UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

ÉCOLE DOCTORALE SCIENCES DE L'HOMME ET DE LA SOCIETE (555)

THÈSE

Pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Discipline : ***SCIENCES DE GESTION***

Spécialité : Contrôle de Gestion

Présentée et soutenue publiquement par

FANE OUMAR

Le 12 novembre 2018

ELABORATION D'UN SYSTEME DE CONTROLE DE L'ESPIONNAGE INDUSTRIEL PAR LA FONCTION CONTROLE DE GESTION

Thèse dirigée par **PR MBENGUE ABABACAR**

JURY

M. Birahim GUEYE,	**Professeur,**	**Université Gaston Berger de Saint-Louis,**	**Président**
M. Ababacar MBENGUE,	**Professeur,**	**Université de Reims Champagne-Ardenne,**	**Directeur de thèse**
M. Mohamed El Bachir WADE,	**Professeur,**	**Université Cheikh Anta Diop de Dakar,**	**Rapporteur**
M. Karim SAID,	**Maître de Conférences HDR,**	**Université de Versailles Saint-Quentin-en-Yvelines,**	**Rapporteur**
Mme Yulia ALTUKHOVA,	**Maître de Conférences,**	**Université de Reims Champagne-Ardenne,**	**Examinatrice**
M. Jean-Luc PETITJEAN,	**Maître de Conférences,**	**Université de Reims Champagne-Ardenne,**	**Examinateur**

Remerciements

Je remercie tout d'abord le Bon DIEU, qui m'a permis de mener ce travail de recherche.

J'exprime ma profonde gratitude au Professeur Ababacar MBENGUE pour avoir accepté d'encadrer cette thèse. Il m'a montré la voie de la rigueur et de la curiosité intellectuelle. Sa disponibilité a été sans faille et je tiens à le remercier vivement pour la confiance et la liberté qu'il m'a accordées.

Je témoigne ma reconnaissance à Monsieur Jean-Luc PETITJEAN pour son indéfectible soutien, son aide, son assistance et sa participation comme membre de jury.

Madame Yulia ALTUKHOVA, Monsieur Birahim GUEYE, Monsieur Karim SAID et Monsieur Mohamed El Bachir WADE ont accepté d'être les membres de jury de ce travail. Je leur en sais profondément gré.

Je remercie exhaustivement toutes les personnes qui ont accepté de me recevoir dans le cadre des différents entretiens semi-directifs sur le terrain.

Merci à Madame Louise DAGUET, Monsieur Jean-Paul MEREAUX et Monsieur Jimmy FEIGE pour leur aide.

Mes sincères remerciements à toute l'équipe pédagogique, administrative et de recherche de l'Université de Reims Champagne-Ardenne.

Je dédie ce travail de recherche à mon Père et ma Mère, qui ont cru en moi et m'ont toujours soutenu dans mes projets.

Je remercie ma femme, mes frères, sœurs, oncles, tantes, cousins, cousines, amis et amies qui m'ont encouragé dans cette recherche.

Résumé

Plusieurs problèmes accablent les organisations, mais l'espionnage industriel occupe de plus en plus une place grandissante. Ses conséquences sont catastrophiques, allant des pertes de sommes colossales à la faillite de certaines entreprises. Ce travail de recherche, s'inscrivant dans le champ disciplinaire des Sciences de Gestion, particulièrement du contrôle de gestion, a pour finalité d'appréhender le processus de contrôle de l'espionnage industriel dans les organisations, en élaborant un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Après une revue de littérature et une première vague d'entretiens semi-directifs, qui ont montré les limites des protections juridiques et les vides de gestion des protections techniques contre l'espionnage industriel, nous avons construit un modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion, qui met en interaction les figures imposées / libres, les leviers de contrôle diagnostic / interactif et leurs outils, et les six dimensions d'analyse réajustées. Ensuite, nous avons élaboré un système de contrôle de l'espionnage industriel, en déterminant ses outils et en spécifiant son instrumentation dans les organisations. Une deuxième vague d'entretiens semi-directifs a été effectuée pour justifier la pertinence dudit système auprès des spécialistes professionnels et universitaires du contrôle de gestion.

Mots-clefs : Espionnage industriel - Contrôle de gestion - Système de contrôle - Elaboration - Processus de contrôle.

Elaboration of a system of control of the industrial espionage by the management control function

Abstract

Several problems overwhelm organizations, but industrial espionage is becoming more and more important. Its consequences are catastrophic, ranging from the loss of colossal sums to the bankruptcy of certain companies. This research work, which is part of the disciplinary field of Management Sciences, particularly management control, aims to understand the process of controlling industrial espionage in organizations by developing a control system of industrial espionage by the management control function. After a literature review and a first wave of semi-directive interviews, which showed the limits of legal protections and management gaps of technical protections against industrial espionage, we constructed a theoretical model of the control process of industrial espionage by the management control function, which puts into interaction the imposed / free figures, the diagnostic / interactive control levers and their tools, and the six readjusted analysis dimensions. Then we developed a system of control of the industrial espionage by determining its tools and specifying its instrumentation in organizations. A second wave of semi-directive interviews was conducted to justify the relevance of this system with professional and academic management control specialists.

Keywords : Industrial espionage - Management control – System of control - Elaboration - Control process.

Liste des abréviations

ABC : Activity-Based Costing

AFDIE : Association Française pour le Développement de l'Intelligence Economique

ALENA : Accord de Libre-échange Nord-Américain

CE : Comptabilité Environnementale

CGE : Contrôle de Gestion Environnemental

CHMCV : Contribution Horaire à la Marge sur Coût Variable

CNRTL : Centre National de Ressources Textuelles et Lexicales

COSO : Committee Of Sponsoring Organizations

ISEOR : Institut Socio-économique des Entreprises et des Organisations

ISO / IEC : Organisation Internationale de Normalisation / Commission Electrotechnique Internationale

KPI : Key Performance Indicators

LICCD : Ligue Internationale Contre la Concurrence Déloyale

NAFTA : North American Free Trade Agreement

OCDE : Organisation de Coopération et de Développement Economiques

ORAA : Objectifs Récurrents et Axes d'Action

OVAR : Objectifs Variables d'Action Responsabilités

PCG : Plan Comptable Général

QQFI : Qualitative Quantitative et Financière

R&D : Recherche et Développement

RS : Référents Sureté

SCIP : Society for Competitive Intelligence Professionals

SOF : Social Organisationnel Financier

SYNFIE : Syndicat Français de l'Intelligence Economique

TGI : Tribunal de Grande Instance

TRIPS : Trade-Related aspects of Intellectual Property Rights

ULC : Uniform Law Commission

USC : United States Code

UTSA : Uniform Trade Secrets Act

SOMMAIRE

INTRODUCTION GENERALE

Le XXI^{ème} siècle connait et ne cesse d'engendrer des phénomènes impactant considérablement les organisations en termes de stabilité politique, économique, sociale… Certains problèmes perdurent et connaissent un essor sans précédent à cause de l'évolution technologique. Toutes les disciplines demeurent unanimes sur le fait que l'avancée scientifique est toujours accompagnée de ses répercussions.

De ce fait, il apparait nécessaire d'accompagner l'évolution scientifique inlassablement des remèdes adéquats aux différentes conséquences néfastes que celle-ci peut engendrer.

C'est tout à fait l'objectif ultime du développement durable, si l'on se réfère à la définition classique provenant du rapport Brundtland de la Commission mondiale sur l'environnement et le développement de l'Organisation des Nations Unies : « *Le développement durable est un mode de développement qui répond aux besoins du présent sans compromettre la capacité des* générations futures *de répondre aux leurs* »[1]. Dans le dessein d'atteindre ces objectifs, les organisations demeurent en permanence à la recherche des solutions adéquates.

Les actualités nous montrent clairement que les organisations évoluent dans un environnement aussi fluctuant qu'incertain. Des nouvelles problématiques naissent en permanence et les organisations se doivent, ne serait-ce que dans un souci de survie pour certaines d'entre elles, d'anticiper les différents changements de l'environnement.

L'adaptation des organisations aux enjeux environnementaux, politiques, économiques, sociaux reste au cœur des priorités de toute structure visant l'atteinte de ses objectifs préétablis. Elle constitue un enjeu majeur, voire principal, pour les organisations et celles-ci se trouvent dans l'obligation de riposter efficacement et de façon efficiente.

Les organisations doivent donc mettre en œuvre toutes les possibilités managériales afin d'assurer la pérennité de leurs affaires, tout en essayant de maintenir un bon niveau de compétitivité.

C'est dans cette finalité de bonne gestion que des pionniers comme Taylor, Fayol, Schell, Simon, Miles, Anthony, Snow, Simons, Woodward, Mintzberg et bien d'autres ont développé des méthodes et outils de gestion.

[1] Définition issue du rapport Brundtland de la Commission mondiale sur l'environnement et le développement de l'Organisation des Nations Unies (1987).

Dans cet ordre d'idée, un des phénomènes nuisibles qui se propage exponentiellement dans les différentes organisations constitue l'espionnage industriel. Au début, il était considéré comme un problème touchant principalement les grandes organisations (Etats, les organismes internationaux, les grandes entreprises…).

En ce qui concerne les précisions sur le vocabulaire dans les développements qui vont suivre, nous utiliserons le terme « espionnage industriel » tout au long de notre travail de recherche, bien que de nombreux organismes et auteurs lui attribuent les expressions : « espionnage économique », ou « espionnage d'affaires », ou « espionnage commercial », ou « violation de secret d'entreprise[2] », etc.

Il est clair que l'intérêt des espions ne se limite guère aux seuls secrets industriels. Toutes les autres activités de l'entreprise, des gouvernements et des organismes internationaux sont également visées par les espions. Nous conservons, toutefois, l'expression « espionnage industriel » par commodité d'usage, même si celle-ci ne restitue pas le phénomène dans sa globalité.

Cependant, les réalités contemporaines démontrent un élargissement des potentielles cibles, incluant aussi bien les grandes organisations que les petites et moyennes organisations. De nombreux rapports internationaux et nationaux exposent les différentes répercussions et chiffrent les coûts infligés par l'espionnage industriel. Néfaste et connaissant une évolution rapide, l'espionnage industriel fait des ravages dans les organisations, même si certaines n'en sont pas conscientes.

L'objectif de la gestion étant globalement d'améliorer les conditions économiques et sociales des organisations au travers des dispositifs et processus de gestion, particulièrement le contrôle de gestion, qui est un processus de management, s'assure de la mise en œuvre des stratégies de l'organisation[3].

C'est dans ce registre que nous nous intéressons à l'espionnage industriel pour le maîtriser et l'éradiquer, afin d'améliorer les conditions économiques des organisations, voire sauver certaines organisations de la faillite.

[2] Expression d'emprunt de la Ligue Internationale Contre la Concurrence Déloyale (LICCD), considérant l'expression « espionnage industriel » comme péjorative et limitative.
[3] Berland, N. (2014). *Le contrôle de gestion : «Que sais-je?» n° 3977*. Presses universitaires de France.

Ce travail de recherche s'inscrit dans le champ disciplinaire des Sciences de Gestion, particulièrement du contrôle de gestion. Il a pour finalité d'appréhender le processus de contrôle de l'espionnage industriel dans les organisations, en élaborant un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Dans notre introduction, nous allons commencer par mettre en exergue l'ampleur de l'espionnage industriel, ensuite nous définissons notre objet de recherche et nous allons conclure avec une présentation de l'architecture de la thèse.

1. L'espionnage industriel : un phénomène au cœur de l'actualité

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 challenge 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.

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.

Les conséquences de l'espionnage industriel sont catastrophiques, allant des pertes de sommes colossales à la faillite de certaines entreprises. 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.

L'espionnage industriel est un phénomène, qui ne ménage aucune entité (publique ou privée). Il apparait nécessaire de mentionner, que toutes les entreprises peuvent être des cibles d'espionnage industriel (sans exception), du moment où l'information revêt une quelconque importance pour les espions.

La taille, le type d'activité et le domaine d'activité de l'entreprise ne constituent pas des motifs 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'évolution du numérique a été le point de départ d'une croissance du phénomène dans le monde des entreprises. Des outils, moyens et techniques de recueil des informations ont été développés. La rude concurrence, l'évolution des entreprises, la recherche de la performance et bien d'autres raisons expliquent la prolifération de l'espionnage industriel au sein des entreprises.

La rareté des ressources et la compétitivité ont également poussé certaines entreprises à recourir à divers moyens pour améliorer leurs performances et ainsi assurer leur pérennité. L'information est pourtant un des moyens indispensables et les plus rapides pour se distinguer des autres concurrents.

Par conséquent, certaines entreprises n'hésitent pas à pratiquer l'espionnage industriel pour acquérir des informations susceptibles de leur apporter un quelconque avantage. Toutefois, nul n'est à l'abri des pratiques d'espionnage industriel, contrairement à ce que cautionnent plusieurs entreprises.

Cette fulgurante évolution du phénomène doit alarmer les entreprises à ce qu'elles définissent des stratégies de lutte contre l'espionnage industriel. Les chercheurs des différentes disciplines doivent également s'intéresser aux questions touchant le phénomène. Cependant, il est regrettable de constater la rareté des écrits et publications scientifiques sur l'espionnage industriel. Pourtant le fléau est d'actualité et connait une croissance active dans le monde des entreprises.

2. Objet de recherche

Nous allons évoquer dans cet objet de recherche notre problématique, la question de recherche, quelques intérêts de la recherche et notre méthodologie de recherche.

2.1. Problématique

L'espionnage industriel est une pratique déloyale, qui engendre des répercussions néfastes sur les entreprises qui en sont victimes.

Les conséquences de l'espionnage industriel ont été suffisantes, pour que des mesures de protection soient définies pour lutter contre le fléau. En effet, les coûts issus de l'espionnage industriel constituent une véritable charge pour certaines entreprises, tandis que d'autres n'en survivent même pas.

Pour riposter, l'espionnage industriel est devenu une affaire de tous (Etats, organismes internationaux, entreprises). Différents types de protection ont été élaborés pour atténuer ses répercussions, voire empêcher sa survenance.

Pour se protéger, l'entreprise dispose des protections juridiques qui se sont multipliées grâce aux différents gouvernements et organismes internationaux, il s'agit notamment : des brevets, des droits d'auteur, des textes législatifs, des textes réglementaires, etc.

Par contre, ces législations et réglementations, qui constituent indéniablement des barrières de protection pour les entreprises, se sont avérées très limitées (protections non exhaustives)[4]. Ces éléments sont certes dissuasifs, mais les espions ont su trouver des moyens pour les contourner.

En renfort, les entreprises se protègent par des moyens et outils de gestion élaborés par elles-mêmes. Il s'agit d'une gestion organisationnelle par les entreprises, pour consolider les protections juridiques et ainsi empêcher la survenance de l'espionnage industriel. Cette gestion se traduit par le contrôle interne et l'ensemble des types de gestion de l'espionnage industriel dans les entreprises.

