu utilisée car les entreprises évaluent souvent le dommage réputationnel de la relation client-fournisseur avant de demander des intérêts compensatoires.

La crise actuelle a mis en lumière de façon cruciale l'impact négatif des délais et retards de paiement sur la trésorerie des entreprises françaises et la nécessité d'une harmonisation des pratiques européennes en la matière. La Commission Européenne travaille d'ailleurs sur le suivi de la transposition de ces mesures en droit national et organise régulièrement des échanges incluant des représentants nationaux, dont les acteurs de l'information d'entreprise et de la gestion du risque client.

Autre instrument européen utile aux entreprises en particulier dans la situation actuelle, la directive sur l'insolvabilité et la seconde chance a été révisée en 2019 et doit être transposée avant juillet 2021. Tout en laissant la possibilité aux États membres de conserver une certaine souplesse quant aux moyens les plus appropriés de mise en œuvre dans leurs contextes nationaux d'outils d'alerte précoce, elle doit permettre une meilleure harmonisation des mesures de restructuration et d'insolvabilité des États membres et de renforcer la culture du sauvetage des entreprises en difficulté dans l'Union Européenne. En permettant de détecter rapidement les circonstances dont pourraient découler une insolvabilité et d'y remédier en amont par des procédures ou mesures rapides visant à maintenir ou restructurer l'activité et éviter l'insolvabilité d'une entreprise, la directive renforce le rôle crucial de la prévention dans la gestion du risque immatériel des entreprises.

Comment intégrer les risques intangibles des longues chaînes d'approvisionnement

Michel Philippart, DBA

Professeur, Département Stratégie,
EDHEC Business School

La « mondialisation » a offert des gains de productivité importants, par la concentration des moyens de production d'une offre standardisée, et des gains de coûts par le transfert vers des pays ou les pressions salariales et régulatoires étaient plus faibles. Ce sont des gains très tangibles. Mais qu'en est-il des éléments intangibles, en particulier les risques liés à la chaîne d'approvisionnement ? La crise actuelle liée au Covid-19 vient brutalement les mettre en évidence, mais il est trop tard pour éviter les coûts qu'elle induit. Pourquoi en sommes-nous là ? Il faut à la France et à l'Europe une réflexion sur l'importance d'une analyse plus poussée des risques intangibles, qu'ils soient liés à la longueur des chaînes d'approvisionnement, aux risques géopolitiques, ou à tout autre risque systémique.

Rappelons que le capital intangible est une promesse de bénéfices futurs qui n'apparaît pas au bilan, et qui est difficile à contrôler. Le risque intangible est son pendant : une exposition à des pertes futures qui n'est pas quantifiable par les méthodes classiques d'analyse de risque basées sur des études statistiques à cause de la nature rare et aléatoire des événements créant ce risque.

Les approches de comparaison des coûts les plus communes sous évaluent le coût des risques tout au long de la durée de vie du produit. Les risques sont identifiés, mais comme ils sont peu matériels, dans un environnement concurrentiel qui discounte fortement les risques futurs par rapport aux gains présents, ils sont rapidement effacés des paramètres de décision. En Europe, les moyens de production ont dû fermer, avec un coût intangible lié à la déconstruction du tissu économique non inclus dans l'analyse. En Asie, nous avons créé des chaînes d'approvisionnement longues qui ont concentré des risques intangibles systémiques également mutualisés.

Certains proposeront un rôle accru pour la puissance publique, qu'elle soit nationale ou européenne. Est-ce une solution ? N'est-ce pas remplacer un risque intangible par un autre, tout aussi intangible ? Une approche législative offre un cadre rassurant, mais s'accompagne souvent de nouvelles complexités de gestion. Elle apporterait un bénéfice au profit d'un groupe déterminé, mais qui en contrepartie imposerait à l'ensemble des contraintes qui alourdissent et freinent le dynamisme économique, une charge invisible et donc intangible pour les rédacteurs et les bénéficiaires.

Bien sûr il y aura toujours un sourcing dans des pays à faible coût, aujourd'hui l'Asie du Sud-Est, peut-être demain l'Afrique, mais l'équilibre entre chaînes d'approvisionnement locale et lointaines doit se construire grâce à la prise en compte des risques intangibles. Nous avons besoin de nouvelles idées, « pouvoir de vivre sainement, avec un futur porteur d'espoirs » tout en conservant la liberté d'entreprendre, sans tomber dans l'inflation de régulations servies par des couches administratives peu efficaces… La crise est donc une opportunité de réfléchir à notre relation avec les « Best Cost Countries », un défi pour nous tous.

Olivier Leduc

Commissaires aux comptes
Membre de la commission résolution des litiges du Conseil régional de l'Ordre des Experts-Comptables de Paris / Ile-de-France, Contrôleur qualité à Compagnie régionale des commissaires aux comptes de Paris
Administrateur de PME.

Comment intégrer l'impact du covid-19 dans l'évaluation des actifs et des passifs lors de l'arrêté des comptes 2019

En cette période d'arrêté des comptes et de pandémie à l'échelle mondiale, nous pouvons nous demander si l'évaluation des actifs et des passifs au 31 décembre 2019 doit refléter les conséquences de l'épidémie de Covid-19 ?

L'évaluation des actifs et des passifs au 31 décembre 2019 doit refléter uniquement les conditions qui existaient à la date du 31 décembre 2019. Les effets de l'épidémie de Covid-19 n'étant pas liés à une situation existant au 31 décembre 2019, la valeur des actifs et des passifs comptabilisés au 31 décembre 2019 n'est pas ajustée.

Au-delà de l'évaluation des actifs et des passifs, quelle l'information faut-il donner dans l'annexe au titre des événements postérieurs à la clôture liés à l'épidémie de Covid-19 ?

En revanche, une information doit être donnée dans les notes aux états financiers (annexe aux comptes annuels) sur l'impact de l'épidémie de Covid-19 sur la valeur comptable des actifs et des passifs au 31 décembre 2019. Ses conséquences post-clôture ainsi qu'une estimation de son impact financier sur les états financiers s'il peut être déterminé ou l'indication que cette estimation ne peut être faite.

Que se passe-t-il s'il apparaît, durant la période entre la clôture du 31 décembre 2019 et la date d'arrêté des comptes par l'organe compétent, que l'entité est dans une situation d'incertitudes significatives sur sa capacité à poursuivre son exploitation ?

Lorsque la direction a connaissance, durant la période entre la clôture du 31 décembre 2019 et la date d'arrêté des comptes par l'organe compétent, d'incertitudes significatives liées à des événements ou à des circonstances postérieurs à la clôture qui peuvent jeter un doute important sur la capacité de l'entité à poursuivre son exploitation, l'entité doit donner une information appropriée dans son annexe. Celle-ci peut consister en :

- la description des principaux faits ou situations à l'origine de cette incertitude significative ;
- la description des plans d'action engagés par la direction de l'entité pour y faire face ;
- la mention qu'en conséquence l'entité pourrait ne pas être en mesure de réaliser ses actifs et de régler ses dettes dans le cadre normal de son activité.

Que se passe-t-il si la continuité d'exploitation est définitivement compromise durant la période entre la clôture du 31 décembre 2019 et la date d'arrêté des comptes par l'organe compétent ?

De façon générale, lorsqu'il apparaît, durant la période postérieure à la clôture du 31 décembre 2019 et jusqu'à la date d'arrêté des comptes par l'organe compétent, que la continuité d'exploitation est définitivement compromise, les comptes préparés au 31 décembre 2019 ne sont pas modifiés mais une information doit être donnée dans l'annexe (présentation de la nature de l'événement ainsi que des comptes simplifiés établis en valeurs liquidatives).

Francis Babé

Cadre dirigeant en retraite d'Organisations Syndicales et Professionnelles (Nord-Pas-de-Calais - Paris)
Administrateur de PME.

De la souveraineté de l'entreprise

La crise de la COVID 19 a cruellement fait apparaître les lacunes béantes de notre « souveraineté sanitaire » c'est-à-dire de la capacité de notre pays à disposer sans délais des outils nécessaires pour faire face à la pandémie : respirateurs, masques, principes médicamenteux, dont les fournisseurs, étrangers étaient à l'arrêt pour cause de confinement, tout comme les circuits commerciaux internationaux. Et chacun de disserter sur la nécessité vitale, pour le pays de recouvrer sa « souveraineté » en la matière.

Qu'en est-il pour l'entreprise ? Est-elle toujours maîtresse de son destin et de son autonomie de décision, quelques soient les circonstances, fussent-elles les plus dramatiques, les plus extrêmes, les plus improbables ?

