Vol. 4, N°16, pp. 267– 292, DECEMBRE 2025

ISSN : 1987-1465
DOI : https://doi.org/10.62197/BMKA8247
Indexation : Copernicus, CrossRef, Mir@bel, Sudoc, ASCI, Zenodo
Email : RevueKurukanFuga2021@gmail.com
Site : https://revue-kurukanfuga.net

La Revue Africaine des Lettres, des Sciences Humaines et Sociales ***KURUKAN FUGA***

ROLE DU CONTROLE DE GESTION DANS LA PREVENTION DE L'ESPIONNAGE INDUSTRIEL

Dr Oumar FANE, Enseignant-chercheur, ENETP, Université de Kindia-fanos41@yahoo.fr

Mme Fanta DIOUBATE,Enseignant-chercheur, Université de Kindia- massadan91@gmail.com

M. Mamoudou DIAKITE, Enseignant-chercheur, Université de Kindia-mamoudoudiakite988@gmail.com

Dr Mamadou Saidou DIALLO, Enseignant-chercheur, Université de Kindia-mamadiallo19@gmail.com

Résumé : Rares sont les travaux qui portent sur le traitement de l'espionnage industriel dans les entreprises. Dans un contexte économique mondialisé et rudement compétitif, l'espionnage industriel constitue une menace majeure pour les organisations et entreprises. Cet article explore le rôle que la fonction contrôle de gestion pourrait jouer dans la prévention et la lutte contre l'espionnage industriel. En mobilisant des concepts théoriques et des cas pratiques d'entreprises, nous proposons un système de contrôle de l'espionnage industriel qui met en synergie les outils de gestion des risques et de sécurité organisationnelle. Nos résultats montrent que le contrôle de gestion peut contribuer à la protection des acquis stratégiques et à la réduction des vulnérabilités internes.
Mots-clés : Contrôle de gestion - Espionnage industriel - Rôle - Système de contrôle.

****

Abstract : Few studies focus on the treatment of industrial espionage in companies. In a globalized and fiercely competitive economic context, industrial espionage constitutes a major threat for organizations and companies. This article explores the role that the management control function could play in preventing and combating industrial espionage. By mobilizing theoretical concepts and practical business cases, we propose an industrial espionage control system which synergizes risk management and organizational security tools .Our results show that management control can contribute to the protection of strategic assets and the reduction of internal vulnerabilities.
Mots clés: Control system - Industrial espionage - Management control - Role

INTRODUCTION

La croissance des cybermenaces et de l'espionnage industriel dans un monde interconnecté interpelle les chercheurs à se pencher sur ces menaces dans le dessein d'apporter des solutions pouvant les endiguer, voire les éradiquer. De nos jours, plusieurs problèmes accablent les organisations, mais l'espionnage industriel occupe de plus en plus une place grandissante. Optimiser les performances économiques est devenu le défi de toutes les organisations actuelles, tant privées que publiques. Cependant, plusieurs moyens d'y parvenir ne respectent pas les réglementations légales et éthiques de la société. Le comble est de constater le développement et la propagation de ces moyens répréhensibles dépourvus d'éthique et de légalité. Les nombreuses affaires d'espionnage industriel des dernières décennies démontrent l'ascension du phénomène dans le monde des entreprises. Faisant l'objet de la guerre économique, qui impliquait plusieurs Etats dans la recherche de renseignements, l'espionnage industriel a été une pratique très utilisée dans le cadre de la compétition sur un marché globalisé. Actuellement, l'espionnage industriel est devenu le moyen illégal et dépourvu d'éthique le plus utilisé par les espions pour dérober des informations pertinentes, confidentielles, secrètes dans les entreprises. Or, il est à noter que les informations occupent dorénavant une place cruciale dans les économies et entreprises. Elles procurent un avantage incontesté à son détenteur, surtout si ces informations englobent des secrets industriels, secrets commerciaux, etc. Nous considérons l'espionnage de l'entreprise vers la concurrence comme une activité déloyale dépourvue de légalité et d'éthique. C'est justement pour lutter contre ce type d'espionnage que nous nous intéressons au cas de l'entreprise victime à ce que cette dernière puisse parfaire sa sécurité dans un registre de « compétitivité loyale ».

Les conséquences de l'espionnage industriel sont catastrophiques, allant des pertes de sommes colossales à la faillite de certaines entreprises (Fané et Feige 2019, 2021). Plusieurs études corroborent cela, notamment l'OCDE (2014) qui affirme que lorsque leurs secrets commerciaux sont compromis, les entreprises s'exposent à des pertes potentielles, notamment de leur réputation mais aussi de leurs avantages concurrentiels. La Commission européenne relève qu'une entreprise sur cinq a été victime d'au moins une tentative de violation de ses secrets d'affaires au cours des dix dernières années et une sur quatre aurait signalé un vol d'informations en 2013 contre 18 % en 2012 (Commission européenne, 2013). Selon le rapport de Frantz (2014), le taux de 20% correspond au pourcentage d'entreprises européennes déclarant avoir subi une violation de leurs secrets d'affaires au cours des 10 dernières années. Indéniablement, l'espionnage industriel ébranle l'entreprise qui en est victime, provoquant une

perte d'activité plus ou moins grande. Les répercussions, qu'elles soient commerciales ou financières, sont toujours très importantes et peuvent aller jusqu'à nuire à la survie de l'entreprise. Pour les entreprises, une question importante est celle des pratiques, outils et processus pour se prémunir efficacement du risque industriel. La question de la dynamique se pose également puisque le risque évolue. Une des fonctions de l'entreprise qui permet de contrôler et de prévenir les actions est le contrôle de gestion. Si les fonctions IT et juridiques jouent un rôle clé dans la gestion de ces menaces, la fonction contrôle de gestion reste sous-exploitée dans ce domaine. Cet article examine comment le contrôle de gestion peut devenir un acteur central dans la mise en place d'un système de contrôle efficace pour prévenir l'espionnage industriel. Ce qui justifie notre problématique, à savoir : comment le contrôle de gestion peut-il contribuer à la prévention et à la lutte contre l'espionnage industriel ?

Ainsi les objectifs de cet article sont d'explorer le rôle de la fonction contrôle de gestion dans le contrôle des risques liés à l'espionnage industriel, et de proposer un système de contrôle intégré basé sur les outils du contrôle de gestion. Quant à la méthodologie employée, nous avons opté pour une analyse théorique et une revue de cas pratiques.

Dans notre développement, nous présentons une revue de la littérature et un cadre théorique dans le point (1) ; la méthodologie et les résultats sont évoqués dans le point (2) ; et nous terminons par une analyse, une discussion et une proposition d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion dans le point (3).

1. Revue de la littérature et cadre théorique

Cette partie est consacrée à la mise en lumière de notre revue de littérature et de notre cadre théorique. Nous exposons les caractéristiques de l'espionnage industriel, tout en évoquant le lien avec le contrôle de gestion et le contrôle interne. Nous terminons par la présentation du cadrage théorique.

1.1. Définitions de l'espionnage industriel :

L'espionnage industriel a sémantiquement connu de nombreuses définitions. De façon générale, le centre national de ressources textuelles et lexicales (2024)[i] définit l'espionnage comme une « *action de recueillir clandestinement des renseignements au profit d'une puissance étrangère* ». L'espionnage industriel est défini, selon Payne (1971), comme l'homme ou la femme qui d'une manière clandestine, s'approprie des renseignements confidentiels et les revend à l'insu de leurs propriétaires. En procédant ainsi, l'espion agit contre les intérêts du

propriétaire, lui dérobant la propriété de son travail, de ses recherches et de son avance technique pour faire bénéficier quelqu'un d'autre. Selon Baud (1998) l'espionnage « *désigne une opération clandestine de collecte de renseignement* ». D'après Crane (2005), l'espionnage industriel est essentiellement « *une forme de collecte de renseignements commerciaux, habituellement, mais pas exclusivement, de la part des concurrents de l'industrie* ». A l'instar de Bulinge (2013), l'espionnage consiste à pénétrer ou violer l'espace cryptique afin de s'approprier les secrets qui y sont échangés. En tant qu'activité humaine très ancienne et courante, il n'est pas l'apanage des Etats, même si le droit public et international en verrouille la pratique justifiée par la notion de raison d'Etat. Le franchissement des lignes juridiques est généralement considéré comme une profanation à laquelle on associe la perfidie et la trahison, conséquence logique d'une sacralisation du secret.