La revue de littérature nous révèle les limites de cette seconde protection (les dangers de l'artillerie sécuritaire, les coûts de la protection…). Cette deuxième protection, que nous pouvons appeler « protection technique », nécessite également des améliorations pour mieux se protéger contre le phénomène.

Ainsi, nous pouvons relever quelques points nécessitant des améliorations, à travers les différents écrits scientifiques, comme :

[4] Cette affirmation sera détaillée dans le chapitre 1.

- l'absence d'outils efficaces à la disposition des entreprises pour évaluer les coûts de l'espionnage industriel ;
- l'absence d'un pilotage des moyens et méthodes de protection contre l'espionnage industriel…

Ces remarques constituent des raisons évidentes, pour améliorer la protection des entreprises contre l'espionnage industriel.

C'est dans cette optique d'amélioration des outils et moyens de protection contre l'espionnage industriel, que nous nous sommes intéressés à ce sujet de recherche, dans l'objectif de proposer des alternatives de gestion, qui permettront de réconforter la protection des entreprises contre l'espionnage industriel.

Dans le cadre de cette recherche, nous nous inscrivons dans une posture défensive de protection contre l'espionnage industriel, c'est-à-dire dans la recherche de solutions de gestion empêchant les espions d'accéder aux informations confidentielles et aux informations secrètes de l'entreprise.

Il s'agit de développer précisément des moyens et outils de gestion, qui sécurisent les entreprises, sans toutefois envisager une attaque offensive.

Ainsi, la problématique de cette recherche s'articule sur l'amélioration et la consolidation des protections techniques des entreprises contre l'espionnage industriel, au travers de la fonction contrôle de gestion.

2.2. Question de recherche

Les limites[5] des textes juridiques et celles du contrôle organisationnel nous poussent à trouver une autre façon de consolider la protection des entreprises contre l'espionnage industriel.

Les caractéristiques des limites citées ci-haut nous renvoient à une fonction spécifique de l'entreprise, qui semble avoir les capacités nécessaires à l'appréhension du phénomène.

Il s'agit du contrôle de gestion, qui est une fonction très dynamique. L'une des premières définitions structurées du contrôle de gestion est d'Anthony, professeur à Harvard, (1965) : « *le contrôle de gestion est le processus par lequel les managers obtiennent l'assurance que les*

[5] Les différentes limites seront détaillées dans le chapitre 1.

ressources sont obtenues et utilisées de manière efficace et efficiente pour la réalisation des objectifs de l'organisation ».

Ayant un caractère trop comptable, le même auteur modifie quelques années plus tard sa définition comme suit : « *le contrôle de gestion est le processus par lequel les managers influencent d'autres membres de l'organisation pour mettre en œuvre les stratégies de l'organisation* » (Anthony, 1988).

D'autres auteurs ont défini le contrôle de gestion en mettant en avant sa capacité à s'élargir, nous pouvons citer celles de :

- Simons (1995) : « *les processus et les procédures fondés sur l'information que les managers utilisent pour maintenir ou modifier certaines configurations des activités de l'organisation* » ;
- Berland et Simon (2010) : « *le contrôle de gestion est en effet un ensemble de pratiques paradoxales qui ne saurait se limiter à des outils ou à une profession au risque d'en présenter une vision trop caricaturale qui ne permet pas d'en saisir la richesse et le potentiel ».*

C'est une fonction transversale de l'entreprise, qui comporte des outils et moyens de gestion efficaces et dynamiques (dans le sens d'une réadaptation).

Les écrits scientifiques, n'étant pas nombreux à la base sur la question des outils et moyens techniques de protection contre l'espionnage industriel, semblent focaliser sur la détermination :

- des procédures internes de protection contre l'espionnage industriel[6] ;
- des conseils pratiques prodigués par les services gouvernementaux, les organismes internationaux… ;
- des mesures pratiques de protection contre l'espionnage industriel…

Nous ne dénigrons nullement ces différentes mesures juridiques et techniques de protection contre l'espionnage industriel. Bien au contraire, ce sont des solutions qui contribuent indéniablement à la protection des entreprises contre le fléau.

[6] Au vu du nombre important des cabinets privés proposant des solutions de protection contre l'espionnage industriel.

Cependant, elles sont dépourvues de pilotage et peuvent être améliorées pour accentuer la protection de l'entreprise contre l'espionnage industriel. Le contrôle de gestion peut être une solution pour résoudre ces problèmes.

Le contrôle de gestion peut intervenir dans un but d'amélioration et de consolidation des protections juridiques et techniques contre l'espionnage industriel, en comblant certains vides de gestion comme l'absence d'un pilotage des moyens et méthodes de protection contre l'espionnage industriel, l'absence d'outils efficaces à la disposition des entreprises pour évaluer les coûts de l'espionnage industriel, etc.

Ainsi, 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.

Dans ce travail de recherche, nous nous proposons d'élaborer un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, afin d'améliorer et de consolider les protections techniques contre l'espionnage industriel dans les entreprises.

Il s'agit de répondre à la question suivante :

Comment élaborer un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion ?

2.3. Intérêt de la recherche

L'intérêt de notre recherche est multiple dans le sens où le sujet traité est novateur et constitue une première dans la discipline du contrôle de gestion. Nous pouvons retenir quelques points d'intérêt :

- sur un plan théorique :

- ❖ après avoir donné quelques définitions de l'espionnage industriel, nous nous proposons d'apporter un éclairage sur la délimitation entre l'espionnage industriel et ses concepts connexes, notamment l'intelligence économique (qui demeure le concept le plus confondu à l'espionnage industriel) ;
- ❖ la mobilisation de plusieurs concepts (contrôle de gestion environnemental, comptabilité environnementale, coûts et performances cachés) pour définir un cadre d'analyse du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion (sujet novateur) ;
- ❖ l'élaboration d'un modèle théorique de gestion de l'espionnage industriel par la fonction contrôle de gestion, en démontrant que ce processus se caractérise par la gestion des figures imposées et des figures libres, qui s'appréhendent par les leviers de contrôle diagnostic et interactif de Simons ;

- sur un plan méthodologique : l'itinéraire de la recherche est un aller-retour entre terrain et théories pour élaborer un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion ;
- sur un plan managérial :
  - ❖ au su des conséquences désastreuses de l'espionnage industriel sur les économies et les entreprises, alerter les entreprises à ce qu'elles reconsidèrent les effets néfastes et la portée du phénomène pour mettre en œuvre les solutions de gestion les plus efficaces et efficientes ;
  - ❖ il semble que les outils du contrôle de gestion ne puissent appréhender l'espionnage industriel que de manière limitée, nous allons définir des outils permettant d'appréhender le phénomène à toutes les étapes de contrôle (avant, pendant et après l'action).

2.4. Méthodologie de la recherche

Pour aborder cette question de recherche, nous avons opté pour une méthodologie de recherche qualitative. Elle s'enregistre dans une démarche hypothético-inductive, qui se traduit par des allers et retours entre le terrain et la littérature théorique.

Un état de l'art de l'espionnage industriel nous a permis de soulever la question du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Ce qui a permis de déterminer un cadre théorique. Conjointement à la revue de littérature, des informations de terrain ont été collectées pour réconforter le cadre d'analyse.

L'objectif est de collecter empiriquement des informations sur le terrain et les confronter aux éléments théoriques de la littérature, afin d'élaborer un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Plusieurs concepts et théories ont été mobilisés pour appréhender la question d'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Certes, le travail de recherche est basé sur l'élaboration d'un système de contrôle, par contre le travail de terrain a débuté avec l'objectif d'explorer un processus de contrôle de l'espionnage industriel dans les organisations.

Nous avons essentiellement privilégié comme mode de recueil des données, les entretiens semi-directifs et les documentations, qui nous semblent être convenables pour collecter des informations pertinentes et ciblées.

Les résultats d'une première vague d'entretiens ont redirigé notre travail de recherche vers l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion (sachant que l'objectif de ce premier contact était différent de l'objectif ultime de notre travail de recherche).

Les résultats d'une deuxième vague d'entretiens nous ont permis de vérifier la pertinence de notre système construit. Les allers et retours nous ont donc permis de définir clairement l'objectif même de cette recherche.

Nous nous inscrivons dans une posture épistémologique interprétativiste, c'est-à-dire que le chercheur est en interaction avec son objet et son objectif n'est pas d'intervenir, mais de comprendre les phénomènes en étant immergé dans ces derniers.

3. Architecture de la thèse

Ce travail de recherche comprend deux parties : une première partie sur l'état de l'art et la définition d'un cadre théorique et conceptuel ; et une deuxième partie sur la détermination empirique d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

La première partie comporte deux chapitres : le chapitre 1 expose un état de l'art de l'espionnage industriel et le chapitre 2 explicite les concepts et théories mobilisés.

Le chapitre 1 comprend trois sections : nous allons exposer dans une première section les différentes définitions de l'espionnage industriel, tout en mettant en exergue ses caractéristiques, mais aussi son évolution ; dans une deuxième section, nous allons appréhender le concept d'espionnage industriel à travers les concepts d'intelligence économique, de droit et d'éthique ; et nous montrerons dans une troisième section, la nécessité d'introduire le contrôle de l'espionnage industriel dans la gestion de l'entreprise, en effectuant un état des lieux des protections juridiques et techniques pour déterminer les perspectives d'amélioration.

Le chapitre 2 se scinde également en trois sections : nous allons aborder dans une première section la mobilisation des concepts de comptabilité environnementale, des coûts cachés et du contrôle de gestion environnemental pour justifier le cadre de la recherche ; ensuite nous explicitons dans une deuxième section la détermination d'un cadre théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion ; enfin nous allons décortiquer les six dimensions d'analyse de Chiapello revisitées et présenter le modèle théorique.

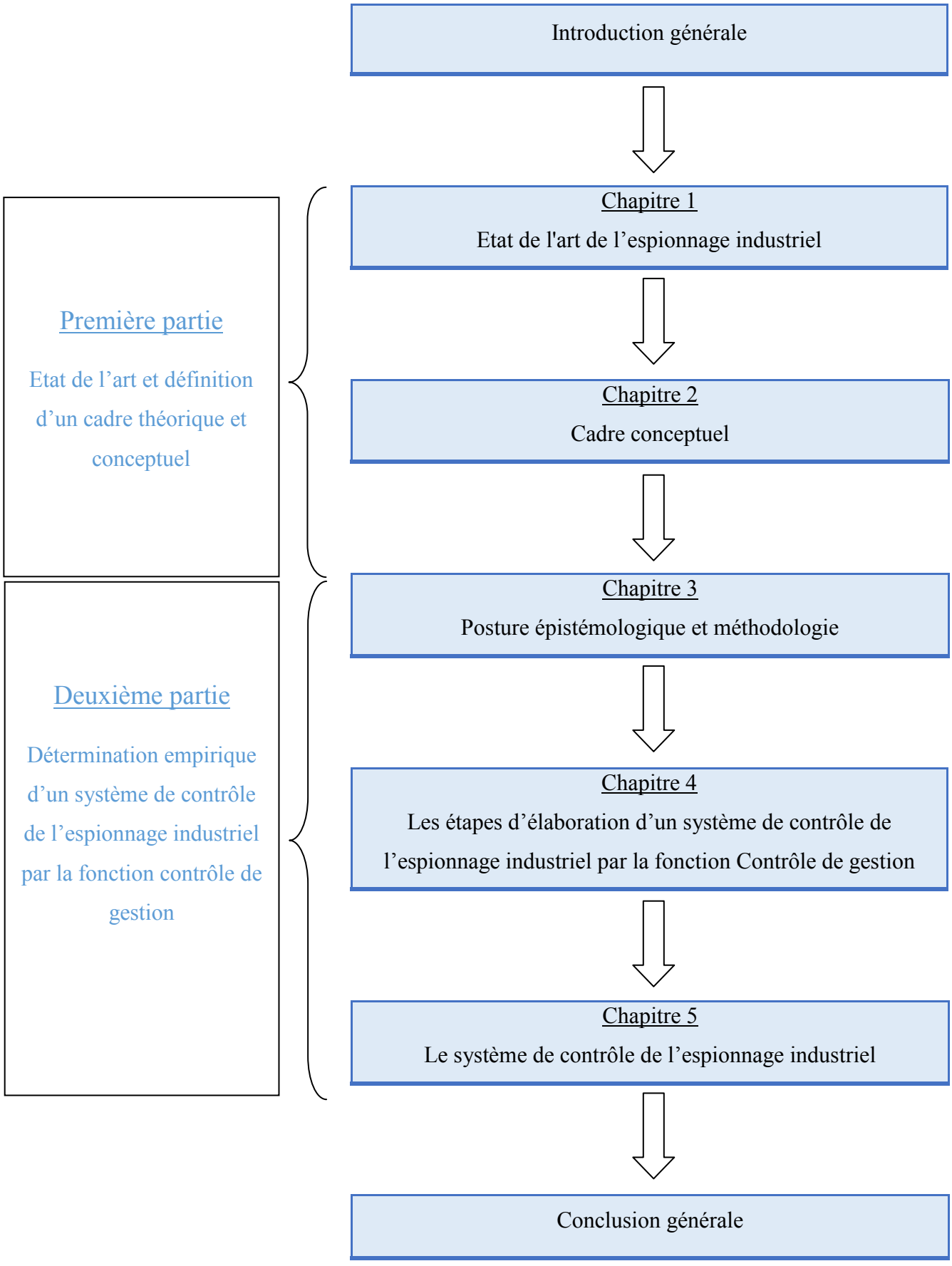
La deuxième partie comporte trois chapitres : le chapitre 3 présente l'organisation méthodologique des travaux de terrain ; le chapitre 4 détaille les étapes d'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion ; et le chapitre 5 fait l'objet d'une présentation dudit système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Le chapitre 3 se subdivise en deux sections : nous présenterons dans une première section la méthodologie de recherche adoptée et la posture épistémologique de cette recherche ; et nous aborderons dans une deuxième section le mode de recueil et le traitement des données, tout en précisant le choix de l'échantillon, les moyens de collecte des données, les outils d'analyse des données et les premiers enseignements du terrain.

Le chapitre 4 contient deux sections, qui explicitent la détermination des outils des leviers de contrôle diagnostic et interactif de notre système de contrôle. La première section fera l'objet d'une détermination des outils du levier de contrôle diagnostic, dans le but de cerner les figures imposées. La deuxième section sera consacrée à l'étude des outils du levier de contrôle interactif, afin d'encadrer les figures libres du processus de contrôle de l'espionnage industriel.

Le chapitre 5 renferme deux sections : la première section fait l'objet d'une présentation de notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion ; ensuite nous allons interpréter et discuter les résultats de la deuxième vague d'entretiens dans la deuxième section.