Dans l'alchimie des relations entre les « parties prenantes » de l'entreprise, son marché, ses produits, ses clients, ses fournisseurs, ses financeurs, son personnel, sa direction, ses propriétaires, son environnement sociétal, rechercher à construire – ou à reconquérir – une indépendance opérationnelle doit faire l'objet, de la part des dirigeants d'une réflexion stratégique permanente :

| Mon capital est-il stable à long terme, ou volatil et vulnérables ?

Mes collaborateurs, de tout niveaux, sont-ils attachés à l'entreprise, à son histoire, à sa culture, ou ne sont-ils que des mercenaires ?

Mes clients sont-ils fidèles aux produits que je leur offre, ou sont-ils des papillons zappeurs, et si oui pourquoi ?

Que mijotent, préparent et manigancent **mes concurrents**, où qu'ils se trouvent dans le vaste monde ?

Mes banquiers et mes créanciers, comme mes débiteurs, sont-ils des partenaires de confiance ?

La société qui m'entoure m'accorde-t-elle une image positive pour l'apport de mes produits, de mes process, de mes relations sociales, de mes impacts environnementaux ?

L'autonomie de décision de l'entreprise, et de l'entrepreneur, s'inscrit pleinement dans la démarche classique du décideur : quelles sont mes volontés ? Quelles sont les opportunités et les menaces de l'environnement ? Quelles sont les forces et les faiblesses de l'entreprise ?

La crise sanitaire, puis économique et sociale que nous traversons amenant la question de la souveraineté de l'entreprise, dans la tourmente, sur le dessus de la pile des préoccupations.

Il ne s'agit pas, bien sûr, de vivre en autarcie, mais de répartir les risques et les dépendances pour en diluer les effets, tant en interne qu'en externe : les outils s'appellent « dialogue social dans l'entreprise », « plan de continuation d'activité » tenu à jour, diversification des fournisseurs, des clients, des financeurs… sans porter atteinte à l'autonomie et à la responsabilité du décideur.

« Lorsque vous avez un missile aux fesses, vous avez quelques secondes pour réagir. Ce n'est pas le moment de réunir le comité d'entreprise » – Vice-amiral Loïc Finaz, Directeur de l'Ecole de Guerre (in Le Point 28 mai 2020. Page 113).

François Humblot

Directeur associé de GRANT ALEXANDER

L'e-réputation, une composante du risque immatériel dans tous les métiers

| La réputation a toujours été l'élément essentiel de la valeur d'une marque.

Beaucoup d'entreprises ou de particuliers choisissent, une société de conseil, un cabinet d'avocat, une banque, un organisme de formation en fonction de leur réputation, souvent sur recommandation. Mais c'est aussi vrai pour les métiers de services qui se sont énormément développés depuis vingt ans et pour l'industrie.

Même si celui qui achète mène une recherche rigoureuse de fournisseur en s'attachant à identifier tous les acteurs du marché qui ont les savoir-faire dont il a besoin, il sera toujours favorablement impressionné par les éléments de réputation qu'il pourra recueillir dans son environnement.

C'est sa réputation qui permet à une entreprise d'être plus souvent consultés que ses concurrents et de fixer parfois des prix un peu plus élevés que la moyenne du marché.

La construction de cette réputation se fait dans la durée et elle repose toujours sur une qualité de service perçue par les clients nettement au dessus de la moyenne. Cette qualité suppose des compétences internes reconnues, une organisation efficace et surtout une culture interne orientée vers la satisfaction du client.

Jusqu'aux années 2000 une bonne réputation, une fois acquise, pouvait assez facilement être entretenue si la qualité du service restait globalement la même.

Le développement exponentiel d'internet a tout changé : une e-réputation peut se construire beaucoup plus vite que par le passé mais elle peut aussi se détruire en un temps record.

Chacun utilise son moteur de recherche préféré pour voir ce qui est écrit sur l'entreprise ou la marque qu'il veut évaluer. Internet garde indéfiniment la trace de tout ce qui est écrit sur une entreprise et il est extrêmement difficile de se débarrasser de commentaires désobligeants qui ont pu circuler sur le réseau à un moment ou un autre.

Le risque de dommage lié à une cabale, une médisance ou une rumeur sur internet est malheureusement de plus en plus important. Cette menace peut venir de partout : un client mécontent, un concurrent jaloux, un fournisseur éconduit, un ancien salarié ou un salarié en conflit avec son employeur.

Conserver une qualité de service ou de produit élevée et bien maîtriser sa communication sont bien sûr des moyens de se protéger mais ce n'est plus du tout suffisant.

L'entreprise doit être irréprochable dans tous les domaines et doit respecter toutes ses parties prenantes. De même tous les salariés de l'entreprise doivent eux-mêmes être les ambassadeurs d'une image positive de leur société ce qui suppose une gestion des relations humaines également de grande qualité.

Louis-Rémy Pinault

Expert développement stratégique chez GENERALI & Membre du Comité Scientifique «Place Escange»

Capital immatériel : nouvel enjeu de la maîtrise des risques

L'approche par le capital immatériel est utilisée habituellement pour réaliser la mesure extra-financière des actifs de l'entreprise ou l'évaluation financière du capital immatériel avec pour objectif de définir le potentiel de création de valeur d'une organisation.

| Il est, en principe, classé de la manière suivante :

Il représente en moyenne 60 % de la valeur des entreprises. Si les grandes entreprises et en particulier les entreprises cotées suivent l'évolution de la valeur de leurs actifs immatériels, il est beaucoup plus rare que les PME/PMI et petites ETI l'intègrent dans leurs analyses d'activité, les pilotent et mettent en œuvre des actions pour le valoriser, ou même cherchent à l'évaluer.

Or, Il traduit la confiance des parties prenantes dans l'entreprise, sa gouvernance, au-delà de sa capacité à atteindre ses objectifs financiers et de la qualité de ses actifs matériels. Il donne un éclairage pertinent sur la mission de l'entreprise, sa raison d'être et ses valeurs.

Il se situe donc au cœur de la stratégie de l'entreprise et peut être approché à la fois comme objet de risques et comme levier du développement de la maturité RSE de l'entreprise. Il est donc pertinent, simultanément de :

Cartographier le capital immatériel pour en mesurer la robustesse par l'analyse des risques en évaluant la vulnérabilité de ses éléments constitutifs et de ses impacts pour anticiper les effets dominos dans un second temps. Ainsi est-il possible par exemple, de relier développement du capital humain, vulnérabilité des systèmes d'information, perte d'image et impacts sur le capital clients.

| Mesurer les impacts des actions RSE sur le capital immatériel.

Les actions menées pour développer le capital humain, notamment dans le cadre du développement des compétences, de la santé sécurité des collaborateurs vont avoir un impact positif sur les risques, notamment accidents du travail, risque pénal du dirigeant, mais aussi sur la motivation du personnel et la qualité du travail et donc de la satisfaction des clients.

Ainsi, en décloisonnant Excellence Opérationnelle/ maîtrise des processus, management par les risques et politique RSE autour du capital immatériel intégré dans cette double dimension objet de risque et Responsabilité, se crée alors une dynamique favorable autour de 5 leviers essentiels à la Performance Globale de l'entreprise : innovation, différenciation, image et réputation, réduction des risques et maîtrise coûts qualité délais.

La crise sanitaire du COVID 19 met en perspective une crise économique qui impose, responsabilité, résilience, redémarrage. La résilience ne se décrète pas mais se construit.

Cette démarche est sans doute le préalable pour affronter les difficultés qui sont à nos portes mais aussi la condition pour repenser le projet de transformation et de relance de l'entreprise autour de la transition énergétique, de la transition numérique, de la transition vers une économie circulaire, et l'implication dans la transition territoriale tant l'ancrage sur le territoire est fondamental.

L'entreprise devra être accompagnée, soutenue dans sa trajectoire de résilience au service de la Performance Globale. C'est aussi un enjeu majeur pour l'assureur qui doit prendre en compte ces nouvelles dimensions de la gouvernance des risques et trouver des solutions pour aider l'entreprise à reconstituer son capital immatériel lorsqu'il est face à des risques dont il doit transférer le financement.

Capital et risque immatériels : les nouvelles dimensions de la valeur de l'entreprise

Michel Philippart, DBA

Professeur, Département Stratégie,
EDHEC Business School

Où se trouve la valeur d'une entreprise ? Un bilan est loin de refléter entièrement cette valeur. En 2019, Apple vaut plus de 10 fois sa valeur comptable. En 2018 le capital immatériel des entreprises du CAC40 représente 76% de la valeur marché des entreprises. Sans atteindre les proportions d'Apple ou Google un tiers de la valeur du CAC est non inscrite au bilan.