En analysant ces différentes définitions, l'espionnage industriel consisterait à l'expropriation de certains « éléments » par des moyens répréhensibles (en termes de légalité et d'éthique). Il semble se caractériser par : la collecte d'informations ou de renseignements ou de secrets ; l'acte est effectué de façon clandestine ; l'acte est effectué par une personne physique ou morale ; les moyens de collecte sont illégaux ; le processus de collecte est contraire à l'éthique ; etc.

1.2. Typologie de l'espionnage industriel

Les méthodes de collecte des informations dans le cadre de l'espionnage industriel évoluent d'une manière exponentielle. A la lecture des articles de presse et de certains écrits scientifiques, la chasse au renseignement se dirigerait en priorité vers les grandes manufactures, les laboratoires et centres de recherche scientifique, mais aussi vers les administrations. L'espionnage industriel est une activité humaine pratiquée, soit par les Etats et leurs services secrets de renseignement : c'est l'espionnage d'Etat ou interne ; soit par les entreprises elles-mêmes contre d'autres entreprises nationales ou étrangères : c'est l'espionnage privé ou externe.

Les moyens utilisés par les espions sont multiples et diversifiés. Ces moyens se sont multipliés à la suite de l'essor des nouvelles technologies. Une entité, qui souhaite se procurer des informations sensibles de ses concurrents, possède plusieurs méthodes : elle a la possibilité d'engager des anciens employés des services secrets, mettre en place sa propre équipe de renseignement ou encore recourir aux services des experts spécialisés dans la collecte d'informations sensibles.

L'évolution de l'espionnage industriel se caractérise également par la naissance d'un nombre croissant d'entités privées qui rivalisent avec les services de renseignement étatiques. Ces différentes entités se sont gangrenées sous des apparences diverses, mais en toute légalité.

Nous pouvons retenir notamment les sociétés de détectives, les entreprises de consulting, les cabinets d'audit, les cabinets de conseil… Ces exemples ne veulent nullement dire que ces types de sociétés sont forcément des entités se livrant aux pratiques de collecte d'informations privées. C'est juste pour signifier quelques types de sociétés, qui ont fait l'objet des accusations d'espionnage industriel.

Par ailleurs, les pratiques de collecte d'informations employées sont le plus souvent dépourvues d'éthique et non conformes aux législations en vigueur. Selon Noailly (1997), la démarche des espions est progressive. Dans un premier temps, les espions s'intéressent aux informations publiques ou ouvertes. Ensuite, ils vont s'intéresser aux informations les plus confidentielles de l'entreprise. A ce stade, les méthodes de collecte ne tombent pas toutes sous le coup de la loi, mais elles ne respectent pas la plupart du temps les principes de l'éthique. Enfin, pour obtenir un secret ou un renseignement ou une information confidentielle, les espions pénètrent dans plusieurs services fermés de l'entreprise. Par conséquent, ils utilisent des moyens illégaux, comme les visites organisées avec des caméras cachées, le piratage informatique, les écoutes téléphoniques, la corruption du personnel interne… Les collaborateurs de recherche ou les stagiaires peuvent également servir de moyen d'intrusion dans les entreprises.

Pour Domingo (2014), la première méthode utilisée consiste à collecter des informations publiques accessibles au public ; la deuxième méthode a trait aux conditions favorables pour attirer des centres de recherche et développement étrangers ; troisièmement, les organisations de transfert de technologie implantées dans un pays étranger comme méthode de collecte d'informations exclusives ; la quatrième méthode est l'éducation à l'étranger ; la cinquième méthode et la plus agressive est l'espionnage, notamment l'approche traditionnelle « mille grains de sable », le cyber, etc.

Les visites d'entreprise constituent une pratique privilégiée par certains espions. Ces visites sont structurées et permettent de cerner les systèmes de gestion, l'agencement des manufactures, les protocoles de sécurité… Les informations ouvertes ou publiques vont orienter les axes d'une recherche approfondie vers des informations confidentielles de l'entreprise.

Un autre moyen agressif de collecte d'informations est l'absorption de l'entreprise ciblée par le rachat pur et simple ou la prise de contrôle. Ainsi, toutes les informations sécrètes deviennent

des informations accessibles, puisque les espions en sont désormais les propriétaires. Les petites et moyennes entreprises sont généralement les plus ciblées par ce genre d'espionnage industriel. Memheld (2012) donne l'exemple des « risques de diffusion non contrôlée » lors d'une fusion acquisition ou lors de la mise en place d'une entreprise commune (joint-venture). Selon Crane (2005), les tactiques douteuses peuvent prendre de nombreuses formes, allant des pratiques clairement illégales, telles que pénétrer par effraction dans les locaux d'un concurrent pour dérober des informations confidentielles, ou installer des dispositifs électroniques (micro, caméra, etc.), ou contacter les concurrents sous un faux nom, etc.

Ces nombreux moyens de collecte d'informations se multiplient au fur et à mesure que les nouvelles technologies évoluent. En résumé, les outils et méthodes de collecte des informations utilisés par les espions sont indénombrables et ont plusieurs formes. Ils ont un caractère imprévisible que les organisations doivent maîtriser par un système de gestion interactif.

1.3. Enjeux économiques et stratégiques pour les entreprises.

L'espionnage industriel est un fléau qui touche toutes les entreprises, même si certaines d'entre elles ne se sentent pas concernées pour diverses raisons, notamment à cause du type d'activités qu'elles mènent. Plusieurs entreprises sous-estiment l'espionnage industriel en comptant sur les barrières d'entrée, qui constituent selon elles une dissuasion pour les espions. D'autres estiment qu'elles n'ont pas des informations sensibles à protéger, or les simples listes de clients ou de fournisseurs constituent des informations sensibles susceptibles d'intéresser les espions.

Parmi les nombreux cas d'espionnage industriel illustrant ses conséquences néfastes sur les entreprises, nous pouvons retenir les illustrations suivantes. En France, la Direction de la Surveillance du Territoire a évalué les coûts de l'espionnage industriel à 10 milliards de francs par an[ii]. D'autres experts quadruplent ce chiffre, car celui-ci ne fait pas état des activités des sociétés privées. Selon Crane (2005), des problèmes d'intérêt public peuvent surgir lorsque l'information recueillie, par le biais de l'espionnage industriel, est utilisée à des fins comme un comportement anticoncurrentiel, y compris l'élimination délibérée ou la ruine de concurrents, la hausse des prix ou l'enracinement d'une position monopolistique. En conséquence de l'espionnage industriel, le public peut souffrir de l'augmentation des prix et de la baisse de l'innovation à long terme. D'après une étude de Rotman-Telus réalisée au Canada auprès de plus de 500 entreprises, les brèches informatiques auraient augmenté de 29 % en 2010, pour un coût moyen unitaire estimé à environ 450 000 €. Quant au secteur public, l'augmentation serait

de l'ordre de 74 %. Ce qui peut logiquement justifier certains montants astronomiques (Nséké, 2012).

Dans leur ouvrage « *Secrets stolen, fortunes lost : preventing intellectual property theft and economic espionage in the 21st Century* », les chercheurs américains Burgess et Power (2011) donnent des pistes intéressantes sur le manque à gagner aux États-Unis. Citant des chiffres du Département américain du Commerce, on évalue à 250 milliards de dollars par an les coûts de l'espionnage économique et du piratage électronique pour les entreprises.

Selon le rapport de Frantz (2014), le taux de 20% correspond au pourcentage d'entreprises européennes déclarant avoir subi une violation de leurs secrets d'affaires au cours des 10 dernières années.