L'architecture de la thèse est la suivante :


Introduction générale
Chapitre 1
Etat de l'art de l'espionnage industriel
Chapitre 2
Cadre conceptuel
Chapitre 3
Posture épistémologique et méthodologie
Chapitre 4
Les étapes d'élaboration d'un système de contrôle de l'espionnage industriel par la fonction Contrôle de gestion
Chapitre 5
Le système de contrôle de l'espionnage industriel
Conclusion générale
Première partie
Etat de l'art et définition d'un cadre théorique et conceptuel
Deuxième partie
Détermination empirique d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion

PARTIE I :
ETAT DE L'ART ET DEFINITION D'UN CADRE THEORIQUE ET CONCEPTUEL

Chapitre 1 : Etat de l'art de l'espionnage industriel

L'espionnage industriel est un fléau mondial, qui prend incessamment de l'ampleur dans les entreprises. C'est un concept qui existe depuis des lustres. Selon Coskun Samli et Jacobs (2003) : l'espionnage n'est pas nouveau. Carlton (1992) affirme que « *les Celtes ont volé les secrets de fabrication des roues supérieures des Romains, et les Perses ont volé les secrets de la production de soie aux Chinois, bien qu'ils aient fait de cette divulgation une offense capitale* ».

Par contre, le début de son essor fulgurant n'est signifié qu'au XX^{ème} siècle. L'amplitude du niveau de progression de l'espionnage industriel est proportionnelle à l'évolution des nouvelles technologies (les multiples cas illustrés dans la presse nous permettent de justifier cette affirmation).

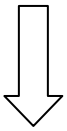
Par ailleurs, il convient de signaler la rareté des travaux scientifiques sur l'espionnage industriel (il existe très peu d'écrits scientifiques sur le concept). Pourtant, il a des conséquences désastreuses sur les entreprises, allant des pertes de millions d'euros à la faillite de certaines entreprises. 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.

Cependant, il ne cesse de se propager dans les économies et les entreprises. 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).
Malgré ces constats, le désintéressement des chercheurs reste flagrant.

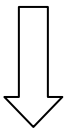
Cet état de l'art comprend trois sections : nous allons exposer dans une première section les différentes définitions de l'espionnage industriel tout en mettant en exergue ses caractéristiques et son évolution ; dans une deuxième section, nous allons appréhender le concept d'espionnage industriel à travers les concepts d'intelligence économique, de droit et d'éthique ; et nous montrerons dans une troisième section, la nécessité d'introduire le contrôle de l'espionnage industriel dans la gestion de l'entreprise, en effectuant un état des lieux des protections juridiques et techniques pour déterminer les perspectives d'amélioration.

L'architecture du chapitre est la suivante :

Section 1 **Espionnage industriel : définitions, caractéristiques et évolution**	
Définitions	Caractéristiques et évolution



Section 2 **Intelligence économique et espionnage industriel : droit et éthique**			
Le concept d'intelligence économique	L'information : la matière première des concepts d'espionnage industriel et d'intelligence économique	Le recours au droit et à l'éthique pour délimiter la frontière entre l'espionnage industriel et l'intelligence économique	Les limites de cette distinction entre l'espionnage industriel et l'intelligence économique



Section 3 **La nécessité d'introduire le contrôle de l'espionnage industriel dans la gestion de l'entreprise**		
Espionnage industriel et protections juridiques	Espionnage industriel et Contrôle Interne	Espionnage industriel et Contrôle de gestion ?

Section 1 : Espionnage industriel : définitions, caractéristiques et évolution

L'espionnage industriel a une nature occulte, ce qui rend le sujet très sensible dans le monde des organisations. Le paradoxe est de constater d'un côté la prolifération du phénomène aussi bien dans les économies que les entreprises, et d'un autre côté le petit nombre des travaux et études scientifiques sur le sujet.

Cependant, les rares chercheurs et auteurs, qui s'y intéressent, l'appréhendent à leur façon. Par conséquent, l'espionnage industriel est devenu un concept polysémique. Certaines définitions tendent à confondre le concept avec d'autres concepts proches, d'autres définitions semblent restreintes ou globales.

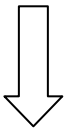
Tous ces éléments évoquent la nécessité d'une définition claire du concept, afin d'éviter toute confusion à l'avenir. Pour ce faire, nous avons souhaité exposer plusieurs définitions de l'espionnage industriel.

L'objectif de cette section est d'éclaircir le concept, en présentant les différentes définitions de l'espionnage industriel, pour ensuite exposer ses caractéristiques tout en évoquant son évolution.

Dans cette section, nous allons montrer l'ambigüité sémantique qui résulte de l'analyse des différentes définitions de l'espionnage industriel (1). Ensuite, nous présenterons les caractéristiques et évolution de l'espionnage industriel (2).

L'architecture de la section est la suivante :

Définitions



Caractéristiques et évolution			
Les principaux éléments de l'espionnage industriel	Méthodes de collecte des informations	Conséquences de l'espionnage industriel	Evolution de l'espionnage industriel

1. Définitions

L'espionnage industriel a sémantiquement connu de nombreuses définitions. A cet effet, il fait allusion à un concept polysémique. Certains auteurs, en expliquant d'autres concepts comme l'intelligence économique, donnent secondairement une définition de l'espionnage industriel. D'autres spécifient la définition tout en détaillant les caractéristiques. Les organismes internationaux et les gouvernements, quant à eux, déterminent exceptionnellement les contours de l'espionnage industriel pour des raisons juridiques. Dans ce sens, l'espionnage industriel peut avoir plusieurs définitions, d'un pays à un autre, d'un organisme international à un autre.

Nous dénombrons plusieurs définitions de l'espionnage industriel. Le tableau ci-dessous permet de classer chronologiquement quelques définitions des auteurs et chercheurs :

Tableau 1 : Définitions de l'espionnage industriel

Auteur (année)	Définition de l'espionnage industriel
PAYNE (1971)	L'espionnage industriel est défini, selon Payne, 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* ».
Annual Report to Congress on Foreign Economic Collection and Industrial Espionage : Rapport annuel au Congrès sur la Collection Économique Étrangère et l'Espionnage Industriel (1995)	L'espionnage industriel est défini comme « *une activité menée par un gouvernement étranger ou par une société étrangère avec l'aide directe d'un gouvernement étranger contre une entreprise privée américaine dans le but d'obtenir des secrets commerciaux* ». Le procureur général des États-Unis définit l'espionnage économique comme étant « *le ciblage ou l'acquisition illicites ou clandestins de renseignements sensibles sur les politiques financières, commerciales ou économiques ; informations économiques exclusives ; ou technologies critiques* ».
Etats – Unis : the Economic Espionage Act of (1996)[7]	En termes généraux, l'espionnage économique est le ciblage illégal ou clandestin ou l'acquisition d'informations sensibles sur la politique financière, commerciale ou économique ; d'informations économiques exclusives ; ou d'informations technologiques. *The Economic Espionage Act of (1996)* définit l'espionnage économique comme « *un vol ou détournement d'un secret d'affaires avec l'intention et la connaissance que l'infraction bénéficiera tout gouvernement étranger, organisation étrangère, ou agent étranger. L'acte de réception, d'achat ou de possession d'un secret d'affaires avec la connaissance qu'il a été volé ou détourné, comme toute autre intention ou conspiration de commettre un espionnage économique sont punissables comme un crime fédéral…* ».

[7] Source de la définition : Legal Information Institute, « Economic Espionage », Cornell University Law School, Disponible sur : www.law.cornell.edu/wex/economic_espionage, consultée le 27/06/2018.

NOAILLY (1997)	Il s'agit de « *l'ensemble des pratiques à travers lesquelles les informations sont obtenues par des moyens répréhensibles (corruption, piratage, vols de documents…). Souvent confondu avec la veille technologique, l'espionnage industriel est une toute autre alternative pour le recueil d'informations. Certaines entreprises, dépourvues de déontologie, n'hésitent cependant pas à tomber dans cette forme d' « illégalité économique ».* Le terme illégalité économique regroupe l'ensemble des pratiques d'espionnage industriel, de contrefaçon, de corruption ; le marché de la drogue ; les économies mafieuses...
BAUD (1998)	L'espionnage *désigne une opération clandestine de collecte de renseignement*.
DUPRE (2001)	Dupré définit l'espionnage économique comme « *le fait pour une personne physique ou morale, de rechercher dans un but économique, pour soi ou pour autrui, de manière illégitime – c'est-à-dire le plus souvent à l'insu et contre le gré de son détenteur – des informations techniques ou de toute nature lorsque ces informations présentent une valeur, même potentielle, dont la divulgation serait de nature à nuire aux intérêts essentiels de ce dernier* ».
CURTIS (2001)	Selon la SCIP (Society for Competitive Intelligence Professionals), *l'espionnage industriel ou l'espionnage est à la fois contraire à l'éthique et illégal, il existe parfois une limite entre la tactique « légitime » de la collecte de renseignements compétitifs et la pratique « illégitime » de l'espionnage industriel*.
COSKUN SAMLI et JACOBS (2003)	La gamme d'activités répertoriées, entrant dans le cadre de l'espionnage, est large. Cela va de l'utilisation des yeux et des oreilles dans le cadre d'activités ouvertes et légales à des opérations d'espionnage clandestines classiques menées par des moyens clandestins. La partie légale de l'espionnage a donné lieu à une veille économique accélérée. Il comprend l'examen d'informations accessibles au public telles que les dossiers judiciaires, les rapports

	annuels des sociétés, les documents gouvernementaux, les rapports de marché, les foires commerciales, les discours des dirigeants et les rapports des représentants commerciaux (Gwynne, Teagarden, 1997). En revanche, les activités d'espionnage industriel sont contraires à l'éthique et souvent illégales. Ces opérations comprennent la corruption de concurrents pour des processus techniques secrets, l'embauche d'employés pour obtenir des informations concurrentielles comme des processus ou des connaissances en marketing, l'écoute de communications et le chantage à des employés clés (Teagarden, 1997). La différence entre l'intelligence économique et l'espionnage industriel est que le premier est l'analyse, l'organisation et la distribution de l'information légalement disponible utile au décideur politique, tandis que l'espionnage industriel est un vol de secrets (M.J. Stedman, 1991).
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.
BULINGE et PEPIN (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* ».
LAROUSSE (2017)[8]	Espionnage industriel, recherche de renseignements concernant les procédés de fabrication industriels.
C.N.R.T.L.[9]	Action de recueillir clandestinement des renseignements sur les secrets de fabrication d'un concurrent.

[8] Définition de l'espionnage industriel, LAROUSSE (2018). Consulté le 21/11/2018. Disponible sur : https://www.larousse.fr/dictionnaires/francais/espionnage/31049/locution.
[9] Définition de l'espionnage industriel par le CNRTL (Centre National de Ressources Textuelles et Lexicales). Consulté le 21/06/2018. Disponible sur : http://www.cnrtl.fr/definition/espionnage.

Pour certains auteurs, l'espionnage industriel est souvent décrit comme un dérivé malsain de la veille technologique, le cancer de l'intelligence économique, etc.

Nous remarquons qu'il existe une multitude de définitions de l'espionnage industriel. Certaines définitions sont globales, puisqu'elles peuvent confondre l'espionnage industriel à des concepts proches, et d'autres sont assez détaillées.

L'espionnage industriel consisterait à l'expropriation de certains « éléments » par des moyens répréhensibles (en termes de légalité et d'éthique). Les différents auteurs et chercheurs utilisent, certes, des termes différents pour ces « éléments » : informations, renseignements, secrets d'affaires, secrets commerciaux…, qui sont pourtant différents. Cependant, ils peuvent être très similaires dans certains contextes.

Les auteurs et chercheurs se rejoignent majoritairement sur le problème de délimitation entre l'espionnage industriel et certaines notions connexes comme l'intelligence économique (Winkler, 1996 ; Coskun samli et Jacobs, 2003 ; Crane, 2005 ; Memheld, 2012 ; etc.). Nonobstant, il apparait nécessaire de clarifier le concept, afin d'éviter toute incohérence avec certaines notions connexes.

2. Caractéristiques et évolution

Dans cette deuxième section, nous allons relever les principaux éléments qui caractérisent l'espionnage industriel (A), pour ensuite mettre en exergue les méthodes de collecte des informations (B), nous citons quelques conséquences de l'espionnage industriel dans la sous-section (C) et nous terminons par quelques points d'évolution du concept (D).

A. Les principaux éléments de l'espionnage industriel

En analysant les différentes définitions de l'espionnage industriel, nous pouvons dénombrer certains éléments du phénomène. 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…

Les principales explications de l'espionnage industriel, que nous pouvons relever, demeurent imprécises. Elles sont souvent globales ou réductrices, ce qui provoque une confusion du phénomène avec des concepts proches.

Plusieurs concepts se rapprochent de l'espionnage industriel, dont les frontières de délimitation sont très floues. Il est important de délimiter le périmètre de l'espionnage industriel, afin que certains praticiens acquièrent toute la légitimité de leur profession.

Au regard des différentes définitions de l'espionnage industriel ci-haut, nous pouvons relever certains points communs avec d'autres concepts susceptibles de faire l'objet d'une confusion, il s'agit notamment de l'intelligence économique, la veille, etc.

Ce problème de confusion est prégnant, car ils sont tous des pratiques utilisées par les entités consistant à recueillir des informations, dans le but de bénéficier des avantages par rapport aux autres entités. Cependant, les moyens de collecte des informations sont nombreux, diversifiés et ne présentent pas les mêmes caractéristiques dans l'ensemble.

B. Méthodes de collecte des informations

Les méthodes de collecte des informations dans le cadre de l'espionnage industriel évoluent d'une manière exponentielle, à tel point qu'on se demande s'il existe des mesures adéquates pour non seulement les détecter, mais aussi empêcher le vol des informations.

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 suite à 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 crossant 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 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 Francis 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. Même les simples fouilles dans les poubelles constituent un acte d'espionnage industriel, si elles visent les informations confidentielles ou sécrètes d'un concurrent.

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.

C. Conséquences de l'espionnage industriel

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.

Les conséquences de l'espionnage industriel sont désastreuses sur ses victimes, allant des pertes de sommes colossales à la faillite de certaines entreprises. Inévitablement, l'espionnage industriel ébranle l'entreprise qui en est victime, provoquant une perte d'activité plus ou moins grande. Les conséquences, qu'elles soient commerciales ou financières, sont toujours très importantes et peuvent aller jusqu'à nuire à la survie de l'entreprise.

Parmi les nombreux cas d'espionnage industriel illustrant ses conséquences néfastes sur les entreprises, nous pouvons retenir :

- En France, la Direction de la Surveillance du Territoire a évalué les coûts de l'espionnage industriel à 10 milliards de francs par an[10]. D'autres experts quadruplent ce chiffre, car celui-ci ne fait pas état des activités des sociétés privées.
- D'après une étude réalisée par Rotman-Telus en 2009, les organisations canadiennes ont rapporté les cinq conséquences les plus importantes en termes de coût :
    - ❖ répercussion sur la réputation ;
    - ❖ perte de temps due à la perturbation ;
    - ❖ perte de clients ;
    - ❖ actions régulatrices ;
    - ❖ contentieux.
- Selon Wanja Eric Naef (2003), des milliards de dollars et des milliers d'emplois sont perdus en raison du vol de secrets commerciaux. Un sondage mené par PricewaterhouseCoopers et la société américaine de sécurité industrielle a révélé que les entreprises du classement Fortune 1000 ont perdu plus de 45 milliards de dollars en 1999 en raison du vol de leurs informations exclusives. Ces pertes, selon l'étude, ont particulièrement frappé les industries manufacturières.