Le capital est ce qui est investi pour assurer des bénéfices futurs. Le capital immatériel contribue au fonctionnement de l'entreprise et lui permet de se différencier par rapport à ses concurrents sans être quantifié dans les documents comptables. On pense immédiatement à la marque et à la confiance sous-jacente. Il faut aussi considérer la donnée, le capital intellectuel, la chaîne d'approvisionnement, les plates-formes de la nouvelle économie. Il est une source de savoir et d'expertise, promesse de bénéfices futurs avec un rendement croissant, sans valeur comptable et donc difficile à échanger ou à défendre. Le test des 4 S pour « sunkenness / Fonds Perdus, Spillovers/ Retombées Collatérales, Scalabilité et Synergies » facilite l'identification de ce capital immatériel.

| Le risque immatériel

Les entreprises sont conscientes du risque sur leur capital physique pouvant causer une interruption des activités. Qu'en est-il du risque immatériel, défini comme tout ce qui peut endommager fortement la valeur du capital immatériel ou interrompre les opérations d'une entreprise alors que son capital physique reste accessible et opérationnel. Puisque la nature même du capital immatériel est d'être difficile à identifier, le risque immatériel est moins pris en compte que le risque sur les éléments tangibles du bilan. Le capital intellectuel, la donnée, la réputation, la confiance des clients ou des fournisseurs sont soumis à des risques difficiles à maîtriser mais qui sont soumises aux dangers liés aux réseaux sociaux, à la numérisation croissante des activités, etc.

| De l'identification au pilotage

Voici les questions qui permettent d'aborder le pilotage de l'immatériel

1. **Identifier** le capital immatériel et sa contribution à vos bénéfices présents et futurs, un effort associant experts financiers et experts métier.
2. **Cartographier** les risques qui peuvent détruire ces flux de bénéfices, les risques sur les données, les marques, l'écosystème.
3. **Piloter** le risque immatériel structurés de la même manière que ceux mis en place pour le risque sur le personnel ou vos biens physiques : Évitement, réduction de l'impact, et de la fréquence, mutualisation, plans d'action.

Les observations sur le terrain montrent que la gestion du capital et du risque immatériels doivent mieux se structurer au sein des entreprises, qu'elles soient de la nouvelle économie ou en conversion vers l'exploitation des nouveaux outils de l'ère numérique.

23 novembre 2022

Place Escange au Club CNRS Entreprises

Dans le cadre de son partenariat avec le CNRS, Place Escange, avec la participation de son Délégué général, Sébastien Bouchindhomme, a vécu au sein du club CNRS Entreprises, un moment fort public-privé avec Sébastien Tanzilli du CNRS – Centre national de la recherche scientifique et Charles Beigbeder de AUDACIA sur les Technologies Quantiques.

Les membres présents : Michael Haddad, Patrick Cogez, Regis Cadot, Fabien Mathieu, Bruno Stoufflet, Denis Haudebault, Alix Gicquel, Philippe Pradel, Daniel Piana, Michel Kurek, Louis Delaittre, Florent Detroy, Pauline Boucher, Stéphane Crochetet, Sophie Muller, Cédric Demeure, Clément Drouet, Hacène Goudjil, Eléonore de Rose et à Jean-Luc Moullet, Carole Chrétien, Clémentine Robert, Estelle Gaspard, Patrizia Borghetti et Pierre Roy du CNRS.

17 novembre 2021

Place Escange renforce ses instances et accueille de nouvelles personnalités !

Place Escange, le think tank du risque immatériel en entreprise, propulsé par la FIGEC, a réuni le 16 novembre les membres de son Conseil scientifique, de son Comité d'experts et ses contributeurs, sous la houlette de leur Président, Charles Battista. En prévision 2022, un programme ambitieux intitulé « 360° sur le risque immatériel », basé sur la pédagogie, l'innovation, le digital, la fiscalité… avec en ligne de mire, une « place » dans le débat des élections présidentielles et législatives.

De gauche à droite : Louis-Rémy Pinault (Expert Développement Stratégique – Generali), Philippe Berna (Médiateur de la filière aéronautique et spatiale, Président du collège des médiateurs), Stéphanie Verilhac-Marzin (SVM Consult), Marie-Anne Desnoulez-Deldique (Co-fondateur WeTalk Group), Antoine-Tristan Mocilnikar (Ingénieur général des mines au Service du Haut fonctionnaire de défense et de sécurité), Jo-Michel Dahan (Conseiller – Médiateur des entreprises), Charles Battista (Président de Place Escange et de la FIGEC), Sébastien Bouchindhomme (Délégué Général de Place Escange et de la FIGEC), Jacky Isabello (Co-fondateur CorioLink), Michel Philippart (Professeur à l'EDHEC Business School), Frédéric Lefret (Président de l'Institut du Dialogue Civil), Bernard Attali (Président du cabinet de conseil en stratégie « Gouvernance et Valeurs »), Olivier Leduc (Expert-Comptable), Valentin Clément (étudiant EDHEC Business School).

17 juin 2021

Conférence « Piloter son risque immatériel »

Place Escange et la FIGEC ont organisé le 16 juin dernier un webinaire exceptionnel sur le thème « Piloter son risque immatériel ». Depuis plusieurs années, l'économie immatérielle s'étoffe progressivement pour revêtir de nombreuses dimensions dans nos sociétés : les flux financiers internationaux, la gestion du risque client / fournisseur, la réputation, la sécurité de l'entreprise, la data, le e-commerce, la responsabilité sociétale, l'environnement, l'éthique… Plus que jamais, échanges, confiance, décloisonnement et transparence économique sont parties prenantes de l'économie française. Aujourd'hui, 80% du risque d'entreprise est immatériel !

Conférence animée par Rachib Arhab (journaliste-auteur, conseiller en communication) avec Paola Fabiani (Présidente-fondatrice de Wisecom, Présidente du Comex40 du MEDEF, élue à la CCI de Paris), Michel Sapin (Avocat, Ancien Ministre), , membre du Collège lutte contre les discriminations auprès du Défenseur des Droits) et Charles Battista (Président de Place Escange et de la FIGEC).

Cybersécurité : un risque immatériel bien tangible

place escange
Le think tank du risque immatériel en entreprise

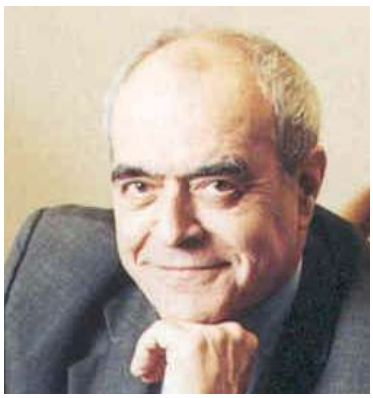
www.place-escange.fr

Ce guide, à destination des entreprises, aborde de façon pragmatique l'ensemble des aspects de la cybersécurité. C'est le résultat d'un travail réalisé par « Place Escange » en collaboration avec **Jean-Noël Barrot,** Ministre délégué chargé de la Transition Numérique et des Télécommunications, **Nicolas Arpagian,** Directeur de la Stratégie en cybersécurité de Trend Micro Europe, Enseignant à l'Ecole Nationale Supérieure de la Police et à Science Po Saint Germain en Laye, **Alain Juillet,** Président d'Honneur de l'Académie de l'Intelligence Economique, **Thibault Lanxade,** Entrepreneur et Président-Directeur Général du Groupe Luminess, **Jérôme Notin,** Directeur général du GIP ACYMA cybermalveillance.gouv.fr et **Michel Van Den Berghe,** Président de Campus Cyber, et bien d'autres experts.

Merci à eux pour leur apport éclairé sur le sujet.

Jean-Noël Barrot,

Nicolas Arpagian,



Alain Juillet,

Thibault Lanxade,

Jérôme Notin,

Michel Van Den Berghe

SOMMAIRE

LinkedIN : @place-escange

Twitter : PlaceEscange

ÉDITORIAL

Faut-il encore le rappeler ? Aujourd'hui, 80% des risques en entreprise sont immatériels… Une domination d'autant plus importante à prendre en considération que ces risques sont protéiformes : risque sanitaire, risque politique, cyber risque, risque des délais de paiements, risque géo-politique, risque de e-réputation…

Pour accompagner les entreprises dans l'identification, la compréhension et la gestion de ces risques, Place Escange, le think tank dédié au patrimoine immatériel des entreprises et à ses risques associés, publie régulièrement de nombreuses tribunes, podcasts, vidéos… sur son site place-escange.fr. Ce guide sur le risque cyber s'inscrit dans cette démarche.

Notre focus sur ce risque n'est pas le fruit du hasard. Depuis quelques années, le risque cyber connait une progression exponentielle notamment portée par l'évolution des entreprises et en particulier par leur transformation digitale et leur ouverture au monde de l'Internet. Or, si un temps les entreprises parvenaient à le contenir, force est de constater que la crise Covid a changé la donne sur le sujet : aujourd'hui, le risque cyber peut conduire à leur perte. Ce n'est d'ailleurs pas pour rien qu'il représente actuellement leur principale préoccupation.