Les différents gouvernements émettent en permanence des rapports et des études chiffrant approximativement les coûts exorbitants de l'espionnage industriel sur les économies et les entreprises. Nous pouvons citer, notamment le rapport de Frantz (2014) sur la protection des secrets d'affaires dans l'Union Européenne, selon lequel le coût annuel de l'espionnage industriel supporté par les entreprises allemandes se situe entre 20 et 50 milliards d'euros.

Les milieux politiques sont muets pour éviter des conflits diplomatiques. Les milieux économiques, eux aussi, restent muets devant l'espionnage industriel. Beaucoup préfèrent garder le silence pour ne pas nuire à leur image ou par peur de devoir détailler les preuves (et donc de dévoiler la nature des éléments dérobés). Si des affaires éclatent, la justice n'est utilisée qu'en dernier recours. Les sanctions imposées aux victimes couvrent rarement le préjudice subi par la victime.

Nous pouvons remarquer que les conséquences de l'espionnage industriel touchent aussi bien les Etats et les organismes internationaux que les entreprises privées. L'espionnage industriel est un phénomène transversal, dans le sens qu'il n'épargne aucune entité (publique ou privée). La taille de l'entreprise ne constitue pas un motif d'exclusion, car ce sont souvent les petites entreprises qui sont les plus ciblées. Cela peut s'expliquer par l'absence des moyens de protection industrielle (brevet, droit d'auteur, etc.) ou parce qu'elles sont facilement absorbables, etc. L'espionnage industriel reste une pratique très dangereuse que les entreprises doivent reconsidérer et par conséquent mettre en œuvre toutes les possibilités de gestion, afin d'éviter ses lourdes conséquences.

1.4. Contrôle de gestion : relations entre le système de contrôle et la stratégie dans une organisation

Les travaux de Simons sont d'une importance considérable et demeurent un cadre de repère incontournable dans la discipline du contrôle de gestion. Simons s'est intéressé aux relations existantes entre le système de contrôle et la stratégie dans une organisation.

Simons (1994) identifie quatre variables clés, qui doivent être analysées et appréhendées pour que la mise en œuvre d'une stratégie soit une réussite. Il s'agit : des valeurs fondamentales (core values) ; des risques à éviter (risks to be avoided) ; des variables critiques de la performance (critical performance variables) ; des incertitudes stratégiques (strategic uncertainties). Pour Simons, chaque variable clé est contrôlée individuellement au travers d'un système de contrôle qu'il nomme « levier de contrôle ». Ainsi, il définit un levier de contrôle pour chaque variable clé.

Les variables clés (valeurs fondamentales, risques à éviter, variables critiques de la performance, et incertitudes stratégiques) correspondent respectivement aux systèmes de contrôle ou leviers de contrôle suivants : systèmes de croyances, systèmes de contraintes, systèmes de contrôle diagnostic, et systèmes de contrôle interactif.

Pour Lepori et Bollecker (2015), les systèmes de contrôle de Simons se caractérisent par :

- Le système de croyances : l'entreprise connaît des incertitudes stratégiques qu'elle va limiter en communiquant sur les valeurs et les missions de l'organisation. Ces éléments contribuent à alimenter la fierté d'appartenance. Il s'agit pour Simons d'un contrôle positif par l'inspiration.

- Le système de contraintes où les règles du jeu sont précisées : des barrières sont établies afin d'identifier les risques à éviter, avec des sanctions en cas de franchissements. Il s'agit pour Simons d'un contrôle négatif par la contrainte.

- Le système de contrôle diagnostic s'apparente au contrôle de gestion classique. Il vise à décliner la stratégie par la définition d'objectifs à atteindre, en mobilisant le couple moyens/résultats sur les facteurs clés de succès, en définissant des variables critiques de performance pour opérationnaliser le pilotage.

- Le système de contrôle interactif vise à favoriser les discussions et remontées d'informations provenant du terrain afin de maîtriser l'incertitude stratégique, faire émerger de nouvelles stratégies et favoriser l'apprentissage. Il s'apparente au contrôle stratégique.

Simons regroupe ensuite les différents leviers de contrôle en deux catégories, selon qu'il s'agisse d'encadrer la stratégie (correspondant aux systèmes de croyances et aux systèmes de contraintes), ou de formuler et de mettre en œuvre la stratégie (correspondant aux systèmes de contrôle diagnostic et aux systèmes de contrôle interactif).

Il a aussi classifié les quatre systèmes de contrôle, d'une part dans un cadre de recherche d'opportunités et d'apprentissage correspondant aux systèmes de croyances et aux systèmes de contrôle interactif ; d'autre part dans un cadre de vigilance et d'attention correspondant aux systèmes de contraintes et aux systèmes de contrôle diagnostic.

Par ailleurs, l'auteur affirme que le contrôle de gestion traditionnel se cadre généralement dans un système de contrôle diagnostic, même si certains auteurs l'imputent dans le cadre des leviers de contrôle diagnostic et interactif, passant du levier de contrôle diagnostic au levier de contrôle interactif (Tuomela, 2005), ou l'inverse (Essid et Berland, 2011).

Avant de confronter l'espionnage industriel au contrôle de gestion, il est important d'évoquer le contrôle interne qui contient plusieurs moyens de protection techniques pour la gestion des risques d'espionnage.

1.5. Contrôle interne et gestion des risques d'espionnage

Il est important de reconnaître les efforts des différents gouvernements et organismes internationaux qui ont introduit des points de départ considérables dans la lutte contre l'espionnage industriel, au travers des réglementations, des textes de loi, etc. Cependant, ces textes de loi et autres s'avèrent insuffisants dans les différents pays pour couvrir les risques d'espionnage.

Le code de la propriété intellectuelle en France a mis en œuvre des moyens de protection dissuasifs tels que les brevets, les marques, les modèles, etc. Ces instruments présentent certaines limites et s'avèrent insuffisants pour répondre à l'ensemble des besoins de sécurité de l'entreprise. Les protections juridiques contribuent à la maitrise de l'espionnage industriel, mais elles ne permettent pas de cerner l'ensemble des actes d'espionnage industriel. Selon le rapport de Frantz (2014), il apparaît que la protection juridique des secrets d'affaires dans l'Union Européenne est à ce jour fragmentée et insuffisante (63% des entreprises déclarent que le niveau de protection juridique des secrets d'affaires est faible dans sa globalité). Ce cadre légal est très vite contourné par les espions et ne peut permettre aux victimes d'engager une poursuite (Winkler, 1996).

D'autres auteurs (Noailly, 1997 et Crane, 2005), mentionnent les vides juridiques. En illustration nous avons : des éléments non couverts par nature (comme les simples idées, les simples présentations d'information, les méthodes intellectuelles ou encore les programmes d'ordinateurs, etc.) ; en plus de la protection légale non-exhaustive ne couvrant que certains éléments du patrimoine informationnel des entreprises, il arrive également que les entreprises souhaitent échapper aux contraintes liées à certains modes de protection.

Comme illustration, certaines entreprises ont du mal à assurer toutes les procédures qui s'attachent à la souscription des droits de propriété industrielle (en effet, les brevets peuvent contenir jusqu'à 80% de la technologie de l'invention, la rendre publique c'est donc mettre directement ses concurrents sur des pistes de recherche) ; un autre inconvénient demeure le coût du brevet ; etc. Les mesures de protection de la propriété intellectuelle sont certes nombreuses, mais elles présentent le plus souvent des contraintes lourdes, qui poussent les entreprises à y renoncer. Les études scientifiques mettent unanimement en exergue les limites de cette protection juridique.

Pour donner suite à ces défaillances législatives, les entreprises se voient contraintes de prendre le relais afin d'affronter elles-mêmes l'espionnage industriel (Samli et Jacobs, 2003). La protection assurée par les entreprises elles-mêmes n'est plus une option, elle est nécessairement importante et complémentaire à la protection juridique. La conciliation des deux types de protection pourrait permettre aux entreprises de mieux appréhender l'espionnage industriel. Cette autonomie se traduit par le contrôle organisationnel des entreprises contre l'espionnage industriel, notamment le contrôle interne.