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

- 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 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[11].
- Dans leur ouvrage « Secrets Stolen, Fortunes Lost : Preventing Intellectual Property Theft and Economic Espionage in the 21st Century », les chercheurs américains Christopher Burgess et Richard Power 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 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.

L'essor des nouvelles technologies a rendu l'espionnage industriel sophistiqué, à tel point que certaines entreprises se font espionner et partent en faillite sans s'en rendre compte. Les nouvelles technologies ont amplifié exponentiellement la prolifération de l'espionnage industriel dans les économies et les entreprises.

Nous sommes, dorénavant, dans une société où l'information occupe une place cruciale, vitale et indispensable. Avoir ces informations procure un avantage incommensurable. Cependant, les espions n'hésitent pas à collecter ces informations, tout en ignorant les conséquences subies par les victimes.

[11] Nséké L. (2012). Espionnage industriel : Des coûts importants. Afrique Expansion Magazine. Revue des affaires et des partenariats Nord-Sud. Consulté le 23/11/2018. Disponible sur : https://afriqueexpansionmag.com/.

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 :

- Selon le rapport Frantz (2014) sur la protection des secrets d'affaires dans l'Union Européenne, le coût annuel de l'espionnage industriel supporté par les entreprises allemandes se situe entre 20 et 50 milliards d'euros.
- Selon le gouvernement des États-Unis (2013), le vol des secrets commerciaux menace les entreprises américaines, sape la sécurité nationale et met en danger la sécurité de l'économie des États-Unis. Ces actes diminuent également les perspectives d'exportation des États-Unis dans le monde entier et mettent en péril les emplois américains.
- 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 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). Il est important d'insister sur le fait qu'il peut être pratiqué dans toutes les entreprises et économies sans exception, du moment où l'information revêt une quelconque importance pour les espions.

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.

D. Evolution de l'espionnage industriel

L'espionnage industriel est une pratique très ancienne qui remonte à une époque aussi lointaine que difficile à déterminer. Etant une activité humaine, il est difficile de dater sa première apparition. Cependant, sa rapide prolifération et son omniprésence dans toutes les activités des entreprises sont assez récentes. Les auteurs révèlent quelques pratiques d'espionnage industriel datant du moyen âge, notamment : Carlton (1992) a mentionné le vol des secrets de fabrication des roues supérieures des Romains par les Celtes.

Certains auteurs l'imputent une origine militaire. Ces derniers affirment qu'il était utilisé à l'époque pour collecter des informations sur les ennemis de guerre, afin de préparer une stratégie permettant de gagner la guerre ou le conflit concerné. Les informations sur les ennemis sont confidentielles, par conséquent cette activité de renseignement militaire tombe naturellement sous le coup de l'espionnage industriel.
Pour plusieurs auteurs, l'espionnage industriel est utilisé dans l'art de la guerre et est connu sous cette étiquette.

Le développement dans le monde, les rivalités entre les différentes puissances, la mondialisation et bien d'autres phénomènes ont suscité la naissance des services secrets de renseignement dans les différents pays. L'information, qui constitue désormais un avantage stratégique, s'est revêtue d'une importance capitale et d'un intérêt indispensable que tout le monde convoite.

Ces différents services secrets gouvernementaux sont à l'affût des informations et ne cachent guère leur objectif de renseignement. Toutes les grandes puissances ont mis en place un service de renseignement.

Au-delà du renseignement par les entités macro-économiques, les entités micro-économiques ont fait leur entrée sur la scène. La rude concurrence, l'évolution des entreprises, la recherche de la performance et bien d'autres raisons expliquent la prolifération de l'espionnage industriel au sein des entités micro-économiques.

Les ressources se font rares, les entreprises ont recours à divers moyens pour booster leurs performances et ainsi assurer leur pérennité. L'information est pourtant un des moyens indispensables et les plus rapides pour se distinguer des autres concurrents. Certaines entreprises n'hésitent pas à recourir à des pratiques d'espionnage industriel pour dérober des informations susceptibles de leur apporter un quelconque avantage.

En somme, l'espionnage industriel est une pratique de jadis, mais s'est fait un renom au travers des cas illustrés durant ces dernières décennies. Les nouvelles technologies ont, sans l'ombre d'un doute, attisé la flamme de l'espionnage industriel. Cependant, nul n'est à l'abri des pratiques d'espionnage industriel, contrairement à ce que pensent plusieurs entreprises. Cette rapide évolution du phénomène doit alarmer les entreprises à ce qu'elles élaborent des stratégies efficaces et efficientes de lutte contre l'espionnage industriel.

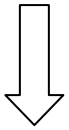
Section 2 : Intelligence économique et espionnage industriel : droit et éthique

Nombreux sont les écrits qui ne spécifient pas clairement la différence entre l'espionnage industriel et l'intelligence économique. Certains auteurs vont jusqu'à confondre les deux concepts et d'autres considèrent l'espionnage industriel comme l'étape supérieure de l'intelligence économique. Tous ces éléments montrent les difficultés de délimitation de la frontière entre les deux concepts. Par conséquent, nous nous proposons de délimiter leurs périmètres dans cette section.

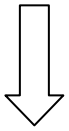
Ainsi, nous expliciterons le concept d'intelligence économique dans une première sous-section (1), ensuite nous aborderons dans une deuxième sous-section l'information qui est la matière première des concepts d'espionnage industriel et d'intelligence économique (2). Le recours au droit et à l'éthique pour délimiter la frontière entre l'espionnage industriel et l'intelligence économique fera l'objet de la troisième sous-section (3), et nous relèverons les limites de la distinction entre l'espionnage industriel et l'intelligence économique dans la quatrième sous-section (4).

L'architecture de la section est la suivante :

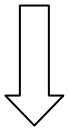
Le concept d'intelligence économique		
Qu'est-ce que l'intelligence économique ?	Les caractéristiques et les objectifs de l'intelligence économique	L'évolution de l'intelligence économique



L'information : la matière première des concepts d'espionnage industriel et d'intelligence économique		
Définition de l'information	Les différents types d'informations	Une frontière très nuancée entre l'espionnage industriel et l'intelligence économique



Le recours au droit et à l'éthique pour délimiter la frontière entre l'espionnage industriel et l'intelligence économique	
La persistance des nuances malgré les notions juridiques	L'introduction de l'éthique pour une délimitation claire



Les limites de cette distinction entre l'espionnage industriel et l'intelligence économique

1. Le concept d'intelligence économique

L'intelligence économique est un concept ayant des points communs avec l'espionnage industriel. Cependant, elle se distingue nettement de l'espionnage industriel et constitue un concept permettant de clarifier celui-ci. Il est nécessaire de spécifier les deux concepts afin d'écarter toute éventuelle confusion.

Considérée comme la fille légitime du renseignement (Alexandre-Leclair, 2001), l'intelligence économique constitue désormais une des premières préoccupations stratégiques des entreprises. Les multiples écrits scientifiques corroborent cette affirmation.

Sans prétendre présenter une revue de littérature du concept, nous allons dénombrer quelques définitions, qui nous serviront de base à la justification d'une explicitation claire du concept d'intelligence économique.

Ainsi, nous allons expliciter le concept d'intelligence économique dans une première sous-section (A), pour ensuite caractériser le phénomène tout en précisant ses objectifs (B), et nous terminons par son évolution (C).

A. Qu'est-ce que l'intelligence économique ?

Le Rapport Martre « Intelligence économique et stratégie des entreprises », qui reste la référence en France, définit l'intelligence économique comme « *l'ensemble des actions coordonnées de recherche, de traitement et de distribution en vue de son exploitation, de l'information utile aux acteurs économiques. Ces diverses actions sont menées légalement avec toutes les garanties de protection nécessaires à la préservation du patrimoine de l'entreprise, dans les meilleures conditions de qualité, de délais et de coût. L'information utile est celle dont ont besoin les différents niveaux de décision de l'entreprise ou de la collectivité, pour élaborer et mettre en œuvre de façon cohérente la stratégie et les tactiques nécessaires à l'atteinte des objectifs définis par l'entreprise dans le but d'améliorer sa position dans son environnement concurrentiel. Ces actions, au sein de l'entreprise, s'ordonnent en un cycle ininterrompu, générateur d'une vision partagée des objectifs à atteindre.* »[12].

Cette définition précise bien le type d'information, à savoir l'information utile qui a été recherchée, traitée et distribuée dans l'entreprise. Cette information utile va permettre de donner un avantage compétitif à l'entreprise. Ayant à sa disposition des informations

[12] Définition issue du Rapport du Commissariat Général du Plan (1994) « Intelligence économique et stratégie des entreprises » p12.

utiles, l'entreprise pourra mettre en place toutes les stratégies nécessaires pour se distinguer des autres entreprises. Le rapport met un accent sur la légalité des modalités de recueil des informations avec toutes les garanties de sécurité nécessaires à la préservation du patrimoine de l'entreprise.

Il spécifie également l'intelligence économique par quatre degrés de complexité :

- intelligence économique de niveau primaire ;
- intelligence économique de niveau secondaire ;
- intelligence économique tactique « dite de terrain » ;
- intelligence économique de puissance « ou stratégique ».

Le tableau ci-dessous contient les explications des différents degrés de complexité de l'intelligence économique :

Tableau 2 : Intelligence économique et ses 4 degrés de complexité selon le rapport Martre (1994)

Type d'intelligence économique	Spécificités
Intelligence économique de niveau primaire	Elle utilise l'information dont l'accessibilité est la plus grande. Elle est pratiquée à partir d'informations sur supports « papier » ou électroniques accessibles par des procédures élémentaires pouvant être maîtrisées par une personne non spécialiste. Elle n'appelle pas de traitement sophistiqué de l'information, qui est généralement déduite sous sa forme brute et définitive. La rareté est la moindre (la notion de rareté varie selon le pays ou l'industrie concernée).
Intelligence économique de niveau secondaire	Elle utilise l'information dont l'accessibilité est aisée ou de difficulté moyenne, mais qui peut être méconnue. Elle est aussi constituée le plus souvent d'informations écrites et publiées. La rareté est moyenne.
Intelligence économique tactique « dite de terrain »	Elle est pratiquée à partir d'informations dont l'accessibilité est plus difficile. Elle consiste en un traitement ou un effort de compréhension plus important. La rareté est plus importante. Il peut s'agir d'une information privée d'un concurrent, qui mettra maladroitement dans le domaine public. Les cabinets et courtiers en intelligence économique justifient leur existence par leur capacité à conduire une telle démarche d'intelligence économique.
Intelligence économique de puissance « ou stratégique »	Elle repose sur des informations dont l'accessibilité est sophistiquée, difficile et délicate. La démarche consiste par exemple dans l'identification des intentions et des capacités futures d'un concurrent. Elle concerne le plus souvent les horizons stratégiques de l'organisation. L'analyse des informations demande un effort important. La rareté est très grande.

En analysant les différents degrés de complexité de l'intelligence économique, la définition du rapport Martre ne semble pas exhaustive. Ceci s'explique tout simplement par les deux derniers types d'intelligence économique (tactique « dite de terrain », et de puissance « ou stratégique »), qui peuvent être qualifiés d'espionnage industriel, même si les informations ont été recueillies en toute légalité.

D'autres définitions[13] de l'intelligence économique :

« *L'intelligence économique englobe toutes les opérations de surveillance de l'environnement concurrentiel : veille, protection, manipulation de l'information (leurre, contre-information, ...), influence (...). La problématique de l'intelligence économique met l'accent sur les deux fossés culturels suivants : passage d'une culture fermée à une culture ouverte de l'information ; passage d'une culture individuelle à une culture collective de l'information* ».
Christian Harbulot, 1992.

« *L'intelligence économique est un outil capable de détecter des menaces et opportunités de toute nature dans un contexte de concurrence exacerbée [...] elle est avant tout la rencontre entre l'ignorance et la volonté de s'affranchir de cette ignorance. Elle est volonté de traduire cette ignorance en questions, puis en objectifs* ».
Bernard BESSON et Jean-Claude POSSIN, « Du renseignement à l'intelligence économique », Dunod, 1996.

« *L'intelligence économique est l'ensemble des moyens qui, organisés en système de management de la connaissance, produit de l'information utile à la prise de décision dans une perspective de performance et de création de valeur pour toutes les parties prenantes* ».
AFDIE (Association française pour le développement de l'intelligence économique), 2001.

Bournois *et al.* (2000)[14] proposent une définition de l'intelligence économique et stratégique émanant de leur recherche auprès de plusieurs dirigeants. Cette définition est la suivante : « *une démarche organisée, au service du management stratégique de l'entreprise visant à améliorer sa compétitivité par la collecte, le traitement d'informations et la diffusion de connaissances utiles à la maîtrise de son environnement (menaces et opportunités) : ce processus d'aide à la décision utilise des outils spécifiques, mobilise les salariés, et s'appuie sur l'animation de réseaux internes et externes* ».

[13] Définitions issues du Rapport Carayon (2003), « Intelligence économique, compétitivité et cohésion sociale ».
[14] Source de la définition « Alexandre-Leclair, L. (2001). La sûreté économique comme stratégie de contre intelligence économique. In *Veille stratégique scientifique et technologique. Colloque* (Vol 2 pp. 123 - 134) ».

Toutes ces définitions contribuent, certes, à la clarification du concept d'intelligence économique, mais elles sont globales ou restreintes dans le sens qu'elles ne précisent pas une frontière claire.

Par conséquent, le Syndicat Français de l'Intelligence Economique « SYNFIE », fondé le 14 décembre 2010 pour rassembler et représenter les professionnels de l'Intelligence Economique exerçant en France, a déterminé un périmètre plus représentatif du concept.

Le SYNFIE définit l'intelligence économique comme « *l'ensemble des activités coordonnées de collecte, de traitement et de diffusion de l'information utile aux acteurs économiques. Ces activités sont menées dans un cadre légal et éthique* »[15]. Cette définition élargit celle du rapport Martre par l'ajout de la notion d'éthique.

Cette dernière définition semble exhaustive, car elle délimite clairement les actions des professionnels d'intelligence économique. A cet effet, le SYNFIE a défini une charte d'éthique[16], qui constitue un code de bonne conduite des membres de la profession d'intelligence économique.

B. Les caractéristiques et les objectifs de l'intelligence économique

L'intelligence économique se distingue par le type d'informations recherchées, traitées et diffusées. Le mode de recueil des informations de l'intelligence économique est très important et constitue une condition indispensable permettant de qualifier un professionnel d'intelligence économique. Cette distinction est nécessaire afin de clarifier le périmètre d'action des professionnels d'intelligence économique.