Cet ouvrage a donc pour vocation de sensibiliser, alerter, conseiller sur les enjeux liés aux menaces issues du monde du net, afin que les entreprises s'en prémunissent le mieux possible.

Sa réalisation a notamment été rendue possible grâce à l'aide et au soutien du Ministre délégué chargé de la Transition numérique et des Télécommunications, Jean-Noël Barrot, de nos deux membres d'honneur Alain Juillet et Thibault Lanxade, des dirigeants du GIP ACYMA cybermalveillance.gouv.fr et du Campus Cyber, et d'autres experts… que nous remercions chaleureusement.

Ce guide se veut être le premier d'une série. En effet, pour demain, notre feuille de route ne varie pas et nous entendons poursuivre nos travaux notamment en publiant d'autres guides sur l'immatériel pour aider et accompagner les entreprises et en réfléchissant sur des notes de prospectives.

Charles Battista,
Président de Place Escange

Introduction

Désormais en tête des préoccupations de nombreuses entreprises et collectivités, le risque cyber fait de plus en plus l'objet de toutes les attentions dans les entreprises. Et pour cause, les « incidents cyber » se placent en tête des différentes études portant sur les risques des entreprises. Selon le Baromètre des risques d'Allianz 2023, la cybersécurité représente ainsi le premier sujet d'inquiétude des dirigeants français (40%).

La prise de conscience semble donc enfin avoir eu lieu et les entreprises se penchent de plus en plus sur leur sécurité numérique. Pour autant, face à l'accélération et à la complexification des attaques cyber, elles vont néanmoins devoir pousser un cran plus loin leurs démarches et renforcer leur stratégie de prévention et de maitrise de ces risques.

Au-delà des entreprises, les pouvoirs publics ont également un rôle important à jouer. Porté par les initiatives européennes, le régulateur français s'attache ainsi à légiférer pour protéger autant que possible les entreprises, en particulier contre ce risque. De même, l'état renforce ses dispositifs d'accompagnement des entreprises et collectivités face aux risques cyber.

Néanmoins, des efforts et des investissements restent à faire, notamment en termes de recherches et de formations, pour que la France dispose des ressources, compétences et expertises nécessaires au développement, à la compréhension et à l'exploitation des solutions propres à lutter efficacement contre le risque cyber.

1 ETATS DES LIEUX

Le numérique qui s'est invité dans le quotidien de tous, continue d'ouvrir la voie à des actes malveillants toujours plus sophistiqués et dont les impacts peuvent s'avérer fortement préjudiciables, voir fatals pour les entreprises visées.

A | Le risque cyber corrélé à la digitalisation de l'économie

Pour ceux qui peuvent encore en douter, le numérique et son environnement sont devenus des évènements essentiels de la civilisation moderne. Cependant, bien qu'étant source d'opportunités et vecteur majeur d'innovations, la transformation numérique s'accompagne également de nouvelles vulnérabilités. *« Aujourd'hui, il n'est plus possible d'exister dans notre civilisation moderne sans utilisation de toutes les facettes du numérique,»* **explique Alain Juillet, Président d'honneur de l'Académie de l'Intelligence Economique.** *« Cela implique d'en comprendre le fonctionnement et de l'intégrer dans notre environnement qui est d'une agressivité croissante. Plus ces systèmes sont efficaces et nous permettent de travailler, plus ils représentent un danger en termes de sécurité des échanges et d'utilisation frauduleuse des données. C'est la raison pour laquelle nous ne devons pas nous étonner des attaques cyber que nous subissons et des pratiques dont nous souffrons : ce sont désormais des composantes de ce nouveau monde ».*

Cette nouvelle dépendance du tissu économique au numérique ainsi que la rapidité de la transition digitale qui s'opère depuis quelques années ont ainsi facilité la multiplication de dommages ayant une origine cyber, en particulier les cyberattaques. La crise sanitaire a encore accéléré cette tendance, notamment à travers l'adoption de nouveaux modes de travail.

« Si auparavant nous pouvions dire que le risque cyber était essentiellement lié à des enjeux géopolitiques ou à l'intérêt de grandes puissances, aujourd'hui, il s'agit également d'un risque de proximité auquel tout un chacun est exposé », **précise ainsi Nicolas Arpagian, Directeur de la stratégie en cybersécurité de Trend Micro Europe et enseignant à l'Ecole Nationale Supérieure de la Police (ENSP) et à Sciences Po Saint Germain en Laye**.

B | Evolution exponentielle des cyberattaques

Selon une étude OpinionWay pour le CESIN, 54% des entreprises déclarent ainsi avoir subi au moins une attaque en 2021. Plus d'une entreprise sur deux est donc touchée. Des chiffres que corroborent le rapport Hiscox 2022, selon lequel 52 % des entreprises françaises auraient subi au moins une cyberattaque en 2022 (contre 49% en 2021).

Gage de la réalité de cette tendance, la plateforme cybermalvaillance.gouv.fr, chargée d'assister les victimes d'actes cyber malveillants, enregistre une augmentation de sa fréquentation depuis sa création « *Notre plateforme a ainsi reçu 1.4 millions de visiteurs en 2020, puis 2.4 millions en 2021 et près de de 3.8 millions en 2022*», **précise Jérôme Notin, Directeur général du GIP ACYMA cybermalveillance.gouv.fr.**

52%

DES ENTREPRISES FRANÇAISES AURAIENT SUBI AU MOINS UNE CYBERATTAQUE EN 2022

Jean-Noël Barrot,
Ministre délégué chargé de la Transition Numérique et des Télécommunications

« La menace cyber est ainsi passée du statut de l'exception à celui du quotidien et elle croit d'année en année en France. En 2021, il y a ainsi eu une augmentation de 37% des intrusions avérées dans des systèmes d'informations supervisées par l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Information). Chaque jour dans notre pays, ce sont près de 500 victimes (particuliers, collectivités, entreprises) qui font une demande d'assistance sur le site cybermalveillance.gouv.fr et nous assistons à 7 attaques sophistiquées contre des cibles critiques. Enfin, l'année dernière, une entreprise sur deux et une collectivité sur trois a déclaré avoir subi une attaque. »

C | Des typologies d'attaques toujours plus sophistiquées

Le cyber risque renvoie à l'ensemble des risques liés à l'usage des technologies numériques et peut être défini comme un risque opérationnel portant sur la confidentialité, l'intégrité ou la disponibilité des données et des systèmes d'information. Il recouvre à la fois des actes malveillants mais aussi les incidents non intentionnels issus d'erreurs humaines ou d'accidents. Les outils et méthodes utilisés pour ces attaques sont en constante évolution. Il semblerait d'ailleurs que le recours au télétravail ait modifié les axes d'attaques.

Selon l'étude Opinionway pour le CESIN, les vecteurs d'attaques les plus répandues en 2021 restent le phishing (73%) et l'exploitation des failles, à savoir la vulnérabilité logicielle ou le défaut de configuration (53%). Viennent ensuite l'arnaque au président (38%), les tentatives de connexion (34%), les acquisitions de noms de domaines illégitimes (31%) ou encore les Ddos, attaque en déni de service (25%). Les attaques indirectes par rebond, via des prestataires, tendent également à augmenter (21% vs 16% en 2019), ce qui souligne la dépendance grandissante des entreprises envers leurs fournisseurs externes. « *Il est à ce titre important de veiller à la sécurisation des sites qui hébergent les données des entreprises*», **souligne Thibault Lanxade, Entrepreneur et Président-Directeur Général du Groupe Luminess**. « *Par exemple chez Luminess, nous sommes dans une logique de souveraineté numérique : nos sites d'hébergement se trouvent à Mayenne et Laval* ».

D | Les points d'entrée des attaques

Vulnérabilité créée par l'erreur humaine

Le premier point d'entrée dans un système d'information est l'humain. En effet, 95% des violations proviennent de l'erreur humaine (Findstack, 2022). « *Le réseau informatique peut être à la pointe des technologies de protection, si l'un des employés de l'entreprise n'est pas vigilant et clique sur un contenu piégé, l'entreprise sera touchée* », **explique Arthur Bataille, CEO de Pr0ph3cy**. « *Plusieurs techniques plus ou moins sophistiquées sont utilisées par les hackers pour exploiter la faille sécuritaire humaine, la plus courante étant le phishing. Depuis 2022, nous assistons également à une augmentation des attaques par smishing* ». Une tendance notamment portée par le développement du travail à distance.

Moindre protection des endpoints

En 2022, les attaques les plus sérieuses se sont portées sur les endpoints (terminal qui peut être connecté à un réseau comprenant des ordinateurs de bureau, des ordinateurs portables, des téléphones mobiles, des tablettes et des serveurs), les identités et les clouds. « *L'essor des Raas (Ransomware as a service) et la professionnalisation des hackers a affaibli les protections des endpoints*», **explique François Berjamin-Salaun, Directeur Général chez Silicom & Open Cyber**. « *Des groupes créent des ransomwares et louent leur utilisation à des groupes spécialisés dans l'effraction virtuelle. La combinaison des deux spécialités rend les attaques beaucoup plus efficaces* ».