Par ailleurs, rares sont les entreprises qui mettent en place une stratégie de protection contre l'espionnage industriel, comme l'illustrent Samli et Jacobs (2003). Comment peut-on expliquer ce comportement des entreprises ? Est-ce par méconnaissance ou par négligence de l'espionnage industriel ?

Un élément d'explication peut faire référence aux barrières à l'entrée que constituent la technologie et la spécificité d'un produit, qui rendent soit trop coûteux ou inimitable le procédé ou le processus de production de l'entreprise qui en bénéficie.

Par définition, le contrôle interne est un processus mis en place par le conseil d'administration, le management et les collaborateurs d'une entité, afin de maîtriser raisonnablement les risques empêchant l'atteinte des objectifs stratégiques. Il peut être en amont (contrôle de prévention) ou en aval (contrôle de détection). Pour le référentiel COSO[iii] , il répond à trois objectifs : un

objectif d'efficacité des opérations, un objectif de fiabilité des informations financières et un objectif de conformité à la loi. C'est un ensemble de dispositifs stratégiques contribuant à la maîtrise des risques pour faciliter l'atteinte des objectifs stratégiques, pouvant faire intervenir plusieurs fonctions de l'entreprise comme le contrôle de gestion, la finance, les ressources humaines, le système d'information, etc. Le recours à ces différentes fonctions s'explique par leurs aptitudes particulières, comme leur savoir-faire ou leur expertise dans l'appréhension de certains types de risques. Par exemple, la fonction contrôle de gestion comporte une panoplie d'outils de budgétisation, d'outils de pilotage, d'outils d'évaluation des coûts, etc.

En résumé, c'est un dispositif global qui ne peut être restreint à la seule définition des procédures, à la séparation des tâches, etc. Le contrôle interne s'adapte à chaque entité et peut utiliser les dispositifs des autres fonctions de l'entreprise pour atteindre ses objectifs. Les insuffisances juridiques de l'appréhension de l'espionnage industriel ont conduit les entreprises à mettre en place des mesures de protection et de discipline internes permettant de contrer l'espionnage industriel.

Plusieurs procédures, outils et méthodes internes sont définis pour fortifier la protection des informations sensibles, afin de dissuader les espions. Des normes internationales existent à cet effet pour réconforter la protection des informations de l'entreprise, nous pouvons citer la norme ISO/IEC 27001 (« ISO » Organisation internationale de normalisation et « IEC » la Commission électrotechnique internationale) sur le système de management de la sécurité de l'information, la norme ISO/CEI 27002 sur la sécurité de l'information, etc.

A l'essor des nouvelles technologies, un des outils les plus utilisés par les espions demeure l'ensemble des outils informatiques qui sont généralement connectés. A cet effet, des mesures de protection ont été élaborées par l'Etat pour combattre cette catégorie de crime qui s'intitule la « cybercriminalité ».

La cybercriminalité peut se définir comme toute action illégale dans laquelle un ordinateur est l'instrument ou l'objet du délit. Elle est définie comme toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet.

Elle englobe trois types d'infractions : les infractions spécifiques aux technologies de l'information et de la communication, comme les traitements non autorisés de données personnelles, les infractions aux cartes bancaires, etc. ; les infractions liées aux technologies de l'information et de la communication, comme la pédopornographie, l'incitation au terrorisme

et à la haine raciale sur internet, etc. ; les infractions facilitées par les technologies de l'information et de la communication comme les escroqueries en ligne, le blanchiment d'argent, la contrefaçon ou toute autre violation de propriété intellectuelle.

Les différents outils et méthodes de protection techniques semblent théoriquement adaptés et efficaces. Des auteurs (Noailly, 1997 ; Samli et Jacobs, 2003 ; Memheld, 2012) dénombrent des limites comme les dangers de l'artillerie sécuritaire, les coûts de la protection, la nécessité de concilier protection et climat social…

Nous en déduisons que la protection assurée par les entreprises elles-mêmes consiste en une mobilisation des outils et méthodes de gestion avec une forte implication du personnel. Il est indéniable de reconnaitre que ces outils et méthodes de protection techniques contre l'espionnage industriel demeureront efficaces, s'ils sont bien utilisés et s'il y a une bonne conciliation protection et climat social de l'entreprise (Memheld, 2012).

1.6. Espionnage industriel et contrôle de gestion

Le contrôle de gestion est généralement associé à la gestion des performances et à l'optimisation des ressources. Cependant, son rôle dans la prévention des risques, notamment en matière de sécurité, reste à développer. Les outils de contrôle, tels que les indicateurs de performance, offrent un potentiel inexploitable pour identifier les vulnérabilités. Le Contrôle de gestion permettrait de cerner l'ensemble des étapes de contrôle de l'espionnage industriel (en amont, en cours et en aval), à savoir : la définition des objectifs de protection et de prévention contre l'espionnage industriel ; une planification opérationnelle desdits objectifs au travers des budgets et autres outils de planification ; la mise en œuvre et le suivi des actions opérationnelles, afin d'alerter l'entreprise à travers les outils de pilotage (comme le tableau de bord, etc.) ; et la post-évaluation afin d'évaluer les coûts de l'espionnage industriel au travers des méthodes d'évaluation des coûts, d'appréhender ses sources, etc.

Le lien entre le contrôle des ressources, la protection des données et la performance constitue une opportunité d'intégrer des outils de détection et de prévention dans les pratiques de contrôle de gestion. Le contrôle des ressources désigne la capacité d'une organisation à gérer, optimiser et sécuriser ses acquis stratégiques, qu'ils soient financiers, humains, technologiques ou informationnels (brevets, savoir-faire, relations clients, données internes, etc.). La protection des données, en particulier des données sensibles, est une composante essentielle du contrôle des ressources. Une gestion rigoureuse des ressources stratégiques permet de minimiser les pertes dues à des intrusions externes ou des dysfonctionnements internes, garantissant ainsi une

continuité opérationnelle. La protection des données n'est pas seulement une obligation légale (comme le respect du RGPD en Europe), mais également un facteur clé de performance. Une entreprise qui protège efficacement ses données évite les interruptions d'activité causées par des cyberattaques. La sécurité des données renforce la confiance des parties prenantes, notamment les clients, les actionnaires, etc. Les incidents de sécurité peuvent engendrer des coûts importants : pertes financières, impact sur la réputation, etc. Une stratégie de protection proactive limiterait ces risques financiers. Les entreprises qui protègent leurs données de recherche et développement conservent un avantage stratégique, ce qui se traduit par une meilleure performance sur le marché. Un contrôle efficace des ressources est une condition nécessaire à la performance durable d'une organisation.

Le contrôle de gestion aide à allouer les ressources de manière optimale, en surveillant les budgets, en ajustant les priorités et en éliminant les inefficiences. La surveillance des processus critiques empêche la perte ou le détournement de ressources stratégiques. Les tableaux de bord et leurs indicateurs de performance, utilisés dans le cadre du contrôle de gestion, permettent d'aligner les objectifs de l'organisation avec ses capacités réelles. La convergence entre le contrôle des ressources et la performance repose sur une gestion transparente et une réactivité face aux éventuelles dérives.

Le lien entre le contrôle des ressources, la protection des données et la performance peut être visualisé comme un cycle. Le contrôle des ressources renforce la protection des données, en identifiant et en limitant les points de vulnérabilité. La protection des données soutient la performance, en garantissant la sécurité des acquis stratégiques et la pérennité des activités. Une performance accrue permet de réinvestir dans des systèmes de contrôle et de sécurité toujours plus efficaces, revenant ainsi au point de départ.

En résumé, une entreprise performante est celle qui intègre la gestion de ses acquis stratégiques et la protection de ses données dans une approche globale. Ces dimensions ne doivent pas être perçues comme des objectifs à part, mais comme des composants interdépendants d'un système organisationnel.