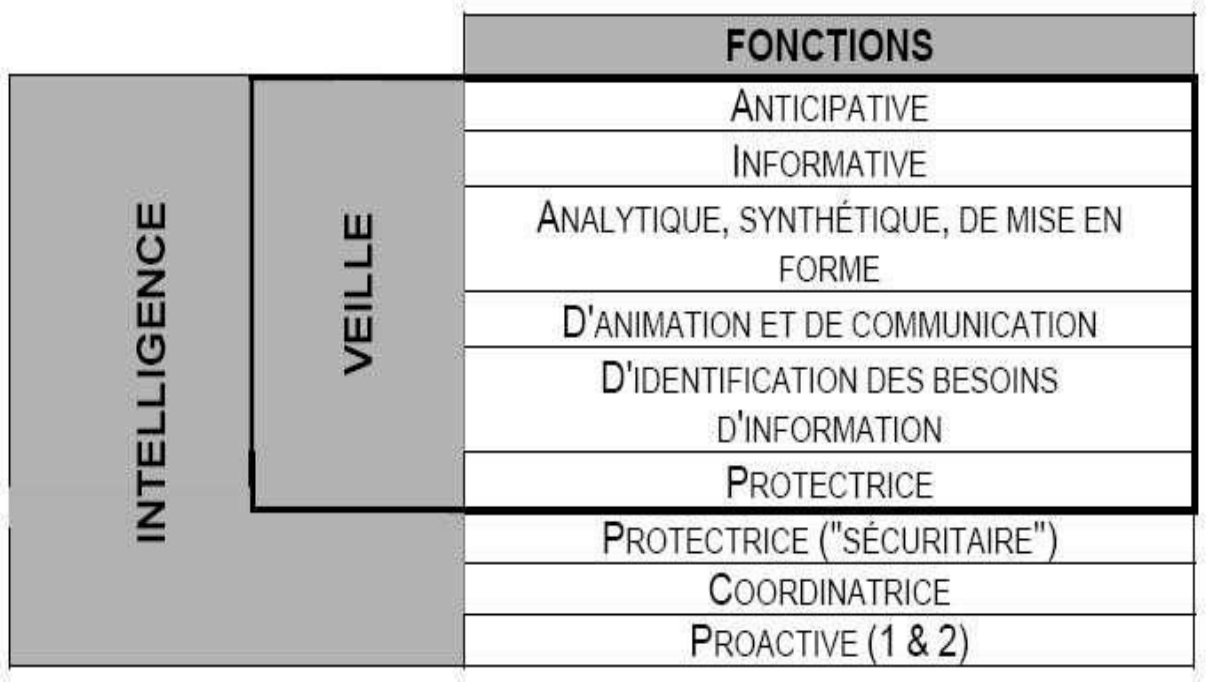
Cette délimitation nous paraît nécessaire dans le sens qu'elle permettrait de faciliter la compréhension sémantique de l'intelligence économique par rapport à certains concepts connexes.

L'intelligence économique se caractérise par des phases structurées partant de la recherche à la transformation des informations en informations utiles, qui seront mises à la disposition des membres de l'organisation.

[15] Définition sur le site du SYNFIE. Consultée le 23/06/2018. Disponible sur : https://www.synfie.fr/.
[16] La charte d'éthique du SYNFIE se trouve dans les annexes (annexe 1).

Pour Cohen (2007), l'intelligence économique se caractérise par plusieurs fonctions contenant celles de la veille. Cette caractérisation est intéressante, car elle montre le rôle de la veille, qui est un concept connexe de l'espionnage industriel.

Tableau 3 : Les fonctions de la veille et de l'intelligence stratégiques de Cohen[17]



Proactive 1 & 2 :

- 1 : mettre en œuvre des actions, faire des recommandations, des préconisations.
- 2 : objectifs d'impacts sur la compétitivité et la performance.

Les différentes fonctions de l'intelligence économique (et donc celles de la veille) sont pertinentes. Elles ont plutôt une allure de protection et d'organisation stratégique.

L'intelligence économique est un outil structuré, qui a pour objectifs de permettre aux entreprises de :

- surveiller leur environnement interne et externe ;
- repérer les menaces et les opportunités ;
- leur procurer des informations utiles afin d'aider à la prise des décisions ;
- avoir un avantage compétitif par rapport aux autres ;

[17] Cohen, C. (2007). Intelligence et performance : mesurer l'efficacité de l'Intelligence Economique et Stratégique (IES) et son impact sur la Performance de l'Organisation. *Vie & sciences de l'entreprise*, (1), 15-50.

- être à jour par rapport à l'évolution technologique…

C. L'évolution de l'intelligence économique

L'intelligence économique connait une évolution remarquable, surtout à l'essor des nouvelles technologies. Une autre raison de sa fulgurante évolution s'explique par la concurrence, qui devient de plus en plus rude.

Alain Juillet, dans la préface à l'ouvrage de Damien Bruté De Rémur (2006, page IX), résume son entrée en France par ces termes : « *importée des Etats-Unis par Robert Guillaumot, explicitée par le rapport signé par Henri Martre en collaboration avec Philippe Clerc et Christian Harbulot, positionnée sur l'échiquier mondial par Bernard Esambert, développée par quelques préfets visionnaires comme Rémy Pautrat, Claude Guéant ou Bernard Gérard, tout en s'appuyant sur les travaux et enseignements de quelques universitaires précurseurs, l'intelligence économique a mis dix ans pour devenir un concept reconnu. Le rapport Carayon a servi de détonateur pour la mettre à la mode et commencer à la prendre en compte dans la gestion des entreprises* »[18].

Selon Juillet (2004), l'intelligence économique est une pratique, dont les premières traces remontent au Moyen-âge, et a été développée par les anglais dans sa forme moderne, il y a environ un demi-siècle. Selon l'auteur, l'intelligence économique a fait l'objet d'un système par les japonais dans les années 50, puis conceptualisée par les américains au milieu des années 1980.

L'histoire de l'intelligence économique nous apprend qu'elle est née chez les anglo-saxons, qui utilisent des termes différents comme « Economic Intelligence » ou « Business Intelligence » ou encore « Competitive Intelligence ».

Selon le rapport Martre, le concept d'intelligence économique a connu son début sur le territoire français en 1994, avec la rédaction d'un rapport « *Intelligence économique et stratégie des entreprises* » par le Commissariat Général du Plan, plus connu sous l'appellation « rapport Martre ».

Le rapport Martre mentionne qu'elle existe en France depuis la troisième République : « *Il en va de même pour les actions d'intelligence économique menées par certaines banques*

[18] Moinet, N. (2010). Petite histoire de l'intelligence économique, une innovation « à la française ». L'harmattan, p65.

françaises sous la IIIe République qui étaient à la pointe de l'information stratégique dans les relations économiques internationales. Toutefois une pratique systématique du non-dit n'a pas laissé de traces cohérentes dans la culture d'entreprises françaises »[19]. Les pionniers de ce rapport ont voulu institutionnaliser le phénomène en France. Le point de départ institutionnel de l'intelligence économique en France est le rapport Carayon de 2003, à l'initiative des pionniers du premier rapport (Martre en 1994).

Cependant, les anglo-saxons sont connus comme les précurseurs de l'intelligence économique. Les français se sont ensuite intéressés au phénomène avec un peu de retard.

L'évolution rapide de l'intelligence économique peut s'expliquer par la mondialisation, les conditions de concurrence accentuées par la prolifération des acteurs aussi bien sur le plan national qu'international, la recherche de la performance, etc.

Aujourd'hui, l'intelligence économique semble indispensable pour faire face à la rude concurrence, ne serait-ce que pour être au même niveau que les autres organisations (s'informer et se mettre à jour). L'intelligence économique s'est encastrée dans toutes les entreprises (petites, moyennes et grandes). La différence réside au niveau de l'utilisation, car certaines entreprises l'utilisent de manière informelle[20].

Les nouvelles technologies ont rendu beaucoup d'informations accessibles, par conséquent la gestion de ce flux d'informations est devenue l'un des moteurs incontournables dans la conduite des stratégies.

[19] Rapport du Commissariat Général du Plan (1994), « Intelligence économique et stratégie des entreprises », p59.
[20] Des études montrent que plusieurs entreprises utilisent l'intelligence économique de manière informelle.

2. L'information : la matière première des concepts d'espionnage industriel et d'intelligence économique

L'information constitue la base commune entre l'espionnage industriel et tous ses concepts connexes. Cependant, le type d'information et les modalités de recueil dissocient les différents concepts. De nos jours, l'information est devenue pour les entreprises un moyen de se distinguer des autres entreprises. Plus une entreprise est en mesure de collecter l'information, plus elle élargit sa puissance.

Il est évident que l'information constitue un élément de compétitivité pour les entreprises. Elle est incontournable dans la gestion d'une structure et demeure un élément nécessitant la mise en œuvre d'une bonne stratégie de management.

A. Définition de l'information

L'information est un terme polysémique, car il existe plusieurs définitions qui peuvent être divergentes ou convergentes. Parmi ces différentes définitions, nous pouvons retenir quelques-unes.

Selon Mongin et Tognini (2015)[21], l'information correspond à « *un ensemble de données non structurées, organisées pour donner forme à un message, résultant d'un contexte donné et donc parfaitement subjectif* », et les auteurs définissent une donnée comme « *un élément fondamental et objectif, qualificatif ou quantitatif, servant de base à un raisonnement ou à la réalisation de traitement* ».

Bulinge et Pepin (2013)[22] proposent la définition suivante : « *une information est le résultat d'un processus intelligent de mise en forme d'une représentation éventuelle (factuelle ou non), dont la communication est censée réduire ou dénouer une incertitude (élément de connaissance), résoudre une alternative ou éclairer une problématique plus ou moins complexe (aide à la décision)* ». Cette définition renvoie à l'information stratégique, puisqu'elle facilite la prise de décision.

Nous pouvons retenir des différentes définitions que l'information est un élément indispensable dans le fonctionnement d'une entreprise. Elle représente un noyau qui facilite

[21] Mongin, P., & Tognini, F. (2015). *Petit manuel d'intelligence économique au quotidien. 2éd : Comment collecter, analyser, diffuser et protéger son information*. Dunod. p108.
[22] Bulinge, F., & Pepin, J. F. (2013). Intelligence économique: l'information au cœur de l'entreprise. Editions Nuvis. p17.

les différents échanges dans une structure. Il est important de préciser la signification de l'information, car elle constitue l'élément central de l'intelligence économique et de l'espionnage industriel.

Les avantages, que procure l'information à une entreprise, sont nombreux et nécessaires à la survie de celle-ci. Il s'agit notamment de :

- repérer les opportunités ;
- identifier les forces et faiblesses ;
- connaitre le positionnement de l'entreprise par rapport aux concurrents ;
- conquérir un nouveau marché ;
- avoir une bonne relation avec les parties prenantes de l'entreprise…

B. Les différents types d'informations

Plusieurs classifications de l'information ont été élaborées et permettent d'avoir une vision claire du phénomène.

Selon la classification établie par le rapport du groupe présidé par René Mayer (Commissariat général au plan « *Information et compétitivité* », 1990), il existe trois familles d'informations :

- les informations dites générales ;
- celles à finalité pédagogique ;
- celles qui servent à travailler : l'information juridique, médicale, financière ; l'information sur les marchés, les innovations ; l'information scientifique et technique, industrielle, commerciale, sociale…

Une deuxième classification est celle du rapport Martre qui correspond aux 4 degrés de complexité de l'intelligence économique :

- un premier niveau est dit primaire : dans ce cas l'accessibilité à l'information est plus grande et la rareté est faible.
- un deuxième niveau dit secondaire : où l'accessibilité de l'information est de faible difficulté et la rareté est moyenne.

- un troisième niveau dit tactique ou de terrain : dont l'accessibilité est difficile et la rareté importante.

- un quatrième niveau dit de puissance ou stratégique : dont l'accessibilité est sophistiquée, délicate et la rareté très grande.

Une autre classification est celle de Bonnivard (1998)[23], qui distingue trois types d'informations utiles (classées selon leur degré de complexité et de rareté) aux acteurs de l'entreprise. Il s'agit des :

- informations publiques : ce qu'on appelle aussi « informations ouvertes », car elles sont libres d'accès et d'exploitation, par exemple les banques de données, les publications scientifiques ou économiques, etc. A ce stade, l'intelligence économique est qualifiée de "primaire" ou "secondaire" ;

- informations réservées : toutes les informations ayant un accès plus difficile. C'est le cas des brevets, des droits d'auteurs, etc. En effet, pour exploiter ce type d'informations, on est soumis à l'autorisation du titulaire du droit. Appartiennent aussi à ce niveau d'informations, les interviews, les indiscrétions, les écoutes, les informations privées qu'un concurrent mettra maladroitement dans le domaine public à l'occasion d'un salon professionnel, de rencontres, etc. A ce stade, l'intelligence économique est qualifiée de "tactique" ;

- informations confidentielles : c'est le cas des informations protégées par le secret. On peut citer par exemple : les secrets de fabrication, les secrets commerciaux tels que : les commissions accordées aux distributeurs, les études de marchés. Le recueil de ces informations est particulièrement délicat. A ce stade, l'intelligence économique est qualifiée de "stratégique ou de puissance".

Ces différentes classifications caractérisent les types d'informations entrant dans le cadre de l'intelligence économique. Nous pouvons remarquer que certaines informations, considérées comme confidentielles, sont incluses dans celles-ci. Il ressort de cette imprécision un problème de délimitation entre l'intelligence économique et l'espionnage industriel.

[23] Alexandre-Leclair, L. (2001). La sûreté économique comme stratégie de contre intelligence économique. In *Veille stratégique scientifique et technologique. Colloque* (Vol 2 pp. 123 - 134).

L'intelligence économique, qui comporte un volet de protection de l'information, peut s'avérer offensive (l'intelligence économique qualifiée de tactique ou de puissance). Ce type d'intelligence économique s'apparente à l'espionnage industriel.

En plus de ces classifications, le secret et le renseignement sont également des informations utilisées dans le cadre de l'intelligence économique et de l'espionnage industriel.

Bulingue et Pepin (2013) définissent le secret comme « *une information, une connaissance occultée, gardée, protégée du regard des autres, de ceux qui n'ont pas le droit de la connaitre* ». C'est donc une information, dont l'inaccessibilité fait l'objet d'une action volontaire. Sans rentrer dans une explication étymologique du terme, la caractéristique du secret est l'espace cryptique, c'est-à-dire l'espace au sein duquel le secret circule ouvertement. Cet espace cryptique constitue une zone réservée aux seuls détenteurs du secret.

Le secret peut avoir plusieurs formes selon le domaine, le secteur, le type d'activité, comme illustration nous pouvons citer : le secret industriel, le secret commercial, le secret médical, le secret d'affaires, etc.