Développement du Cloud

Si les serveurs d'entreprise constituent le principal point d'entrée des pirates, le nombre d'intrusions signalées via le Cloud a considérablement progressé. Ainsi, selon l'étude OpinionWay pour le CESIN, la non maitrise de la chaine de sous-traitance de l'hébergeur (48%) et les difficultés de contrôles des accès par les administrateurs de l'hébergeur (43%) sont les deux principaux facteurs de risques émis par les entreprises en ce qui concerne l'utilisation du Cloud.

Fragilité de la chaine d'approvisionnement

En 2022, les attaques par la chaine d'approvisionnement ont pour leur part connu une augmentation de 650 % par rapport à 2021 (Rapport de la Sécurité 2022). Ce type d'attaque exploite les relations de confiance qui existent entre différentes organisations et cible le maillon le plus faible de cette chaine. Une fois qu'ils ont réussi à pénétrer dans le réseau de ce fournisseur, les attaquants peuvent alors accéder au réseau plus sûr par le biais de ce lien.

Augmentation de la surface d'attaque

D'autre part, la surface d'attaque des entreprises s'élargit du fait du travail à distance, de l'adoption généralisée de l'IoT (Internet des Objets) et du nombre important d'identités numériques créé pour une seule et même entreprise. Une augmentation de la surface qui fait également la part belle aux attaques basées sur la compromission et/ou usurpation des identités.

LEXIQUE

Le malware est un terme générique utilisé pour désigner une variété de logiciels hostiles ou intrusifs : virus informatiques, vers, cheval de Troie, ransomware, spyware, adware, scareware, etc. Il peut prendre la forme de codes exécutables, de scripts, de contenu actif et d'autres logiciels.

Le phishing est une technique frauduleuse destinée à leurrer les internautes en se faisant passer pour un organisme ou une personne de confiance afin d'entrer dans un système d'information et/ou récupérer des données sensibles de la victime. Il envoie un mail demandant généralement de «mettre à jour» ou de «confirmer» des informations suite à un incident technique (coordonnées bancaires, numéro de compte, codes personnels, etc.). Le phishing se décline en fonction des besoins des attaquants : le spearphishing nécessite par exemple une phase de reconnaissance plus importante, mais permet d'être plus efficace ; le smishing est une technique d'hameçonnage passant par les téléphones portables.

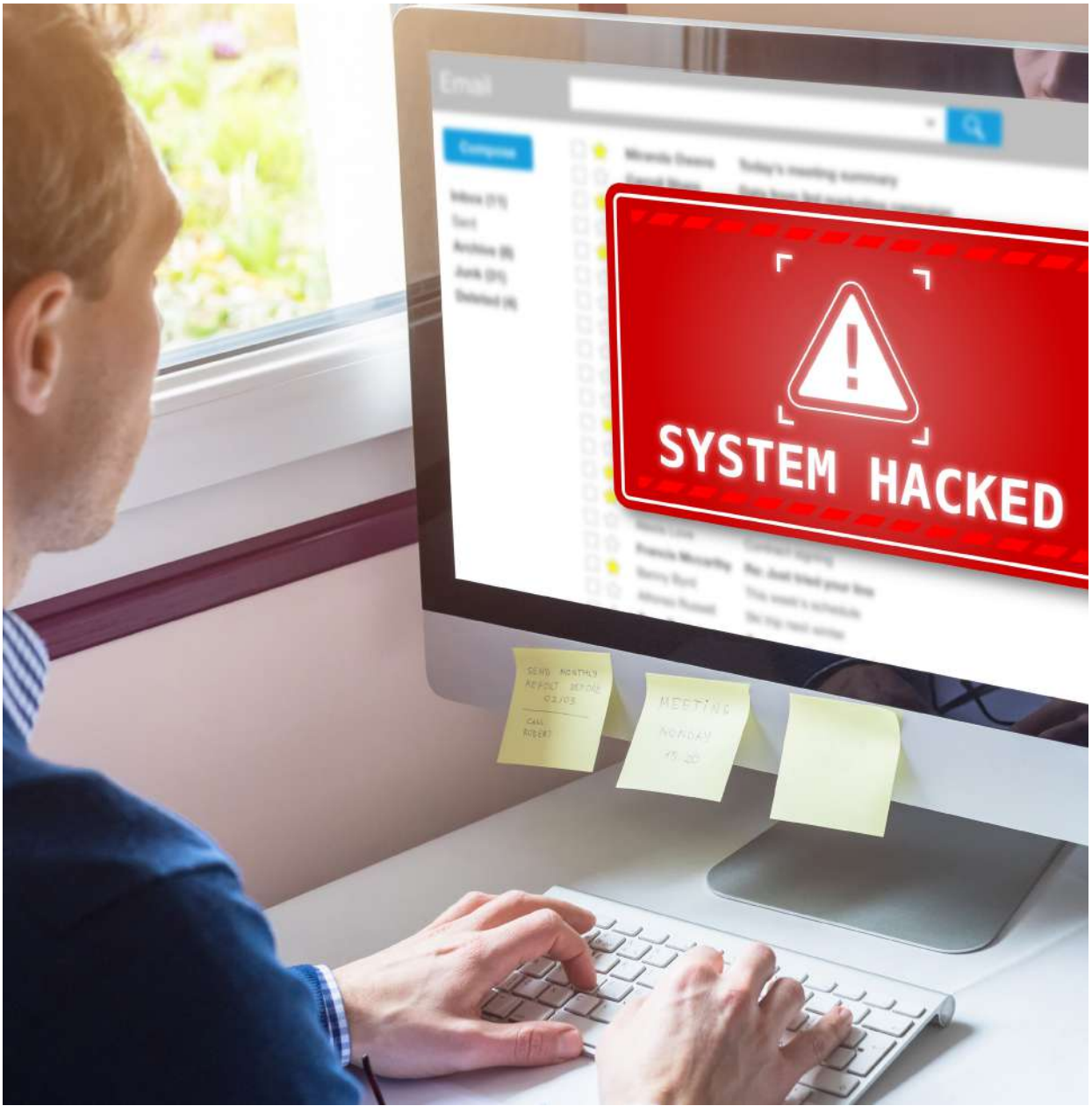
Le Ddos, Déni de service, vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé.

Les attaques man-in-middle : consistent à intercepter une conversation ou un transfert de données existant, soit en écoutant, soit en se faisant passer pour un participant légitime.

Les failles zéro-day, également orthographiée 0-day — ou faille / vulnérabilité du jour zéro est une vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. L'existence d'une telle faille sur un produit informatique implique qu'aucune protection n'existe, qu'elle soit palliative ou définitive

E | Conséquences de ces attaques

Les conséquences d'une attaque cyber peuvent être de différentes natures. Six entreprises sur dix ayant vécu une attaque ont ainsi été impactées sur leur business, principalement en raison d'une perturbation de la production (21%) ou par la compromission d'information (14%) (OpinioWay/CESIN). Deux entreprises sur cinq (41%) attaquées ont subi un détournement de paiement et parmi les entreprises françaises attaquées, 24% déclarent que leur solvabilité a été menacée (Rapport Hiscox 2022). *« Une entreprise sur deux qui ne paie pas la rançon réclamée par le cyber attaquant dépose le bilan dans les 18 mois suivant l'attaque »*, **rappelle ainsi Michel Van Den Berghe, Président de Campus Cyber**. Les pertes financières peuvent donc être directes ou indirectes. Les pertes directes sont dues au règlement de rançon et/ou d'amende à la suite de l'attaque, aux coûts liés à l'arrêt de l'exploitation et la gestion de crise, ou encore aux éventuels frais de notification de pertes de données…. Les pertes indirectes sont notamment liées aux conséquences de l'attaque cyber sur d'autres acteurs en raison des effets de contagions aggravés par les interdépendances numériques. *« Il convient également de ne pas négliger l'impact de ces attaques sur la réputation de l'entreprise,»* **poursuit Arthur Bataille CEO de Pr0ph3cy.** *« Même si ce n'est généralement pas l'objectif recherché par les cyberattaquants, il représente un risque important pour l'entreprise victime ».*



2 SE PROTÉGER CONTRE LE RISQUE CYBER

Au sein même des entreprises, différentes mesures sont à mettre en place pour prévenir autant que possible les cyberattaques. De différentes natures, ces dispositifs vont du simple « bon sens » à des outils sophistiqués, en passant par la formation, les assurances, et la mise en place de process. L'intensité de ces mesures dépend alors de l'exposition et de la sensibilité au risque des entreprises.