1.7. Cadre Théorique

Dans notre cadrage théorique, nous avons mobilisé deux théories sous-jacentes qui permettent de comprendre notre objet de recherche. La première est la théorie des ressources. Selon Prévot, Brulhart et Guieu (2010), « *l'approche par les ressources trouve son origine en 1984 avec l'article fondateur de Wernerfelt (1984), mais elle revendique des sources plus anciennes en*

référence aux travaux de Penrose (1959) ». Il s'agit sans aucun doute de l'approche fondamentale, qui est la plus diffusée et qui constitue l'origine des autres courants. Cette théorie stipule que les ressources stratégiques d'une organisation / entreprise (dans notre cas, les brevets, le savoir-faire, les données sensibles, etc.) doivent être protégées pour garantir un avantage concurrentiel durable. Or, l'objectif de cet article de recherche est de savoir comment le contrôle de gestion peut-il contribuer à la prévention et à la lutte contre l'espionnage industriel ?

La deuxième théorie mobilisée est la théorie de l'agence. Selon Tajer et *al.* (2022), la théorie de l'agence « *trouve son origine dans l'article publié en 1976 dans le journal of financial economics de Jensen et Meckling* ». La séparation entre le contrôle et la propriété dans les entreprises constitue l'origine de la théorie d'agence. Cette théorie étudie d'une manière distincte les rapprochements entre les agents économiques, ainsi que l'analyse de la relation qui lie un mandant « le principal » et un mandataire « l'agent » (Jensen et Meckling, 1976). La théorie de l'agence a été largement étudiée par Jensen et Meckling (1976). Ces auteurs définissent la relation d'agence comme étant « *un contrat dans lequel une (ou plusieurs) personne (s) a recours aux services d'une autre personne pour accomplir en son nom une tâche quelconque, ce qui implique une délégation décisionnelle à l'agent* ». La vision de cette théorie montre également, que les managers sont censés maximiser leurs intérêts en termes de richesse et d'avantages financiers. Le contrôle amené sur le comportement des dirigeants est assuré par différents systèmes disciplinaires à savoir, la structure de propriété, la politique de rémunération, le conseil d'administration, la politique financière et d'autres (Jensen et Meckling, 1976).

De notre point de vue, elle met en évidence les risques liés à l'asymétrie d'information entre les employeurs et les employés. L'alignement des objectifs pourrait réduire les comportements opportunistes susceptibles de faciliter l'espionnage industriel. Il est donc indispensable de tenir compte de l'ensemble du personnel d'une organisation / entreprise quels que soient les outils du contrôle de gestion qui seront mobilisés pour prévenir et empêcher la survenance de l'espionnage industriel.

Ces deux théories cadrent notre objet de recherche dans le sens où il est question de protéger des ressources stratégiques, à savoir les informations, les secrets, les brevets, les données sensibles, etc. (théorie des ressources), afin de permettre l'alignement des intérêts entre employeurs et employés pour réduire les risques (théorie de l'agence).

2. Méthodologie et résultats

Nous justifions dans cette partie notre démarche méthodologique et les sources des données. Ensuite, nous présentons les résultats qui ont fait l'objet d'une analyse et d'une discussion. Nous terminons par la proposition d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

2.1. Sources des données

Nous nous inscrivons dans une démarche qualitative. Elle a pour finalité de tenir compte des éléments empiriques permettant l'élaboration de notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Selon Thietart *et al.* (2014), :

> *« toute recherche repose sur une certaine conception de son objet de connaissance ; utilise des méthodes de nature variée (expérimentale, historique, discursive, statistique…) reposant sur des critères de validité spécifiques ; avance des résultats visant à expliquer, prédire, prescrire, comprendre ou encore construire et transformer le monde auquel elle s'adresse. »*

Notre question de recherche, portant sur l'élaboration d'un système de contrôle de l'espionnage industriel, est le résultat d'itérations entre théorie et cas pratiques d'entreprises. Dans le cadre de cette recherche, nous avons opté pour une analyse exploratoire basée sur une revue documentaire et des cas pratiques d'entreprises. Cela se justifie par la nature occulte de la pratique d'espionnage industriel. En effet, les organisations et entreprises ne communiquent leurs affaires d'espionnage industriel sauf si elles sont obligées. C'est ce qui justifie notre choix de récolter des données issues des cas pratiques d'espionnage industriel des publications académiques et professionnelles au travers des cas d'entreprises ayant été victimes d'espionnage industriel.

2.2. Cas pratiques d'entreprises ayant été victimes d'espionnage industriel

Nous nous sommes intéressés à 10 grands cas pratiques d'entreprises ayant été victimes d'espionnage industriel. Nous mettons en exergue pour chaque cas le contexte et le mode opératoire.

Tableau 1

Contextes et modes opératoires de 10 grands cas pratiques d'espionnage industriel

Cas	Contexte	Mode opératoire	Source
Cas Renault (France, 2011)	Renault, un des leaders mondiaux de l'automobile, a découvert une fuite	Utilisation d'un réseau interne de collaborateurs recrutés pour divulguer des informations.	Laroche, H., & Théron, C. (2016). Managers et espions :

	d'informations confidentielles relatives à ses programmes de véhicules électriques, une technologie stratégique pour son avenir.	Les données ont été transmises à des tiers via des outils numériques non sécurisés.	L'affaire Renault. *Revue française de gestion*, (1), 37-51.
Cas Huawei et T-Mobile (États-Unis, 2014)	Huawei a été accusé d'avoir tenté de voler des informations liées à un robot de test développé par T-Mobile USA.	Les ingénieurs de Huawei ont accédé au laboratoire de T-Mobile et ont photographié les composants du robot "Tappy". Ils ont également emporté illégalement une pièce du robot pour en analyser le fonctionnement.	Corcoral, M. (2022). Le droit comme outil diplomatique : le cas de l'offensive américaine contre Huawei. *Raisons politiques*, *85*(1), 101-116.
Cas Coca-Cola (États-Unis, 2006)	Une employée a tenté de vendre des secrets commerciaux de Coca-Cola, y compris des échantillons de produits, à son concurrent PepsiCo.	L'employée a volé des documents confidentiels et des échantillons dans les laboratoires de Coca-Cola. Elle a contacté PepsiCo pour leur proposer ces informations, mais PepsiCo a informé Coca-Cola et les autorités.	Asseman, A. (2009). Vol et fuites de données.
Cas Nortel Networks (Canada, années 2000)	Nortel, ancien géant des télécommunications, a été victime d'une cyberattaque prolongée par des acteurs malveillants étrangers.	Les pirates ont accédé aux courriels, rapports stratégiques et informations techniques pendant près de dix ans, contribuant à l'effondrement de l'entreprise.	Radio-Canada[iv] (2012)
Cas Volkswagen et General Motors (Allemagne/États-Unis, 1993)	Volkswagen a été accusé d'avoir recruté des cadres de General Motors qui ont apporté avec eux des milliers de documents confidentiels.	Recrutement d'anciens cadres de son concurrent pour accéder aux informations sensibles.	Le monde (1993)[v]
Cas ASML (Pays-Bas, 2019)	ASML, un fabricant néerlandais, a été victime d'un vol de propriété intellectuelle par des anciens employés liés à une entreprise chinoise.	Vol par des employés.	Les échos (2019)[vi]
Cas Concorde (années 1960-1970)	Le Concorde, avion supersonique développé conjointement par la France et le Royaume-Uni, était une prouesse technologique de l'époque. Des espions soviétiques ont obtenu des documents détaillant la construction du Concorde, permettant à l'URSS de développer le Tupolev Tu-144, un avion similaire.	16 février 1965 : Sergueï Pavlov, directeur du bureau parisien de la compagnie soviétique Aeroflot, est sommé de quitter la France. En sa possession sont retrouvés les plans du train d'atterrissage, des freins et de la cellule du Concorde.	Ambrose, A. (2023). Ecole de guerre économique.[vii]
Cas Autolib' (2013)	Le groupe Bolloré, opérateur du service Autolib', a été victime d'espionnage industriel.	Des informations confidentielles sur les batteries électriques ont été dérobées, compromettant la compétitivité de l'entreprise.	Figaro (2013)[viii].