Barry (1998) mentionne les secrets commerciaux et affirme qu'ils sont largement définis selon la loi : « *un secret commercial désigne toutes les formes et types d'informations financières, commerciales, scientifiques, techniques, économiques ou d'ingénierie, y compris les schémas, les plans, les compilations, les programmes, les formules, les dessins, les prototypes, les méthodes, les procédés, les procédures, les programmes ou les codes, qu'ils soient matériels ou immatériels, et qu'ils soient ou non stockés, compilés ou mémorisés physiquement, électroniquement, graphiquement, photographiquement ou par écrit ».*

Par ailleurs, le renseignement est défini par le dictionnaire Larousse (2018) de deux manières :

- comme une *indication, information, éclaircissement donnés sur quelqu'un, quelque chose (exemple : donner des renseignements sur une affaire) ;*
- *comme une activité visant à acquérir et à tenir à jour la connaissance de l'ennemi ou des puissances étrangères.*

A la base, le renseignement a une origine militaire dans le sens que certains auteurs[24], tels que Silberzahn (1995) et Lacoste (1997) le considèrent comme la recherche d'information sécrète. Ainsi, l'acception militaire le définit comme : « *l'information concernant l'ennemi* » (Dictionnaire Petit Robert, 1990) ; et comme : « *l'ensemble des informations dont le commandement a besoin pour élaborer sa ligne de conduite* » (Dictionnaire Hachette, 1998).

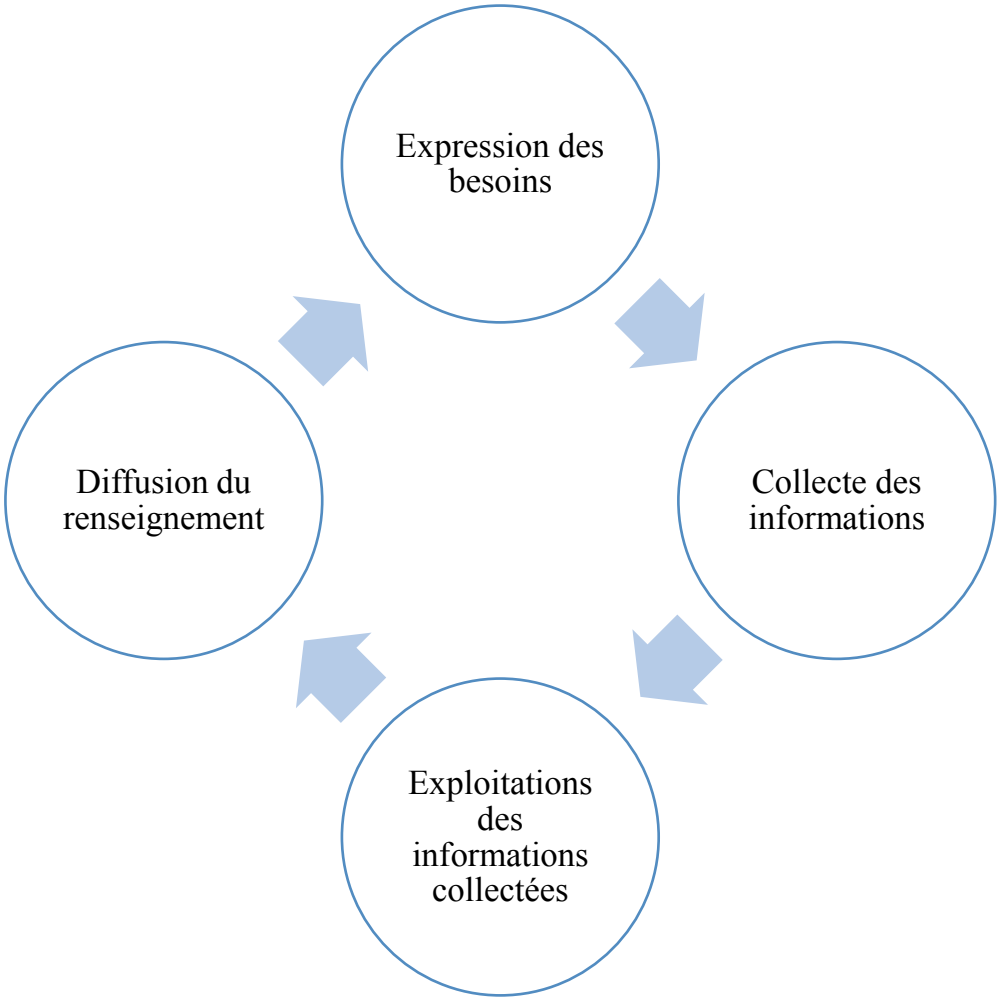
Baud (1998) définit le renseignement comme : « *une information évaluée et exploitée ayant passé le cycle du renseignement et prête à être diffusée à un client* ».

L'analyse de ces définitions nous apprend que l'information correspond au renseignement brut, qui passe par le cycle du renseignement pour devenir du renseignement. Selon Bruté De Rémur (2016), le cycle du renseignement ou le cycle de production du renseignement est un processus itératif et continu comportant quatre phases :

- l'expression des besoins ;
- l'acquisition (ou collecte des informations);
- l'exploitation (traitement et analyse des informations collectées) ;
- la diffusion du renseignement (ou diffusion des informations traitées et analysées).

[24] Bulinge, F., & Pepin, J. F. (2013). Intelligence économique: l'information au cœur de l'entreprise. Editions Nuvis. p.60.

Figure a : Le cycle du renseignement de Bruté De Rémur (2016)



A présent, nous faisons la distinction entre une information, une donnée, un renseignement et un secret. Le point commun entre ces différents éléments est qu'ils sont utilisés dans les pratiques d'intelligence économique et d'espionnage industriel.

Cependant, des questions subsistent, notamment :

- Où s'arrête l'intelligence économique ?
- Où commence l'espionnage industriel ?
- Les deux concepts sont-ils indissociables ?

C. Une frontière très nuancée entre l'espionnage industriel et l'intelligence économique

Au regard des différentes définitions de l'espionnage industriel et de l'intelligence économique, il est évident que les deux concepts sont confondus, car une frontière délimitant clairement les deux phénomènes n'est pas définie par les différents auteurs.

Rechercher, collecter, analyser et utiliser les informations (toutes ces actions menées stratégiquement) constituent le socle commun entre l'espionnage industriel et l'intelligence économique. Cette remarque accentue le problème de délimitation entre les deux pratiques. S'ajoutent à cela, des imprécisions flagrantes comme certains types d'intelligence économique qui entrent clairement dans le cadre de l'espionnage industriel (intelligence économique qualifiée de tactique et celle qualifiée de puissance). Ces deux formes admises comme de l'intelligence économique offensive sont complètement indissociables des pratiques d'espionnage industriel.

Cependant, nous allons utiliser les concepts de droit et d'éthique pour délimiter une frontière claire entre l'espionnage industriel et l'intelligence économique.

3. Le recours au droit et à l'éthique pour délimiter la frontière entre l'espionnage industriel et l'intelligence économique

Pour préciser les périmètres des deux pratiques, nous allons introduire les notions de légalité et d'éthique pour réconforter la distinction. Dans cette sous-section, nous allons préciser la persistance des nuances malgré une délimitation légale (A), pour ensuite clarifier le périmètre au travers des notions d'éthique (B).

A. La persistance des nuances malgré les notions juridiques

En rapprochant certaines définitions de l'espionnage industriel et de l'intelligence économique, la différence est inexistante, car ils se caractérisent par les mêmes pratiques. A cet effet, plusieurs auteurs et chercheurs se sont penchés sur les deux concepts, afin de définir une frontière claire.

Les premiers éléments de distinction constituent la légalité des pratiques de collecte d'informations. Plusieurs organismes et auteurs[25] ont distingué les deux concepts en adossant :

[25] En se référant à certaines définitions données ci-haut des deux concepts.

- les pratiques de collecte illégales à l'espionnage industriel ;
- les pratiques de collecte légales à l'intelligence économique.

A ce stade, une question pertinente se hisse, à savoir : cette distinction est-elle suffisante pour délimiter une frontière claire entre l'espionnage industriel et l'intelligence économique ?

Pour répondre à cette question, nous analysons cet exemple suivant : une entreprise récupère une information confidentielle sur papier dans une poubelle de son concurrent située au bord de la voie publique.

Deux questions permettent d'analyser cet exemple, à savoir :

- Cette entreprise a-t-elle effectué un acte illégal ?
- Est-ce de l'espionnage industriel ?

Les réponses des deux questions nous clarifient la capacité d'appréhension de la distinction entre les deux concepts par le caractère légal ou illégal des pratiques de collecte d'informations.

Réponse à la question « cette entreprise a-t-elle effectué un acte illégal ? » : aucun texte légal en France n'interdit de récupérer des papiers dans une poubelle située au bord de la voie publique, par conséquent la pratique de collecte de cette entreprise n'est pas illégale.

Réponse à la question « est-ce de l'espionnage industriel ? » : l'acte constitue de l'espionnage industriel, car l'entreprise s'est procurée d'une information confidentielle de son concurrent.

En somme, toutes les pratiques de collecte d'informations entrant dans le cadre de l'espionnage industriel ne sont pas illégales. Il existe énormément de moyens de se procurer des informations sécrètes d'un concurrent qui demeurent dans la légalité.

Il en résulte de cette analyse l'insuffisance du caractère légal comme moyen de distinction entre l'espionnage industriel et l'intelligence économique.

B. L'introduction de l'éthique pour une délimitation claire

L'échec d'une délimitation claire par la légalité a conduit bon nombre d'organismes et d'auteurs à trouver d'autres critères de distinction entre l'espionnage industriel et l'intelligence économique. Ceci montre le problème de délimitation entre les deux concepts.

Le deuxième élément de distinction permettant de réconforter une délimitation claire entre l'espionnage industriel et l'intelligence économique constitue les différents principes d'éthique, notamment sur les pratiques de recueil d'informations.

L'éthique se définit comme : « *l'ensemble des principes moraux qui sont à la base de la conduite de quelqu'un* »[26].

Ce critère de distinction crée un fossé entre les deux pratiques et spécifie une frontière claire, en introduisant les principes d'éthique dans les méthodes de recueil d'informations des professionnels d'intelligence économique. Cependant, les espions ne peuvent appliquer ces principes, sinon ils seraient des simples praticiens d'intelligence économique.

Ainsi dépourvu des principes d'éthique, l'espionnage industriel se distingue clairement de l'intelligence économique. Les espions, qui sont à l'affût des informations confidentielles, peuvent collecter celles-ci sans tomber sous le coup des textes légaux et réglementaires, mais ils ne peuvent, en aucun cas, recueillir des informations sécrètes sans tomber sous le coup des principes d'éthique.

Cette affirmation se justifie par la simple raison suivante : les informations confidentielles ont un caractère secret, par conséquent elles se caractérisent par un espace cryptique. Cet espace, étant réservé à la personne ou au groupe de personnes, ne doit pas être violé. En s'invitant dans cet espace cryptique, l'espion tombe sous le coup des principes d'éthique.

Ce deuxième critère de distinction réconforte la délimitation entre les deux pratiques. A cet effet, plusieurs organismes ont défini des principes d'éthique pour une protection tant interne qu'externe des informations confidentielles.

Le syndicat français de l'intelligence économique (SYNFIE) a défini une charte d'éthique érigeant le code de bonne conduite des membres de la profession (en annexe 1).

[26] Définition du dictionnaire Larousse 2018.

4. Les limites de cette distinction entre l'espionnage industriel et l'intelligence économique

Une frontière entre l'espionnage industriel et l'intelligence économique est définie, en introduisant les critères de légalité et d'éthique dans les méthodes de collecte d'informations. Cependant, cette distinction a des limites notamment sur un plan pratique.

Certaines collectes d'informations confidentielles passant au filtre des textes légaux et réglementaires, les principes d'éthique permettent certainement de délimiter théoriquement la frontière entre l'espionnage industriel et l'intelligence économique, mais qu'en est-il sur un plan pratique ?

L'accès aux informations est devenu très facile, surtout avec le réseau Internet et les outils informatiques. Les espions peuvent recueillir des informations par des moyens dépourvus d'éthique, ensuite prétendre que celles-ci ont été collectées en toute légalité et respectant les principes d'éthique.

Par conséquent, il sera difficile de prouver le non-respect de ces principes à l'encontre des espions. C'est une limite nuançant la distinction entre l'espionnage industriel et l'intelligence économique.

Par ailleurs, beaucoup d'entreprises méconnaissent leurs vulnérabilités et ne se sentent pas concernées par l'espionnage industriel. Cette négligence réconforte les espions dans leurs collectes d'informations, car ils n'ont quasiment pas d'obstacles pour dérober les informations confidentielles. S'ajoutent à cette sous-estimation des entreprises, les limites juridiques et le problème de preuve du respect des principes d'éthique.

Tous ces points évoqués constituent des raisons valables, qui doivent alarmer les entreprises à ce qu'elles élaborent des outils et méthodes de gestion pour se protéger contre l'espionnage industriel.

Section 3 : La nécessité d'introduire le contrôle de l'espionnage industriel dans la gestion de l'entreprise

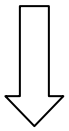
Les rares études scientifiques, la presse et d'autres exemples concrets nous montrent clairement et de façon détaillée les effets néfastes de l'espionnage industriel sur les économies et les entreprises. Ces conséquences désastreuses citées ci-haut exigent, ne serait-ce que dans un but de survie de certaines entreprises, une main mise sur la gestion de l'espionnage industriel.

La stratégie de cette gestion passe nécessairement par le contrôle ou la maitrise de l'espionnage industriel dans le but d'atténuer, voire éliminer, ses répercussions sur les économies et les entreprises.

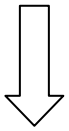
Nous abordons dans ce cadre les deux types de protection, à savoir : la protection juridique et la protection assurée par les entreprises elles-mêmes. Ensuite, nous étudions une perspective d'amélioration de la gestion de l'espionnage industriel.

L'architecture de la section est la suivante :

Espionnage industriel et protections juridiques	
Des protections juridiques diversifiées	Les limites des protections juridiques



Espionnage industriel et Contrôle interne	
Elargissement des protections juridiques : les protections techniques	Les limites et perspectives d'amélioration des protections techniques



Espionnage industriel et Contrôle de gestion ?

1. Espionnage industriel et protections juridiques

Les conséquences de l'espionnage industriel sur les économies et les entreprises ont conduit les différents organismes internationaux et gouvernements à élaborer des textes réglementaires et juridiques, afin de cerner le fléau.

Ainsi, nous allons expliciter la diversification des protections juridiques (A), pour ensuite exposer les limites desdites protections (B).

A. Des protections juridiques diversifiées

Pour ce faire, les organisations internationales et les Etats n'ont pas failli à leurs devoirs, dans le sens où des protections juridiques contre l'espionnage industriel ont été élaborées. Ces différentes mesures de protection sont cependant variables selon les gouvernements.

Ainsi, le rapport de Frantz (2014) révèle que d'un point de vue global, il ressort des études menées par la Commission européenne que seule la Suède dispose d'une loi exclusivement consacrée à la répression des atteintes aux secrets d'affaires. Quelques pays ont prévu, au sein de textes plus généraux, des dispositions législatives spécifiques à ce sujet (tel est par exemple le cas de l'Autriche, de la Hongrie ou de la Lettonie, dont les dispositions relatives aux secrets d'affaires relèvent du droit de la concurrence déloyale, ou du Portugal et de l'Italie, qui règlent la question par des dispositions incluses dans leur code de propriété intellectuelle).