A | Prévenir le risque

Sensibiliser les collaborateurs

L'humain est le principal point d'entrée des cyberattaques. La prévention de ce risque passe donc nécessairement en premier lieu par la sensibilisation et la formation de l'ensemble des collaborateurs de l'entreprise. *« Cette sensibilisation de tous les collaborateurs, y compris ceux réalisant des activités sans lien avec le cyber, est même indispensable pour que l'ensemble des autres mesures de protection mises en place par l'entreprise fonctionne,»* **explique Yasmine Douadi, Directrice stratégie cybersécurité de Seela et Pr0ph3cy**. *« A partir du moment où l'employé a un accès ne serait-ce qu'à une toute petite partie du réseau de l'entreprise (comme une messagerie) alors il représente un potentiel point d'entrée pour une cyberattaque »*. Indispensable, cette sensibilisation des collaborateurs a d'ailleurs progressé depuis la crise sanitaire et le développement du télétravail. Selon l'enquête OpinionWay pour le CESIN, les mesures de sensibilisation au risque cyber des personnes en télétravail ont ainsi été renforcées pour 70% des entreprises interrogées.

« Cette sensibilisation passe en premier lieu par la diffusion d'informations auprès des collaborateurs, notamment sur les bonnes pratiques à adopter lorsqu'ils se connectent à Internet, ou pour protéger et sauvegarder ses données les plus sensibles,» **souligne Michel Van Den Berghe, Président de Campus Cyber**. *« Souvent, c'est une question de bon sens »*. Dans le cadre de cette démarche, les entreprises peuvent notamment se faire accompagner par le site Cybermalveillance.gouv.fr. *« Nous mettons à la disposition de nos publics de nombreux outils de sensibilisation tels que des guides, des kits, des vidéos pour les aider, à mieux comprendre et à faire face aux menaces»* **explique Jérôme Notin, Directeur général du GIP ACYMA cybermalveillance.gouv.fr**. *« Ces outils sont tous disponibles en licence Etablab2.0, de façon à ce que les organisations puissent s'approprier nos contenus et les personnaliser, afin de sensibiliser à leur tour leurs parties prenantes, être conscientes des risques encourus et sécuriser leurs équipements, tout en maîtrisant les réflexes et bonnes pratiques à adopter en matière de cybersécurité. »* Dans le cadre de cette sensibilisation, il convient également que l'entreprise réalise une veille régulière sur les différentes failles et techniques utilisées par les pirates afin de parer à toute éventualité d'attaque et construire ainsi une stratégie de sécurité la mieux adaptée aux enjeux du moment.

Assurer le risque cyber

L'assurance a également un rôle majeur à jouer dans la prévention et la prise en charge de ce risque. Elle permet aux différents acteurs de mieux l'anticiper et y répondre. En France, de nombreux assureurs du marché des risques d'entreprise proposent désormais une offre cyber. Ces garanties peuvent être intégrées dans des contrats classiques ou faire l'objet de contrats spécifiques. Dans le cadre de ces assurances, il convient néanmoins de veiller aux « exclusions » liées au risque cyber. *« Dans les assurances contre le risque cyber, il est recommandé de choisir un prestataire qui adapte le montant de sa prime à la totalité du risque auquel l'entreprise est exposée et qui n'exclut pas le remboursement de certaines prestations comme le coût de la remédiation et de la perte d'exploitation »*, **précise Jérôme Notin, Directeur général du GIP ACYMA cybermalveillance.gouv.fr.**

Questions à Jean Noël Barrot, Ministre délégué chargé de la Transition numérique et des Télécommunications

En quoi l'indemnisation des rançons et cyberattaques par les assureurs permet-elle de lutter efficacement contre le risque cyber ? N'y a-t-il pas un risque que ces assurances soient contre-productives ?

« La doctrine de l'Etat pour les sites publics est toujours la même : nous ne payons pas les rançons demandées par les cybercriminels et nous recommandons aux entreprises de ne pas le faire.

Par ailleurs, les entreprises doivent mieux se préparer au risque cyber et être accompagnées par des experts mais aussi par d'autres acteurs de proximité, dont les assureurs. En cas d'attaque, pouvoir compter sur une assistance fournie par l'assurance et voir ses frais de reconstruction du système informatique pris en charge par l'assurance peut être utile.

Nous ne laissons pas de côté la prévention qui est la clé pour lutter contre ce risque. Les assureurs ont leur rôle à jouer en sensibilisant leurs assurés, et notamment les PME.

La démarche de l'Etat est avant tout d'augmenter l'information et la prévention. Il s'agit donc surtout de renforcer les moyens à disposition des entreprises, en particulier les plus petites, qui, si elles ne sont pas protégées, peuvent voir leur activité anéantie.

Les assureurs sont un relais utile dans le cadre de cette démarche de sensibilisation. En effet, ils entretiennent un dialogue régulier avec les assurés sur la nature des risques couverts et peuvent devenir acteur de cette prévention nécessaire. »

B | Repenser les process de gestion des risques

La cartographie des risques cybers auxquels l'entreprise peut être exposée et qui diffèrent en fonction de sa taille et se son secteur d'activité est indispensable à l'entreprise pour ensuite mettre en place les bons process de gestion de crise ainsi que les bons outils de sécurisation de son système d'information. Dans le cadre de cette démarche, l'entreprise doit se pencher sur la criticité de ses données, mais également sur l'organisation de ses ressources humaines et de son écosystème

- **Identifier les données les plus critiques :** Certaines données doivent être impérativement protégées d'une attaque pour ne pas mettre en danger l'entreprise. « *Tout l'enjeu pour les entreprises consiste à trouver le juste équilibre entre l'intérêt qu'elle représente et les risques qu'elle peut prendre* » **précise Alain Juillet, Président d'Honneur de l'Académie de l'Intelligence Economique**. « *Il faut préserver ce qui est essentiel sans pour autant bloquer tous les échanges et le travail collaboratif.* » Dans le cadre de cette analyse, il convient également que les entreprises prennent en considération le cycle de vie de leurs données.
- **Se pencher sur les droits d'accès des individus :** Cette démarche est valable pour les données, mais aussi pour les individus. Un collaborateur peut entrer dans une entreprise et évoluer de manière transverse dans différents départements, gravir différents échelons hiérarchiques ou encore être amené à quitter l'entreprise. « *Sa consommation des services numériques évoluera donc en conséquence*», **poursuit Nicolas Arpagian, Directeur de la Stratégie en cybersécurité de Trend Micro Europe, Enseignant à l'Ecole Nationale Supérieure de la Police et à Science Po Saint Germain en Laye**.» *Il convient de faire un suivi de qui a accès à quoi, pour faire quoi. Même si l'exercice est exigeant, c'est une condition d'une connaissance précise des usages numériques au sein de l'organisation. Cela facilite la détection des pratiques problématiques et la traçabilité des opérations* ».
- **Placer l'entreprise au cœur de son écosystème :** La prévention du risque cyber nécessite également de prendre en compte l'ensemble des partenaires, fournisseurs et sous-traitants de l'entreprise. « *Il faut toujours considérer l'entreprise comme étant partie prenante d'une chaine numérique au sein d'un écosystème, en gardant à l'esprit que les attaquants visent en priorité les éléments les plus faiblement protégés* », **ajoute Nicolas Arpagian.**

Nicolas Arpagian,
Directeur de la Stratégie en cybersécurité de Trend Micro Europe, Enseignant à l'Ecole Nationale Supérieure de la Police et à Science Po Saint Germain en Laye.

> Pour se protéger, il convient de combiner les règles juridiques avec la technologie. Dans le cadre de cette démarche, l'entreprise doit fixer des critères de protection et d'engagement avec des qualifications des données, des procédures de réponses à incidents, la mise en place de systèmes de sauvegarde et de gestion des accès. Il lui faut également avoir une vision qui soit la plus claire possible de toutes interactions techniques tant en interne que vers l'externe. Et veiller à toutes les évolutions pouvant les concerner. Il est primordial d'adapter les environnements techniques en fonction des données, des individus et des organisations connectées au système d'information. Cela conditionne l'instauration d'une politique de cybersécurité, qui devra être évaluée et sera adaptée en fonction des évolutions opérationnelles et de la réglementation.

85%

DES ENTREPRISES ESTIMENT QUE LES SOLUTIONS PRÉSENTES SUR LE MARCHÉ DE PROTECTION SONT ADAPTÉES À LEURS BESOINS

C | Mettre en place des solutions technologiques pour se protéger

La protection contre les cyberattaques passe également par la mise en place de solutions technologiques adaptées à l'exposition au risque de l'entreprise. Selon l'étude Opinion Way/CESIN, 85% des entreprises estiment d'ailleurs que les solutions présentes sur le marché sont adaptées à leur entreprise. Le nombre moyen de solutions mises en place dans les entreprises (plus de 10) reste élevé. En tête de ces solutions se trouvent notamment le VPN (91%) et le proxy (81). L'étude souligne également l'importante progression des solutions d'EDR (Endpoint detection and response) (68%, +17%) et de chiffrement (56%/+7%). En termes de détection des attaques, les entreprises tendent également à s'équiper de SOC (Security Operation Center).