Cas Gillette (1997)	Gillette a révélé que des employés avaient transmis des informations sur de nouveaux produits à la concurrence.	Les employés ont envoyé des courriels contenant des secrets commerciaux à des entreprises rivales	Los Angeles Times.[ix]
Cas IBM versus Hitachi (1982)	IBM a accusé Hitachi de voler des secrets concernant la technologie des ordinateurs centraux.	Deux des employés de Hitachi se sont fait prendre pour espionnage sur IBM.	Léveillée, M., & Coggins, M. F. (2019). L'effet de contagion des événements médiatiques liés aux fraudes financières sur le risque des entreprises (Doctoral dissertation, Université de Sherbrooke).

3. Analyse, discussion et proposition d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion

Les illustrations issues des 10 cas pratiques d'entreprises nous enseignent plusieurs éléments. Comme évoqué dans la revue de la littérature et le cadrage théorique, l'humain est au cœur des pratiques d'espionnage industriel (Noailly, 1997 ; Domingo, 2014 ; Memheld, 2012 ; Crane, 2005). Les 10 cas pratiques le confirment majoritairement à travers le mode opératoire impliquant le personnel interne de l'organisation / entreprise. D'autres méthodes sont également constatées à travers les 10 cas pratiques, comme l'intrusion des personnes externes de l'organisation / entreprise, le recours à la technologie, aux courriels, aux rapports stratégiques, aux outils numériques, etc. Domingo (2014), Memheld (2012) et Crane (2005) ont mis l'accent sur la diversité des méthodes de collecte d'informations afférentes à la technologie et l'évolution rapide desdites méthodes.

Partant de notre cadre théorique, le contrôle de gestion peut être un recours pour surveiller des processus critiques comme le contrôle des flux d'information et l'évaluation des risques liés aux accès non autorisés. Il peut également permettre l'optimisation des systèmes de reporting, en identifiant des anomalies dans les données comptables ou opérationnelles et en auditant des écarts significatifs. En intégrant de façon stratégique les préoccupations liées à la lutte contre l'espionnage industriel, le contrôle de gestion peut jouer un rôle dans la sensibilisation et la formation, en promouvant la sécurité organisationnelle via des outils de contrôle et en définissant des indicateurs extra-financiers sur la formation des collaborateurs et sur les risques liés à la divulgation d'informations.

L'espionnage industriel est une pratique extrêmement difficile à cerner, malgré l'existence des textes de loi, des réglementations, des méthodes de protection propres aux organisations et entreprises. Cependant, il est indéniable de reconnaitre l'existence de cet ensemble de pratiques protectrices déjà cadrées empêchant la survenance de l'espionnage industriel. Même si une bonne partie des pratiques d'espionnage industriel échappent à leur périmètre. Ce qui constitue un ensemble de pratiques qui se déploient dans des champs d'action non maitrisés nécessitant une adaptation rapide et permanente des organisations et entreprises.

A cet effet, il est pertinent de s'intéresser aux définitions des deux cas de figures de Acquier (2008), parce qu'elles permettent d'expliquer les deux cas de figures ci-haut. Pour Acquier (2008, p.16), les figures imposées désignent :

> *« un ensemble de pratiques qui se déploient dans des champs d'action déjà cadrés, du point de vue social et technique. Elles s'appliquent de manière transversale à l'ensemble des acteurs d'un secteur donné et sont structurées par l'existence de règles, de standards ou de normes ; et les figures libres constituent un espace potentiel d'innovation environnemental, social mais aussi managérial et politique. Elles constituent un ensemble de pratiques qui se déploient dans des champs d'action controversés, en cours de construction et moins cadrés, à la fois d'un point de vue technique et social. Par son action dans le domaine des figures libres, l'entreprise peut participer aux processus de cadrages techniques et sociaux qui vont structurer de nouveaux champs d'action. »*

Une première qualifiée « de conformité » c'est-à-dire des figures imposées et une seconde « d'opportunité » visant les figures libres.

Dans le même ordre d'idée, Antheaume (2013) affirme que la gestion de figures imposées implique de mettre en place des outils de gestion de projet ainsi que de contrôle de conformité des actions et des résultats ; tandis que la gestion de figures libres implique de mettre en place des outils de gestion dans une optique d'apprentissage organisationnel, de manière à informer les dirigeants sur le sens à donner à leur stratégie en fonction des informations que font remonter les outils.

Dans cette optique, nous pouvons statuer le processus de contrôle de l'espionnage industriel, en termes de figures imposées et ou de figures libres. Le processus de contrôle de l'espionnage industriel contient logiquement des figures imposées, si l'on se réfère aux différentes réglementations et protections juridiques et techniques, allant des règles à respecter aux lois légiférées dans certains pays. Ce sont des règles et des normes légitimes, qui peuvent être propres aux entités, sectorielles, nationales ou parfois internationales, permettant aux organisations d'anticiper la survenance de l'espionnage industriel et d'engager des poursuites

vis-à-vis des espions, dans le cas où elles seront victimes. Ces réglementations peuvent être appliquées dans toutes les organisations et constituent des variables critiques de la performance contrôlables, comme exemples nous pouvons citer notamment, la norme internationale ISO 27001 sur les bonnes pratiques pour la gestion de la sécurité des informations, les clauses de contrat, les contrôles d'accès physiques et informatiques, les clauses de confidentialité, la formation des employés sur la prévention de l'espionnage industriel, la fréquence de sensibilisation des employés, la fréquence des mises à jour des logiciels anti-espionnage, etc.

Cependant, le processus de contrôle de l'espionnage industriel semble se caractériser aussi par d'autres éléments n'entrant pas dans le cadre des figures imposées. Nous avons déjà évoqué l'incapacité de ces protections et normes juridiques, quant à l'appréhension exhaustive de l'espionnage industriel. Nonobstant toutes ces dispositions, les espions demeurent imprévisibles, surtout à l'essor du progrès technologique. Les organisations ont beaucoup de difficultés à prévoir les méthodes et les actions des espions et doivent, par conséquent, rester aux aguets en permanence. Ainsi, toutes ces incertitudes s'apparentent aux figures libres, qui se caractérisent par des champs d'action controversés (en cours de construction et moins structurés).

En rapprochant les 4 systèmes de contrôle de Simons (1994) évoqués dans la revue de littérature, le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion semble se caractériser par des variables d'incertitudes stratégiques (notamment des difficultés de prévision des méthodes et actions des espions, de l'imprévisibilité des espions, de l'évolution technologique, etc.), et des variables critiques de la performance (en faisant référence à la conformité des actions et des résultats vis-à-vis d'un référentiel technique interne, des normes sur la prévention contre l'espionnage industriel, etc.). Caractérisé par des figures imposées et des figures libres, le processus de contrôle de l'espionnage industriel pourrait être appréhendé par les leviers de contrôle diagnostic et interactif. La grille d'analyse des deux leviers de contrôle de Renaud (2013) met en exergue leurs caractéristiques.

Tableau 2

La grille d'analyse des leviers de contrôle diagnostic et interactif de Renaud (2013).

Caractéristiques	Contrôle diagnostic	Contrôle interactif
Objectifs	Décliner la stratégie délibérée en permettant de fixer des objectifs, de mesurer des résultats et de corriger les écarts	Gérer les incertitudes stratégiques, favoriser l'apprentissage organisationnel et l'émergence de nouvelles stratégies
Rôle des dirigeants	Intervention limitée à la fixation des objectifs et à la résolution de problèmes imprévus ou complexes	Implication personnelle et fréquente à tous les niveaux de l'organisation