D'autres n'accordent aucune protection particulière, mais appréhendent néanmoins les violations de secrets d'affaires par le biais de principes fondamentaux du droit (tel est le cas, notamment, au Royaume-Uni, en Irlande, aux Pays-Bas, à Malte ou encore, en France, où la question est, pour l'essentiel, réglée par le recours aux principes généraux du droit de la responsabilité).

En France, il n'existe aucun texte de loi explicite qui s'applique à la protection des secrets de l'entreprise condamnant l'expropriation de biens informationnels par espionnage industriel, exception faite du contenu de l'article[27] 410-1 du Code pénal et l'atteinte aux intérêts fondamentaux de la Nation.

[27] Art. 410-1 - "Les intérêts fondamentaux de la Nation s'entendent au sens du présent titre de son indépendance, de l'intégrité de son territoire, de sa sécurité, de la forme républicaine de ses institutions, des moyens de sa défense et de sa diplomatie, de la sauvegarde de sa population en France et à l'étranger, de l'équilibre de son milieu naturel et de son environnement et des éléments essentiels de son potentiel scientifique et économique et de son patrimoine culturel".

En renfort de ces dispositions légales des Etats et des organismes internationaux, plusieurs instruments juridiques sont à la portée des entreprises pour réconforter leur protection contre l'espionnage industriel.

Il est question des instruments de la propriété intellectuelle, notamment des brevets, des clauses de confidentialité, des clauses de non concurrence, des autres moyens de protection de l'innovation technologique, soit des dessins et des modèles, des copyrights et des droits d'auteurs, etc. (Corbel, 2006). La loi prévoit les exceptions particulières de protection, qui sont signifiées dans les textes législatifs et réglementaires du code de la propriété intellectuelle (Articles L 112-1, L112-2, etc.).

Légalement, l'espionnage industriel n'est pas puni en tant que tel, ce sont les moyens répréhensibles utilisés pour obtenir les informations (secrets, procédés de fabrication, etc.) qui sont punissables. Dans le tableau suivant, nous pouvons retrouver quelques exemples de textes de loi condamnant les moyens répréhensibles en France :

Tableau 4 : Quelques exemples de textes de loi condamnant les moyens répréhensibles en France

Moyens illicites	Textes de loi
Corruption	Article 445-1 et 2 du Code pénal
Action de vol du matériel supportant le savoir-faire	Article 311-1 et suivants du Code pénal
Violation du secret professionnel	Article 226-13 du code pénal
Violation du secret de fabrique	Articles L 1227-1 du code du travail et 621-1 du code de la propriété intellectuelle
Abus de confiance dans le cadre de relations contractuelles	Article 314-1 et suivants du Code pénal

Au-delà des articles, plusieurs arrêts de la jurisprudence s'appliquent sur les moyens illicites inhérents à l'espionnage industriel. Le tableau suivant illustre quelques arrêts de la jurisprudence condamnant les moyens répréhensibles en France :

.

Tableau 5 : Quelques arrêts de la jurisprudence condamnant les moyens répréhensibles en France

Moyens illicites	Arrêts de la Jurisprudence
Est condamné le fait de débaucher un employé en lui proposant une rémunération très élevée dans le but de connaître les secrets d'un concurrent.	Arrêt de la Chambre sociale du 07/07/1960
Fait figure d'acte d'espionnage industriel répréhensible, le fait, pour un commerçant, de se procurer par l'intermédiaire d'un préposé transportant les produits d'une maison concurrente, la liste des clients de cette dernière.	Arrêt du TGI de Lure, du 13/04/1962
L'accès et le détournement des connaissances contre la volonté de leur détenteur, caractérisant l'espionnage industriel, aussi appelé captation du savoir-faire d'autrui.	Arrêt de la Cour d'appel de Paris du 09/04/1992
Le cas d'usurpation répréhensible le plus évident reste celui de personnes extérieures à l'entreprise, pratiquant des actes d'espionnage industriel ou commercial.	Arrêt de la Cour de Paris du 09/04/1992
la Cour de cassation est prête à appliquer des textes généraux pour sanctionner de tels faits d'appréhension, avec les dispositions relatives à l'abus de confiance sur le détournement de « projet ».	Arrêt de la Chambre criminelle du 22/09/2004 ; voire même au vol d'informations Arrêt de la Chambre criminelle du 21/01/2003

Tous ces moyens légaux constituent des dispositions à la portée des entreprises pour faire face aux incidents du fléau. Cependant, les espions n'en demeurent pas dissuadés et multiplient les moyens permettant de contourner lesdites réglementations légales.

Chaque pays appréhende l'espionnage industriel selon ses réalités locales. A cet effet, des protections juridiques ont été élaborées par les Etats et les organismes internationaux, afin de lutter contre le phénomène.

Le tableau ci-dessous illustre chronologiquement quelques protections juridiques des différents pays et organismes internationaux :

Tableau 6 : Quelques protections juridiques et autres mesures des pays et organismes internationaux contre l'espionnage industriel

Etats et Organismes internationaux (année)	Protections juridiques et autres mesures
LICCD : Ligue Internationale contre la concurrence déloyale, (1969-1976).	"Violation des secrets industriels et commerciaux en matière concurrentielle" (Congrès Vienne 1969, Genève 1972, Rome 1974, Munich 1976). (Alexandre-Leclair, 2001).
Etats - Unis : l'*Uniform Trade Secrets Act,* UTSA, (1979).	Ce texte, proposé par l'*Uniform Law Commission* (ULC) en 1979 n'est pas obligatoire pour les Etats américains ; toutefois 47 d'entre eux ainsi que le District de Columbia, Porto Rico et les Iles Vierges Américaines l'appliquent dans leur législation nationale (Frantz, 2014).
Suède (1990).	Loi 1990:409 du 31 mai 1990 relative à la protection des secrets commerciaux.
Multilateral treaty of Canada, Mexico, and the United States : North American Free Trade Agreement (NAFTA) (1992).	En 1992, le Canada, le Mexique et les États-Unis ont signé l'accord de libre-échange nord-américain « ALENA » (en anglais NAFTA : North American Free Trade Agreement) en tant que premier traité multilatéral contenant des dispositions protégeant les secrets commerciaux. Cela a été complété par le traité de 1994 créant l'organisation mondiale du commerce avec son annexe IC, accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (plus communément appelé accord sur les TRIPS : Trade-Related aspects of Intellectual Property Rights). L'article 39 de l'Accord sur les TRIPS prévoit la protection des renseignements non divulgués. Le préambule énonce spécifiquement son objectif : "réduire les distorsions et les entraves au commerce international, en tenant compte de la nécessité de promouvoir une protection effective et adéquate des droits de propriété intellectuelle". Les secrets commerciaux sont définis comme des informations non divulguées et sont protégés en vertu du présent accord.
Japon (1993).	Loi sur la prévention de la concurrence déloyale n°47, du 19

	mai 1993, article 2, § (iv) à (ix) : le Japon prévoit également des mesures de nature à satisfaire cet objectif. En droit japonais, sont des actes de concurrence déloyale l'acquisition, l'utilisation et la divulgation frauduleuses de secrets d'affaires (Frantz, 2014).
Chine : Loi sur la protection contre la concurrence déloyale du 2 septembre 1993.	La Chine, à l'instar du Japon, aborde les atteintes aux secrets d'affaires sous l'angle de la concurrence déloyale. Ainsi, la loi chinoise sur la concurrence déloyale prévoit une définition des secrets commerciaux protégés et l'existence d'un droit pour leur détenteur d'obtenir des mesures d'injonction ou de réparation en cas de violation. Les manquements aux secrets commerciaux sont également sanctionnés par l'autorité administrative et incriminés par le droit pénal (la loi sur la protection contre la concurrence déloyale ne prévoit pas expressément cette possibilité, mais la jurisprudence chinoise a pu ordonner de telles mesures sur le fondement de l'article 100 de la Loi de Procédure civile réformée en 2012), (Frantz 2014).
Etats-Unis : Economic Espionage Act of 1996 (ou Cohen Act), (L. 104-294) du 11 octobre 1996, amendé par le « Theft of Trade Secrets Clarification Act of 2012 » (L. 112–236) du 28 décembre 2012.	La Loi sur l'espionnage économique est entrée en vigueur le 14 octobre 1996 : la Loi interdit de nombreuses actions. Entre autres, la loi interdit expressément de voler, sans autorisation, de s'approprier, de prendre, de dissimuler, de copier, de reproduire, de dessiner, de photographier, de télécharger, de modifier, de détruire, de photocopier, de répliquer, de transmettre, poster, communiquer ou transmettre les secrets commerciaux d'autrui. La Loi sur l'espionnage économique rend également illégale la réception, l'achat ou la possession de secrets commerciaux en sachant qu'ils ont été volés ou appropriés, obtenus ou convertis sans autorisation. Il y a deux sections principales de la Loi : 18 U.S.C. § 1831 (a) criminalise le vol de secrets d'affaires au profit d'une puissance étrangère, d'une société ou d'un individu ; 18 U.S.C. § 1832 incrimine le vol domestique à des fins commerciales ou économiques. Une personne peut être condamnée à une amende pouvant aller

	jusqu'à 250 000 $ et être emprisonnée pendant 10 ans ou à une amende pouvant aller jusqu'à 500 000 $ et emprisonnée pendant 15 ans si le défendeur voulait ou savait que le vol profiterait à une entité étrangère. Une entreprise peut être condamnée à une amende pouvant aller jusqu'à 5 millions de dollars pour avoir enfreint la Loi, ou jusqu'à 10 millions de dollars si elle a agi avec l'intention ou la connaissance qu'une entité étrangère bénéficierait (Halligan, 2008).
Administration strategy on mitigating the theft of U.S. trade secrets, the U.S. Government (2013)	Éléments d'action de la stratégie : 1. Concentrer les efforts diplomatiques pour protéger les secrets commerciaux à l'étranger ; 2. Promouvoir les meilleures pratiques volontaires par l'industrie privée pour protéger les secrets commerciaux ; 3. Améliorer les opérations d'application de la loi.
Commission européenne, 28 novembre 2013, COM(2013) 813 final.	Dépôt d'une proposition de directive « *sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites* ». Elle entend protéger les positions concurrentielles des entreprises, leur capacité d'innovation, notamment dans le domaine de l'innovation collaborative, et stimuler l'emploi pour favoriser le marché intérieur et la croissance en Europe. A cette fin, le texte vise à assurer la convergence des droits civils nationaux en ce qui concerne la détermination du caractère illicite des actes d'appropriation, d'utilisation et de divulgation de secrets d'affaires, les voies de recours, et la protection de la confidentialité de ces secrets pendant et après une action en justice. (Frantz, 2014).

B. Limites des protections juridiques

Les textes de loi s'avèrent très insuffisants dans les différents pays pour couvrir les risques d'espionnage. Cependant, il faut reconnaître les efforts des différents gouvernements et organismes internationaux qui ont introduit des points de départ considérables dans la lutte contre l'espionnage industriel.

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. Cependant, ces instruments présentent certaines limites et s'avèrent insuffisants pour répondre à l'ensemble des besoins de sécurité de l'entreprise.

Toutes ces 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 (Commission du droit de l'entreprise et avec la collaboration de l'Institut de Recherche en Propriété Intellectuelle, 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 ; Crane, 2005), mentionnent les vides juridiques, en illustration nous avons : des éléments non couverts par nature[28] (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.

[28] Article L. 611-10 Code de la Propriété Intellectuelle : « 1. Sont brevetables les inventions nouvelles impliquant une activité inventive et susceptibles d'application industrielle. 2. Ne sont pas considérées comme des inventions au sens du premier alinéa du présent article notamment : a) Les découvertes ainsi que les théories scientifiques et les méthodes mathématiques ; b) Les créations esthétiques ; c) Les plans, principes et méthodes dans l'exercice d'activité intellectuelles, en matière de jeu ou dans le domaine des activités économiques, ainsi que les programmes d'ordinateurs ; d) Les présentations d'informations ».

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.

Suite à ces défaillances législatives, les entreprises se voient contraintes de prendre le relais afin d'affronter elles-mêmes l'espionnage industriel (Coskun 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.

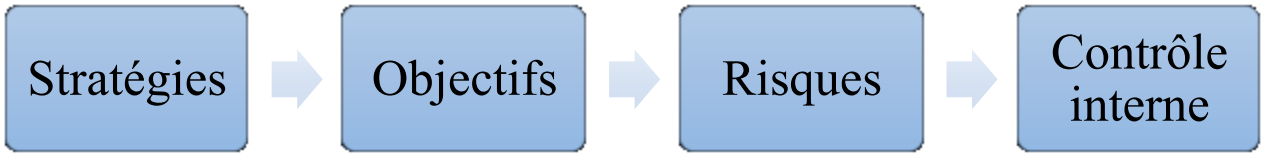
Par ailleurs, rares sont les entreprises qui mettent en place une stratégie de protection contre l'espionnage industriel, comme l'illustrent Coskun Samli et Jacobs (2003). Comment peut-on expliquer ce comportement des entreprises ? Est-ce par méconnaissance ou par négligence de l'espionnage industriel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

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.

Pour certaines entreprises, il faudrait disposer des outils industriels, qui coûtent pour répliquer la même chose et les outils industriels coûtent très chers. Si on a recours aux produits agricoles de la région, cela constitue de facto une protection ; le vol est peu envisageable en vertu de coûts dissuasifs liés au transport.

2. Espionnage industriel et Contrôle interne

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 représenté par le processus suivant :



Il peut être en amont (contrôle de prévention) ou en aval (contrôle de détection). Pour le référentiel COSO[29], 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 ont conduit les entreprises à mettre en place des mesures de protection et de discipline internes, permettant de contrer l'espionnage industriel. Ainsi, nous allons aborder deux points dans cette rubrique : un premier point présentant les différentes

[29] 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.

protections techniques (A), et un second point mettant en exergue les limites desdites protections et l'ouverture sur des perspectives d'amélioration (B).

A. Elargissement des protections juridiques : les protections techniques

Le Contrôle Interne désigne, dans cette optique, l'ensemble des outils et méthodes de protection mis en œuvre contre l'espionnage industriel avant sa survenance. Nous distinguons les outils et méthodes de protection :

- défensifs ;
- offensifs.

Le recours aux deux catégories de protections diffère selon les caractéristiques et les types des entreprises. Les secrets d'affaires procurent aux espions un avantage compétitif sur leurs concurrents. De ce fait, certaines entreprises protègent leurs informations au travers des outils et méthodes de protection empêchant l'accès aux informations sensibles (protection défensive).

Par ailleurs, pour se protéger, d'autres entreprises n'hésitent pas à mettre leurs espions sur des pistes erronées, en leur laissant accéder aux informations truquées (protection offensive). Les différents types de protections offensives sont :

- La dissimulation, elle consiste à conserver les informations sensibles de l'entreprise en secret, c'est-à-dire les conserver au sein de l'organisation sans prétendre à la souscription d'un brevet. Considérée comme préalable à la souscription d'un brevet, la dissimulation est utilisée à très long terme par certaines entreprises, qui s'exposent ainsi à un risque considérable (puisqu'elles ne bénéficient pas de la protection juridique).
- L'intoxication ou la désinformation, elle consiste à mettre délibérément les concurrents sur des fausses pistes, en leur laissant accéder à des informations piégées. Cependant, elle nécessite une préparation cohérente, rigoureuse et structurée pour que les concurrents tombent dans le piège.