Alain Juillet,
Président d'Honneur de l'Académie de l'Intelligence Economique

> Le choix de ces défenses techniques dépend de la situation de l'entreprise. En fonction de son degré de criticité, elle peut mettre en place des systèmes de mots de passe sur les ordinateurs pour créer une barrière au niveau de l'outil. Elle peut également mettre en place une sécurité plus globale à l'extérieur de l'entreprise, par exemple en implantant des systèmes de blocage des attaques s'articulant autour de l'intelligence artificielle, au niveau global dans les SOC ou sur les terminaux individuels tels que les systèmes d'EDR ou de XDR (Détection et réponses attendues)

LEXIQUE

LES PRINCIPAUX DISPOSITIFS DE PROTECTION ET DÉTECTION LES PLUS SOUVENT MIS EN PLACE DANS LES ENTREPRISES

VPN (réseau privé virtuel) : système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics (et en particulier Internet).

Proxy et filtrage d'URL : passerelle qui sert d'intermédiaire entre un ordinateur et les sites web et services Internet utilisés. Elle intercepte et gère le trafic entre deux appareils, réseaux ou protocoles.

Passerelle de sécurité mail : dispositif ou logiciel utilisé pour surveiller les courriers électroniques envoyés et reçus. Cet outil a pour vocation de se protéger contre les courriers électroniques indésirables (spam, phishing, logiciels malveillants ou frauduleux…) et de délivrer les bons courriers électroniques.

Authentification multi-facteur (MFA) : méthode d'authentification dans laquelle l'utilisateur doit fournir au minimum deux facteurs de vérification pour accéder à une ressource de type application, compte en ligne ou VPN

Solution et/ou service de scan de vulnérabilité : analyse complète qui détecte les vulnérabilités grâce à un processus entièrement automatisé basé sur des failles de sécurité connues.

Système de gestion des logs (SIEM) : logiciel qui identifie et catégorise les incidents et événements, et les analyse. Il fournit des rapports sur les incidents et événements liés à la sécurité, tels que les connexions réussies ou non, les activités malveillantes.

EDR (Endpoint Detection Response) : technologie logicielle de détection des menaces de sécurité informatique des équipements numériques (ordinateurs, serveurs, tablettes, objets connectés, etc.)

XDR (Extended Detection and Response) : surveille les Endpoints, mais aussi les emails, serveurs et le Cloud. En augmentant les capacités de détection, le XDR permet une réaction rapide aux menaces, en amont de la kill chain, limitant nettement les dégâts. Le XDR surveille en continu et de manière proactive pour alerter rapidement en cas de suspicion d'attaque.

SOC (Security Operation Center) : le SOC est une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance.

3 MOBILISER ET FÉDÉRER AUTOUR DU RISQUE

Parallèlement aux différents dispositifs pouvant être mis en place dans les entreprises, la protection contre le risque cyber passe également par l'engagement et la mobilisation de tous, y compris l'état, autour de cet enjeu. Au-delà de la prise de conscience, il s'agit maintenant de fédérer les forces vives pour lutter efficacement contre le risque cyber.

A | La prise de conscience

Si de nombreuses actions peuvent être menées dans les entreprises, il convient néanmoins qu'elles soient pilotées par un véritable expert interne ou externe. C'est lui qui va nouer des liens et favoriser le partage des bonnes pratiques. *« Il faut créer de l'échange et instaurer une confiance entre les différents acteurs»*, **souligne Alain Juillet, Président d'Honneur de l'Académie de l'intelligence Economique.** *«Cela peut se faire au sein ou entre des clubs d'entreprises, des fédérations ou syndicats professionnels ou encore des associations. Ces différents liens doivent se construire et nous n'en sommes qu'aux balbutiements ». « Le gouvernement a un rôle de sensibilisation et d'information»*, **ajoute pour sa part Thibaut Lanxade Entrepreneur et Président-Directeur Général du Groupe Luminess**. *«Il lui revient notamment de renforcer la sécurisation des échanges, en légiférant (comme il l'a par exemple fait avec la réglementation à venir sur la facturation électronique obligatoire), en favorisant le Cloud Souverain ou encore en continuant d'investir dans la formation et la mise en place d'un écosystème pour lutter contre le risque cyber. »*

Une responsabilité dont convient d'ailleurs le gouvernement qui a initié plusieurs démarches en faveur de la lutte contre le risque cyber. *« La menace est réelle, se développe et surtout se standardise ce qui permet aux assaillants d'augmenter leur volume d'attaque,»* **déclare Jean-Noël Barrot, Ministre délégué chargé de la Transition numérique et des Télécommunications**. *«Face à ce constat, les particuliers, les entreprises et les administrations doivent être mieux armés. C'est le sens des actions que je mène sous l'autorité de Bruno Lemaire, Ministre de l'Economie et des Finances, pour les soutenir et pour que chacun adopte les bons gestes barrières en ligne ».*

B | Les actions

Réguler

La cybersécurité occupe une place à part dans le domaine des technologies de l'information. *« Elle est toute à la fois façonnée par des enjeux techniques, économiques, juridiques et géopolitiques avec une implication des intérêts stratégiques des Etats,»* **précise Nicolas Arpagian, Directeur de la Stratégie en cybersécurité de Trend Micro Europe, Enseignant à l'Ecole Nationale Supérieure de la Police et Science Po Saint Germain en Laye.** *« Ainsi des pays comme la Chine, les Etats-Unis et même la Russie peuvent s'appuyer sur leur écosystème national respectifs avec des acteurs de référence (BATX, GAFAM, Yandex, VKontakte…), tandis que l'Europe est davantage en situation de consommatrice de services conçus et pilotés à partir d'autres continents que le sien. Cela explique l'importance prise par la production normative de l'UE, avec des textes structurants comme le Règlement Général sur la Protection des Données (RGPD) ou encore les directives NIS sur la protection des opérateurs de services essentiels (OSE), pour maîtriser au maximum le déploiement de politiques de cybersécurité.»*

Pour agir sur la cybersécurité et assurer un niveau de sécurité suffisant des acteurs économiques, plusieurs réglementations ont ainsi été mises en œuvre au niveau Français et/ou Européen tels que la Loi Godfrain du 5 janvier 1988, le Cybersecurity Act, le Règlement Général sur la Protection des Données (RGPD), la Norme ISO/CEI 27001, le Règlement DORA, la Directive NIS2 et plus récemment le Visa SecNumCloud.

Fédérer

Au-delà des réglementations, le gouvernement entend également mobiliser les différents acteurs de l'écosystème économique pour mieux lutter contre le risque cyber. Une démarche qui passe par l'impulsion, la mise en place et puis le soutient d'organisations propres à accompagner les entreprises et collectivités dans la prévention et la gestion du risque cyber, mais également à former et développer des expertises autour de ce sujet.

> L'ANSSI

L'état œuvre ainsi au travers de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Service du Premier ministre, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. En qualité d'acteur majeur de la cyber sécurité, l'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

> Cybermalveillance.gouv.fr

En 2017, l'ANSSI et le ministère de l'Intérieur ont créé Cybermalveillance.gouv.fr, le dispositif national d'assistance aux victimes d'actes de cybermalveillance, de prévention et sensibilisation aux risques numériques et d'observation de la menace. *« Nous avons pour vocation d'accompagner les particuliers, les entreprises (hormis celles dont s'occupent l'ANSSI) et les collectivités territoriales »*, **Jérôme Notin, Directeur Général du GIP ACYMA cybermalveillance.gouv.fr.**

La mission consiste à assister les victimes d'actes de cybermalveillance, en assurant un service d'assistance en ligne et une mise en relation avec des professionnels en sécurité numérique référencés sur la plateforme. Le groupement a également pour vocation de prévenir les risques et de sensibiliser aux bonnes pratiques en sécurité numérique, avec la production de différents contenus, et à travers l'accompagnement à la sécurisation des systèmes d'information des publics professionnels par des prestataires labellisés ExpertCyber. Enfin, cybermalveillance.gouv.fr a pour rôle d'observer le risque notamment au travers de ce que remontent les prestataires et les victimes afin d'adapter en conséquence le contenu de ses outils de prévention ainsi que ses parcours d'accompagnement à la lutte contre le risque cyber.