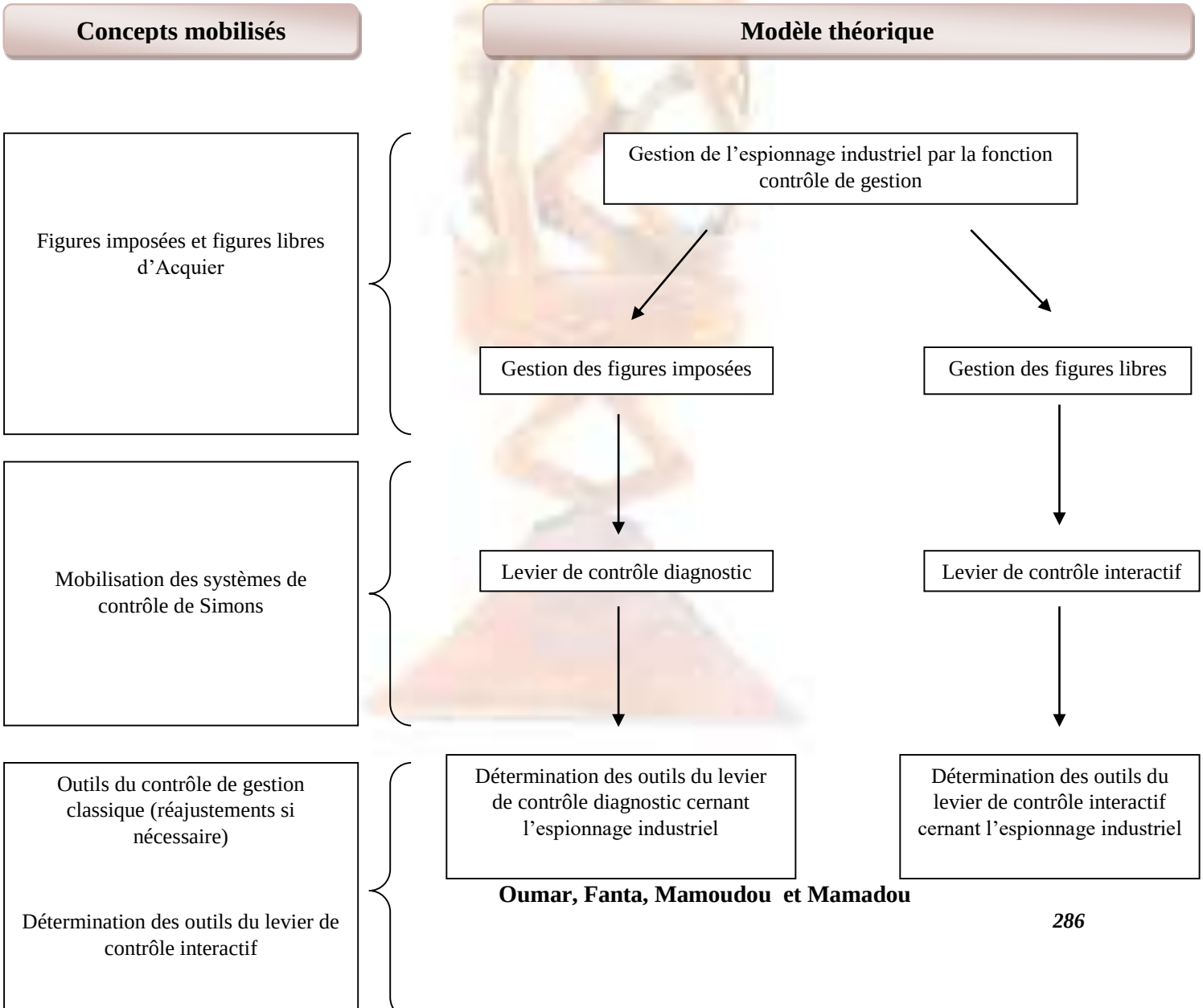
Rôle des fonctionnels	Rôle central dans la préparation et l'interprétation de l'information : construire et maintenir le système, interpréter les données, préparer les rapports concernant les exceptions, s'assurer de l'intégrité et de la fiabilité du système	Rôle limité dans la préparation et l'interprétation des résultats : collecter, compiler les données, faciliter le processus interactif
Processus de transmission des informations	Procédures formelles de *reporting*	Réunions hebdomadaires ou mensuelles, débats et dialogues fréquents
Fréquence d'interaction entre les acteurs	Ponctuelle, exceptionnelle	Répétitive, continuelle
Indexation de la rémunération sur l'atteinte des objectifs	Forte	Faible
Glissement dans l'utilisation avec le temps (du diagnostic vers l'interactif et inversement)	Oui/non	Oui/non

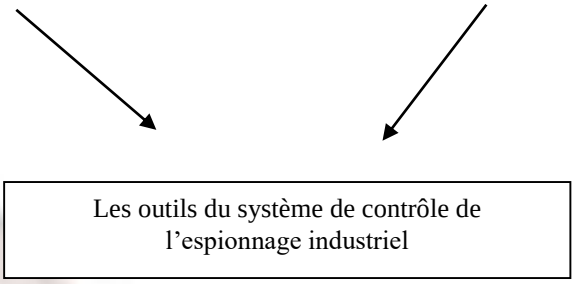
Source : Renaud (2013).

En résumé de tout ce qui précède, nous pouvons schématiser le modèle (qui s'inspire des travaux de Fané et Feige 2019, 2021) comme suit :

Figure 1

Système de contrôle de l'espionnage industriel par la fonction contrôle de gestion





Comme forces, le contrôle de gestion adopte une approche systématique offrant une perspective globale liée à la performance et intégrant des outils analytiques avec une vision transversale sur l'ensemble des actions de l'organisation / entreprise. En termes de limites, la fonction contrôle de gestion aura besoin de compétences spécifiques (notamment en cybersécurité et sur les pratiques très changeantes des espions) et les coûts pourraient être élevés pour certaines catégories d'organisations / entreprises (les PME par exemple).

Cependant, la réussite de la fonction contrôle de gestion dans l'appréhension de l'espionnage industriel nécessiterait la prise en compte de plusieurs aspects, notamment une bonne intégration des outils de contrôle de gestion et de cybersécurité, la collaboration entre les contrôleurs de gestion et les autres responsables (contrôleurs internes, responsables des systèmes d'information, etc.), l'évaluation de la conformité aux normes internes, etc.

Conclusion

L'espionnage industriel constitue une menace sérieuse pour les organisations et entreprises dans un contexte de rude concurrence et de mondialisation des marchés. Cet article a démontré que la fonction contrôle de gestion peut jouer un rôle déterminant dans la prévention et la gestion des risques d'espionnage. En intégrant des mécanismes de surveillance, des indicateurs de performance adaptés et des outils d'analyse des vulnérabilités, le contrôle de gestion peut dépasser son rôle classique pour devenir un acteur majeur dans la protection des acquis stratégiques. Ainsi, nous avons pu démontrer, à travers les travaux de Simons (1994), Acquier (2008), Antheaume (2013), Renaud (2013), que le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion se caractérise par l'appréhension des figures imposées et des figures libres, et pourrait, par conséquent, se faire théoriquement via les leviers de contrôle diagnostic et interactif. De ce fait, l'étape suivante va consister à réadapter les outils classiques du contrôle de gestion pour cerner l'espionnage industriel (côté diagnostic) et à

déterminer les outils appréhendant les incertitudes stratégiques liées à l'espionnage industriel (côté interactif).

Les contributions majeures de la fonction contrôle de gestion dans la lutte contre l'espionnage industriel incluent la gestion des acquis stratégiques en les cartographiant de façon dynamique afin de les identifier et les protéger (théorie des ressources). Par ailleurs, le suivi et l'analyse des performances au travers de la détermination des indicateurs de performance qui permettront de détecter des anomalies dans les processus et les comportements pour un meilleur alignement stratégique des intérêts entre employeurs et employés pour réduire les risques (théorie de l'agence). Cependant, la collaboration avec d'autres fonctions de l'organisation et de l'entreprise est indispensable pour favoriser une approche intégrée et proactive.

Les résultats de cette recherche mettent également en exergue des défis incontournables dus à la complexité progressive des menaces, la rapide évolution des technologies et la nécessité d'une sensibilisation renforcée au sein des organisations et entreprises. Il ressort que la lutte contre l'espionnage industriel requiert non seulement des outils techniques sophistiqués et des processus internes cadrés (système de contrôle diagnostic). Cependant, une culture organisationnelle forte axée sur la vigilance et la résilience est nécessaire pour une adaptation aux évolutions du contexte technologique et économique, en intégrant les nouvelles pratiques de gouvernance et les innovations en matière de cybersécurité (système de contrôle interactif).