Ce dispositif piloté par une instance de coordination, le Groupement d'intérêt Public (GIP) ACYMA, est composé d'une soixantaine de membres issus du secteur public, du privé et du domaine associatif, et qui contribuent chacun à sa mission d'intérêt général. « Gage de l'intérêt de ce partenariat public/privé, en cas d'incident de cybersécurité majeure, nous diffusons par exemple une « Alerte Cyber » auprès de nos membres (parmi lesquels MEDEF, CPME ,U2P et AMF), qui la relaient à leurs adhérents, poursuit Jérôme Notin. Ce dispositif a été lancé en 2021 par le secrétaire d'Etat Cédric O en 2022 et touche un potentiel de 3,5 millions d'organisations

> Campus Cyber

Plus récemment en 2021, le Président de la République Emmanuel Macron a initié le projet de Campus Cyber, qui consiste à rassembler en un lieu « totem » l'ensemble des acteurs nationaux et internationaux liés à la cyber sécurité. Le Campus Cyber s'articule également autour de forces vives issues aussi bien du privé que du public. *« Ce Campus est aujourd'hui porté par des acteurs privés et soutenu par l'état (40% de l'actionnariat), et rassemble désormais plus de 250 entités qui représentent l'ensemble de l'écosystème : banques, transports, sociétés spécialisées dans le risque cyber, start-up, organismes de formation, acteurs de la recherche et des associations »*, **précise Michel Van Den Berghe, Président du Campus Cyber.** *« Nous avons pour vocation de mettre en place des actions visant à fédérer la communauté de la cybersécurité et à développer des synergies entre ces différents acteurs : partage de bonnes pratiques, création de projets opérationnels… Notre rôle consiste également à promouvoir l'excellence française en matière de cybersécurité, en centralisant les talents et les acteurs du secteur dans un lieu commun autour de projets d'innovations. Nous hébergeons à ce titre un incubateur de jeunes entrepreneurs qui souhaitent développer un projet autour du risque cyber. Nous entendons également participer à la formation d'expert en sécurité et cyber sécurité et créer de l'attractivité autour de ces métiers ».*

C | La souveraineté numérique, une solution ?

Les technologies numériques prennent une importance croissante dans les activités de production, de gestion, de commercialisation et d'administration des entités privées et publiques. La question de la souveraineté technologique comme composante de la sécurité collective s'invite également dans le débat de la lutte contre le risque cyber. *« Cependant, il reste encore difficile de parler de souveraineté numérique en France voir même de l'envisager car pour le moment la France n'a pas réalisé la globalité des investissements nécessaires à sa mise en place, notamment en termes de recherches et formation,»* **précise Alain Juillet Président d'Honneur de l'Académie de l'Intelligence Economique**. *Certaines technologies ou outils existent malgré tout et proposent les contours d'une souveraineté numérique partielle. C'est notamment le cas pour certaines solutions EDR ou XRD. De même, OVH travaille actuellement au développement d'un Cloud Souverain. Il faudrait néanmoins investir bien davantage»*. D'autre part, le principe de souveraineté numérique reste assez éloigné des préoccupations actuelles des entreprises qui jonglent au quotidien avec des problématiques commerciales, financières, fiscales, juridiques, sociales ou encore technologiques. *« C'est la raison pour laquelle les entreprises du privé lui préfèrent le principe d'autonomie, qui désigne la faculté d'agir librement,»* **précise Nicolas Arpagian**. *«Elles ont à cet effet besoin de comprendre le fonctionnement des technologies qu'elles achètent et ce qui est fait des données exploitées par ces applications ».*

Pour répondre à ce double enjeu et tendre vers la souveraineté numérique, il faudrait donc favoriser l'émergence de solutions technologiques propres à limiter autant que possible le risque cyber mais aussi le développement de compétences et d'expertises capables de concevoir ces technologies de lutte contre les cyberattaques et d'accompagner les entreprises en la matière. *« Il devient donc urgent de miser sur la formation, initiale et continue, pour élargir le nombre et l'origine des talents qui peuvent s'exercer dans le domaine de la cybersécurité,»* **poursuit Nicolas Arpagian.** *« Cette expertise est indispensable pour assurer la souveraineté à laquelle les démocraties aspirent ».*

Malgré ces différents dispositifs et investissement l'état ne peut et ne pourra pas tout. *« Il revient également aux éditeurs, consultants, conseillers et autres sociétés de service d'accompagner les entreprises,»* **conclut Thibault Lanxade, Entrepreneur et Président-Directeur Général du Groupe Luminess** *« Ce rôle de pédagogie et de sensibilisation des entreprises revient également aux Chambres de Commerce et d'Industrie et aux Chambres des métiers, aux organisations patronales, experts comptables, commissaires aux comptes et avocats ».*

Questions à Jean Noël Barrot, Ministre délégué chargé de la Transition numérique et des Télécommunications

Quelle est la feuille de route du Gouvernement concernant la lutte contre le risque cyber ?

Face à la cybercriminalité qui évolue, je veux garantir la cybersécurité du quotidien. J'ai annoncé récemment, pour l'année 2023, une enveloppe de 30 millions d'euros pour des actions de sécurisation. Ces actions comprennent plusieurs volets qui couvrent tous les Français.

Pour les entreprises, nous allons réaliser une campagne massive de communication, en lien avec cybermalveillance.gouv.fr, pour inciter les entreprises à s'inscrire dans une démarche de cybersécurité. De plus, un outil d'auto diagnostic, gratuit, en ligne et de référence sera créé pour permettre à toutes les entreprises de connaitre leur niveau de protection et les premières mesures à mener. Enfin, pour 750 PME et ETI, issues des secteurs stratégiques visés par la directive NIS2, le Gouvernement mettra en place un bouclier cyber avec une phase d'évaluation et d'audit puis la mise en œuvre de solutions de sécurité.

Vous renforcez également vos actions aux côtés des collectivités ?

Pour les collectivités, nous prolongerons les parcours de cybersécurité en les renforçant pour 125 des 950 collectivités qui ont déjà bénéficié du plan 2021-2022 et en permettant à 50 nouvelles collectivités de commencer ce programme. En août 2022, j'avais annoncé, avec l'accord de la Première ministre, une enveloppe supplémentaire de 20 millions d'euros dédiée spécifiquement aux hôpitaux. Au total, fin 2023, ce sont plus de 1 000 collectivités et administrations qui auront suivi ce programme.

De plus, pour toutes les communes et y compris les plus petites, une plateforme de services mutualisés sera créée. Il s'agit d'un outil clé en main, sur la base d'un abonnement, via lequel l'État proposera notamment aux collectivités de bénéficier d'un nom de domaine, d'une messagerie et de services en ligne sécurisés.

Et pour les particuliers ?

Pour les particuliers, conformément à l'engagement du Président de la République, le filtre anti-arnaque sera mis en place en version bêta à l'été 2023 avant d'être généralisé à l'été 2024. Simple, facultatif et gratuit, il sera basé sur l'analyse de la menace cyber en temps réel et permettra d'avertir les internautes (web et mobile) en filtrant préventivement les adresses web malveillantes.

Enfin, nous développerons également le cyberscore. Fruit des travaux parlementaires, il certifiera les plateformes numériques destinées au grand public. Déployé d'ici la fin 2023, il permettra aux internautes d'avoir une idée générale du niveau de sécurité des sites qu'ils fréquentent en majorité, à l'image du Nutri-score pour les produits alimentaires.

CONCLUSION

Si les entreprises et collectivités commencent à mesurer les dangers des cyberattaques et que le gouvernement renforce ses dispositifs d'accompagnement, des efforts restent à faire pour lutter efficacement et durablement contre ce risque immatériel. Une démarche qui ne pourra se faire qu'en fédérant et en mobilisant le plus grand nombre autour de cet enjeu.

D'autre part, le meilleur bouclier contre ce fléau reste la connaissance et la maitrise des risques et des solutions propres à le prévenir voire à l'éradiquer. C'est la raison pour laquelle nombre d'intervenants à ce guide ont pointé l'urgence de former et de développer de nouvelles expertises pour favoriser la conception de stratégies et de solutions de cyber sécurité. Une démarche qui passera certes par des investissements mais aussi par l'innovation, que ce soit en termes de méthodes d'apprentissage ou de contenu des formations relatives à ce sujet.

Les professionnels de la sécurité, les universitaires et chercheurs, mais également l'état, les entreprises et les organismes et fédérations professionnelles doivent donc continuer à se mobiliser ensemble pour faire émerger les solutions et expertises nécessaires à la lutte contre le risque cyber.

Etymologiquement le lieu des « échanges » – Place Escange est l'endroit privilégié, regroupant acteurs publics et acteurs privés, pour mener une réflexion prospective sur la prise en compte et l'évolution du capital immatériel des entreprises.

Place Escange est soutenu par la Fédération Nationale de l'Information d'Entreprise, de la Gestion de Créances et de l'Enquête Civile.

www.place-escange.fr
@PlaceEscange
@place-escange
Contact : sbouchindhomme@figec.com

www.place-escange.fr