Pour les futurs travaux, il serait opportun d'approfondir les recherches pour non seulement explorer des solutions technologiques avancées, mais aussi de mener des études empiriques approfondies pour déterminer davantage l'apport de la fonction contrôle de gestion dans la prévention et la gestion de l'espionnage industriel.

Bibliographie

Acquier, Aurélien. (2008, May). « Développement durable et management stratégique : piloter un processus de transformation de la valeur. » In *Actes du colloque de l'AIMS*.

Antheaume, Nicolas. (2013). « Le contrôle de gestion environnemental. État des lieux, état de l'art. » *Comptabilité-Contrôle-Audit.* 19 (3) : 9-34.

Baud, Jacques. (1998). *Encyclopédie du renseignement et des services secrets*. Lavauzelle.

Bulinge, Franck. (2013). *Intelligence économique : l'information au cœur de l'entreprise* (p. 320). Nuvis-CIGREF.

Commission européenne (2013). « La Commission propose des règles pour la protection du secret d'affaires. » http://europa.eu/rapid/press-release_IP-13-1176_fr.htm?locale=fr, novembre.

Corcoral, Mark. (2022). « Le droit comme outil diplomatique : le cas de l'offensive américaine contre Huawei. » *Raisons politiques*, *85*(1), 101-116.

Coskun, Samli, A. & Jacobs, Laurence. (2003). « Counteracting global industrial espionage: a damage control strategy. » *Business and Society Review*, 108(1), 95-113.

Crane, Andrew. (2005). « In the company of spies: when competitive intelligence gathering becomes industrial espionage. » *Business Horizons*, 48(3), 233-240.

Domingo, Francis, C. (2014). « Chinese industrial espionage: technology acquisition and military modernization. » *Philippine Political Science Journal*, 35 (2), 281-283.

Essid, Moez, & Berland, Nicolas. (2011). « Les impacts de la RSE sur les systèmes de contrôle. » *Comptabilité-contrôle-audit*, *17*(2), 59-88.

Fané, Oumar, & Feige, Jimmy. (2019). « Espionnage industriel : protections, outils de gestion et perspectives ? » *Question (s) de management*, 23(1), 89-102.

Fané, Oumar, & Feige, Jimmy. (2021). « Proposition d'un nouveau cadre d'analyse de la gestion de l'espionnage industriel. » *ACCRA*, 1, 39-56.

Frantz, Jérôme. (2014). « La protection des secrets d'affaires dans l'Union européenne. » Observations de la CCI Paris-Ile-de-France sur la proposition de directive sur la protection des savoir-faire et des informations commerciales non divulgués contre l'obtention, l'utilisation et la divulgation illicites, rapport au nom de la Commission du droit de l'entreprise et avec la collaboration de l'IRPI, 41 p. https://data.over-blog-kiwi.com/0/12/22/11/20180401/ob_0bc8bc_protection-secrets-affaires-rapport-fr.pdf.

Guarnieri, Franck, & Przyswa, Eric. (2009). « Cybercriminalité-contrefaçon : les interactions entre « réel et virtuel ». » *Revue internationale de droit économique*, *23*(1).

Jensen, Michael, C. & Meckling, William, H. (1976). « Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. » *Journal of Financial Economics*, vol.3, pp 305-360.

Laroche, Hervé, & Théron, Christelle (2016). « Managers et espions : L'affaire Renault. » *Revue française de gestion*, (1), 37-51.

Lepori, Elvia, Bollecker, Marc. (2015). « Les leviers de contrôle de SIMONS : vers une compréhension des freins à l'équilibrage diagnostic/interactif. » In : *Comptabilité, Contrôle et Audit des invisibles, del'informel et de l'imprévisible*.

Memheld, Pierre. (2012). « Intelligence économique, déontologie, conformité et anticipation des risques. » *Revue Internationale d'Intelligence Économique*, 4(2), 125-137.

Noailly, Joelle. (1997). *L'espionnage industriel au cœur de la guerre mondiale du renseignement économique*, Mémoire de maîtrise, Université Lyon 2.

Nobre, Thierry & Zawadski, Cindy. (2015). « Une lecture des leviers de contrôle de Simons par la théorie de la structuration en contexte ETI. » In : *Comptabilité, Contrôle et Audit des invisibles, de l'informel et de l'imprévisible*.

Nseke, Léopold. (2012). « Espionnage industriel : Des coûts importants. Afrique Expansion Magazine. » *Revue des affaires et des partenariats Nord-Sud*. https://afriqueexpansionmag.com/.

OCDE (2014). « Approaches of protection of undisclosed information (trade secrets). » http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=TAD/TC/WP(2013)21/FINAL&docLanguage=En.

Payne, Harold, J. (1971). « Model of freeway traffic and control. » in G.A. Bekey, *Mathematical Model of Public System*, Virginie: Simulation Councils, 51-61.

Penrose, Edith, Tilton. (2009). *The Theory of the Growth of the Firm*. Oxford university press.

Power, Richard & Burgess, Christopher. (2011). *Secrets stolen, fortunes lost: Preventing intellectual property theft and economic espionage in the 21st century*. Syngress.

Prévot, Frédéric, Brulhart, Franck, & Guieu, Gilles. (2010). « Perspectives fondées sur les ressources. » *Revue française de gestion*, *204*(5), 87-103.

Renaud, Angèle. (2013). « L'articulation des usages diagnostique et interactif d'un seul et même système de contrôle de gestion : le cas d'un système d'indicateurs environnementaux dans une entreprise française de vins et spiritueux. » *Finance Contrôle Stratégie*, 16-3.

Simons, Robert. (1994). *Levers of control: how managers use innovative control systems to drive strategic renewal*. Harvard Business Press.

Tajer, Abdellah et *al.* (2022). « The governance of the family business from the perspective of agency and stewardship theory. » *Revue du contrôle, de la comptabilité et de l'audit*, *6*(2).

Thiétart, Raymond-Alain. (2014). *Méthodes de recherche en management-4ème édition*. Dunod.

Tuomela, Tero-Seppo. (2005). « The interplay of different levers of control: A case study of introducing a new performance measurement system. » *Management accounting research, 16*(3), 293-320.

Wernerfelt, Birger. (1984). « A resource-based view of the firm. » *Strategic management journal*, *5*(2), 171-180.

Winkler, Ira, S. (1996). « Case study of industrial espionage through social engineering. » *In Proceedings of the 19th Information Systems Security Conference*, 1-7.

Notes

[i] Centre national de ressources textuelles et lexicales (2024). Disponible sur : https://www.cnrtl.fr/definition/espionnage.

[ii] J.Isnard. « La France cherche à mieux lutter contre les formes modernes de l'espionnage ». *Le Monde*, 1 mars 1995, p8.

[iii] COSO est l'acronyme abrégé de Committee Of Sponsoring Organizations of the Treadway Commission, c'est un référentiel de contrôle interne visant à limiter les risques de fraudes dans les états financiers des entreprises. Il a été défini en 1992 par le Committee of Sponsoring Organisation of the Tread way Commission, mais c'est en 2002 qu'il a véritablement émergé.

[iv] Disponible sur : https://ici.radio-canada.ca/nouvelle/549910/nortel-cyberespionnage-chinois.

[v] Disponible sur : https://www.lemonde.fr/archives/article/1993/05/25/vie-des-entreprises-pour-violation-du-secret-de-l-entreprise-general-motors-intente-un-proces-a-sept-de-ses-cadres-passes-chez-volkswagen_3949474_1819218.html.

[vi] Disponible sur : https://www.lesechos.fr/tech-medias/hightech/asml-victime-despionnage-industriel-1008652.

[vii] Disponible sur : https://www.ege.fr/infoguerre/retour-sur-laffaire-despionnage-russe-sur-le-concorde.

[viii] Disponible sur : https://www.lefigaro.fr/actualite-france/2013/09/11/01016-20130911ARTFIG00599-les-precedentes-affaires-d-espionnage-industriel-en-france.php?utm_source=chatgpt.com.

[ix] Disponible sur : https://www.latimes.com/archives/la-xpm-1997-sep-26-fi-36269-story.html.