Dans cette recherche, nous nous basons sur la protection défensive, à savoir : comment protéger efficacement les informations sensibles de l'entreprise, au travers des outils et méthodes de gestion ?

Plusieurs outils et méthodes de protection ont été divulgués par les rares études scientifiques, la presse et d'autres sources. Nous pouvons illustrer quelques uns dans le tableau ci-dessous :

Tableau 7 : Outils et méthodes de protection techniques contre l'espionnage industriel

Auteur (année)	Outils et méthodes de protection techniques
Winkler (1996)	Un programme de sécurité complet incluant toutes les disciplines de sécurité est la seule contre-mesure efficace à une attaque coordonnée d'espionnage industriel. Un programme de sensibilisation détaillé et continu est la meilleure méthode pour dissuader de nombreuses attaques. Si tous les employés savent ce qu'il faut rechercher, les chances de réussite de l'attaque sont réduites au minimum. Il y a quatre parties d'un effort global de sécurité qui se renforcent mutuellement : sécurité technique, opérationnelle, physique et personnelle.
Shanley and Crabb (1998)	Les 12 étapes du programme de défense de Shanley et Crabb : 1. Retirez tous les ordinateurs, imprimantes et télécopieurs des zones de travail communes et des sites de R & D. 2. Aucun papier ne doit être laissé sur les bureaux et les tables, en particulier dans les laboratoires et les zones de vente. 3. Tous les terminaux doivent avoir des économiseurs d'écran protégés par mot de passe. 4. L'accès par niveaux doit être établi en utilisant des badges d'identification avec le code couleur et inspecter tous les gros colis quittant les locaux de l'entreprise. 5. Tous les fax et les messages Internet doivent être protégés. 6. Tous les anciens documents de R & D et autres documents sensibles doivent être déchiquetés. 7. Les contrats des employés doivent avoir des « accords de non-divulgation » hermétiques. Ils doivent être complets et mis à jour. 8. Les stagiaires et les chercheurs étudiants/diplômés doivent également signer les mêmes accords juridiques.

	9. Les employés doivent être formés pour reconnaître la différence entre les secrets commerciaux et les connaissances générales. 10. Les documents juridiques de non-divulgation doivent être signés avant que toute donnée confidentielle ne soit partagée dans les discussions relatives à la licence, à la co-entreprise ou à la recherche coopérative. 11. Les retraités de l'entreprise ne doivent pas avoir accès aux secrets d'entreprise. 12. Les systèmes de sécurité physique de l'usine doivent être en bon état et les agents de sécurité doivent être bien formés.
Massé et Thibaut (2001)	Ils distinguent quatre types de protection à envisager : Protection mécanique : contrôle des accès… Protection humaine interne et externe : infiltration, faux stagiaires… Protection juridique : confidentialité, propriété intellectuelle, brevets, clause de non concurrence… Protection logique : sécurité informatique.
Wanja Eric Naef (2003)	Voici quelques étapes simples pour aider à prévenir les fuites d'informations. Les entreprises doivent d'abord évaluer quelle information est sensible et la classer comme telle. Deuxièmement, une entreprise devrait mener une évaluation des risques afin de déterminer la vulnérabilité des transmissions d'informations non désirées et la probabilité que les rivaux cherchent à exploiter ces vulnérabilités. Troisièmement, une politique de sécurité répondant à ces préoccupations spécifiques devrait être développée. Enfin, cette politique de sécurité devrait être régulièrement évaluée et modifiée pour refléter les changements de concurrents et d'informations.
Coskun Samli et Jacobs (2003)	Les cinq étapes de l'approche de contrôle des dommages dans l'ordre de leur succession sont : les mesures de précaution,

	l'évaluation de la sensibilité, les plans d'urgence, la détection et le contrôle des catastrophes.
Enterprise Risk Management, Inc. (2008)	La sécurité de l'information est la pierre angulaire de la protection des ressources informationnelles d'une organisation et sa mise en œuvre correcte est essentielle. Les 8 étapes d'y parvenir sont : le soutien à la gestion ; les politiques et les procédures ; les tests de pénétration ; les évaluations sans fil ; les évaluations d'ingénierie sociale ; audits de sécurité ; audits de sécurité physique ; et la vérification des antécédents.
Menuet et Boloh (2012)	Connaitre en priorité ce qu'on veut protéger, appuie Jean-Patrick Guiraud. Pour le consultant, cette analyse préalable est capitale pour ne pas disperser ses moyens de protection. Qui sont les personnes ayant accès aux informations à protéger, où sont ces informations, sur un support ou est-ce de la matière grise? Une fois réalisée, cette démarche permet la mise en place d'une organisation adaptée. Et de l'avis des experts, le reste n'est que bon sens et affaire humaine. Badger les visiteurs, vérifier le profil des stagiaires, opter pour des broyeurs plutôt que des corbeilles à papier, ne pas travailler dans le train, autant d'acte de prudence visant à ne pas transformer des données stratégiques en informations dites blanches. « Se protéger relève du bon sens, or c'est presque trop facile, d'où ce manque de vigilance », commente Christelle Bodet. Un constat partagé par Jean-Patrick Guiraud. « Pour une bonne protection, il faut bien comprendre que les failles sont humaines ».

Plusieurs procédures, outils et méthodes internes sont définis pour fortifier la protection des informations sensibles, afin de dissuader les espions. Les protections techniques contre l'espionnage industriel sont nombreuses et diversifiées.

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*[30]*peut se définir comme toute action illégale dans laquelle un ordinateur est l'instrument ou l'objet du délit* ». Elle est définie dans le rapport du groupe de travail interministériel sur la lutte contre la cybercriminalité (2014) 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 : 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 : cette catégorie regroupe 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.

Le gouvernement français a défini, au travers de la gendarmerie nationale, des moyens de protection contre les cybermenaces, qui sont à la disposition des particuliers et des entreprises. Deux référents gendarmerie agissent au quotidien au profit des entreprises, il s'agit de :

- CYBERGEND qui est l'appellation fédérée d'un dispositif regroupant des enquêteurs cyber de la gendarmerie ;

[30] Guarnieri, F., & Przyswa, E. (2009). Cybercriminalité-contrefaçon: les interactions entre «réel et virtuel». *Revue internationale de droit économique*, vol. *23 n°*1, p.12.

- RS (référents sureté) de la gendarmerie qui sont déployés dans l'ensemble des départements, en métropole et en outre-mer.

Selon la gendarmerie nationale française, les cybermenaces se caractérisent par trois types de risques majeurs :

Tableau 8 : Les trois types de risques majeurs des cybermenances

Risque économique	Le vol de savoir-faire et de données commerciales ; des pertes d'exploitation suite à une prise en otage de votre système d'information ; l'interception de données confidentielles (contacts, mail, mots de passe) lus sur des supports mobiles (smartphone, tablette, etc.).
Risque d'image	L'image de la société peut être directement touchée par une campagne de dénigrement propagée sur le Net.
Risque juridique	la responsabilité civile et pénale de l'entreprise est engagée, si elle n'a pas protégé juridiquement ses données et si elle n'a pas mis en œuvre les moyens à l'état de l'art pour les protéger.

Elle sensibilise également les entreprises par des conseils pratiques à mettre en œuvre[31] :

- Sensibiliser vos collaborateurs : discrétion lors des déplacements, identification des informations sensibles et formation des collaborateurs à ne pas les diffuser sur les réseaux sociaux, etc.
- Fixer des règles pour l'utilisation du système d'information : adoption d'une charte informatique, introduction des clauses de confidentialité avec vos prestataires ou personnels temporaires (stagiaires), etc.

[31] Données disponibles sur le site de la gendarmerie nationale. Consulté le 21/06/2018. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/Nos-conseils2/Pour-les-professionnels/Cybermenaces-comment-proteger-votre-entreprise.

- La sécurité du système d'information : faire le bilan avec votre responsable informatique, effectuer des sauvegardes régulières de vos données, etc.

Il est important de signaler l'importance du rôle joué par le personnel de l'entreprise dans la réussite des différentes protections techniques. Le personnel demeure au cœur des stratégies de lutte contre l'espionnage industriel.

Etant incontournable, le personnel de l'entreprise doit être sollicité avant la définition et la mise en œuvre d'une quelconque stratégie de protection des informations. Cela pourrait accroitre les chances de l'entreprise de bénéficier d'une pleine implication de son personnel.

B. Limites et perspectives d'amélioration des protections techniques

Ces différents outils et méthodes de protection techniques semblent théoriquement adaptés et efficaces. Des auteurs (entre autres : Noailly, 1997 ; Coskun 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 remarquons que l'humain est au cœur de cette protection assurée par les entreprises elles-mêmes, quelques soient les outils et méthodes de protection cités ci-dessus. Pour assurer cette protection, le personnel d'une entreprise ressort comme la clé de la réussite.

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, si ils sont bien utilisés et si il y a une bonne conciliation protection et climat social de l'entreprise (Memheld, 2012).

Ils ne constituent pas une perfection en soi, mais aident les entreprises à bien cerner l'espionnage industriel et à atténuer ses effets néfastes.

3. Espionnage industriel et Contrôle de gestion ?

Nous relevons que les auteurs se sont attardés sur le Contrôle interne de l'espionnage industriel, au vu du nombre des outils et méthodes de protection techniques contre l'espionnage industriel. Ils semblent délaisser le Contrôle de gestion.

Or 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.

Ce manque d'écrits scientifiques sur l'espionnage industriel dans le domaine du Contrôle de gestion soulève plusieurs questions. Le contrôle de gestion ne permet-il pas d'appréhender l'espionnage industriel ? Les outils et méthodes du Contrôle de gestion ne sont-ils pas adaptés au contrôle de l'espionnage industriel ?

Cet état de l'art de l'espionnage industriel et de son contrôle organisationnel montre d'énormes progrès quant à la lutte contre l'espionnage industriel dans les entreprises, mais distingue aussi des lacunes, des vides qui nécessitent des études scientifiques apportant des réponses adéquates.

Tableau 9 : Les lacunes et vides scientifiques relevés sur l'espionnage industriel

Thème		Lacunes et vides scientifiques relevés
Concept d'espionnage industriel		Rareté des travaux scientifiques sur l'espionnage industriel, malgré ses conséquences désastreuses sur les économies et les entreprises.
Définition de l'espionnage industriel		Problème de délimitation entre l'espionnage industriel et certaines notions connexes comme l'intelligence économique.
Protections juridiques		Failles et vides juridiques ne permettant pas une protection exhaustive. Des instruments juridiques contournables et présentant des périmètres de protection.
Protections techniques par les entreprises	**Contrôle interne**	Des limites techniques de gestion, comme les dangers de l'artillerie sécuritaire, les coûts de la protection, la nécessité de concilier protection et climat social…
	Contrôle de gestion	Partie non encore étudiée par les chercheurs : absence totale d'études scientifiques. Or, le Contrôle de gestion englobe plusieurs étapes du Contrôle interne et s'élargit à d'autres étapes comme le pilotage des actions de prévention, le calcul des coûts de l'espionnage industriel, etc.

Conclusion du chapitre 1

L'objectif de ce chapitre était de présenter un état de l'art de l'espionnage industriel, en caractérisant le concept avec une délimitation claire des périmètres de distinction avec ses concepts connexes, et en soulignant la nécessité d'une introduction de l'appréhension de l'espionnage industriel dans la gestion de l'entreprise.

Pour ce faire, nous avons exposé plusieurs définitions de l'espionnage industriel, tout en mettant en exergue ses caractéristiques, mais aussi son évolution. Ainsi, nous avons pu montrer l'ambigüité sémantique résultant de l'analyse des différentes définitions de l'espionnage industriel.

Ensuite, nous avons évoqué ses caractéristiques et évolution, en détaillant les principaux éléments qui le caractérisent, en mettant en évidence certaines méthodes de collecte des informations, en citant quelques conséquences de l'espionnage industriel sur les économies et les entreprises, et en spécifiant les points d'évolution du concept.

Une appréhension du concept d'espionnage industriel a été effectuée à travers les concepts d'intelligence économique, de droit et d'éthique, pour davantage élucider les nombreuses confusions. Ainsi, nous avons présenté les multiples définitions du concept d'intelligence économique, qui demeure le concept le plus proche de l'espionnage industriel.

Puis, nous avons explicité l'information, qui est la matière première des concepts d'espionnage industriel et d'intelligence économique, tout en explicitant les différents types d'informations et les nuances de confusion entre les deux concepts. Par la suite, nous avons détaillé le recours au droit et à l'éthique, pour délimiter une frontière claire entre l'espionnage industriel et l'intelligence économique, et présenté les limites de distinction entre les deux concepts.

Enfin, nous avons étudié la question de la nécessité d'introduire le contrôle de l'espionnage industriel dans la gestion de l'entreprise, en effectuant un état des lieux des protections juridiques et des protections techniques, pour faire émerger les perspectives d'amélioration.

Il ressort de cette étude, une panoplie de protections juridiques présentant des insuffisances, qui ont conduit les entreprises à mettre en place des mesures de protection et de discipline internes contre l'espionnage industriel.

Ces protections techniques ont également montré des limites de gestion, qu'il conviendrait d'appréhender par des outils et méthodes de gestion adéquats. Par conséquent, nous estimons que la fonction contrôle de gestion est une alternative de gestion efficace.

Appréhender l'espionnage industriel par la fonction contrôle de gestion est une nouveauté, cela s'explique simplement par son absence dans la littérature scientifique. Partant d'une explicitation de l'espionnage industriel et d'un inventaire de ses outils et moyens de protection tant juridiques que techniques, nous avons relevé des insuffisances scientifiques.

Ces différents vides et lacunes scientifiques relevés, même si cela ne constitue pas une exhaustivité en soi, restent des arguments solides pour attirer l'attention des chercheurs de tous les domaines scientifiques pouvant être mobilisés. L'ampleur et la rapide propagation de l'espionnage industriel dans les économies et les entreprises, surtout à l'essor des nouvelles technologies invitent le chercheur à œuvrer des solutions au service des entreprises.

De ce fait, nous nous proposons d'élaborer un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, afin de combler les insuffisances relevées dans cet état de l'art. Le chapitre suivant consiste en une explicitation des théories et concepts mobilisés pour construire le modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Chapitre 2 : Cadre conceptuel

La rareté des écrits et publications scientifiques sur l'espionnage industriel nous conduit à la mobilisation de plusieurs concepts, approches et théories pour mieux cadrer conceptuellement et théoriquement le processus de contrôle de l'espionnage industriel.

Cette manière de mobiliser permet de s'adosser sur des concepts connexes ayant certaines caractéristiques communes. Par ailleurs, elle consolide également la méthode de recherche qui se base sur des éléments conceptualisés avec des cadres théoriques.

Après un état de l'art du concept dans le premier chapitre, nous voulons expliciter dans ce deuxième chapitre les concepts, théories et approches qui s'apparentent à notre objet de recherche et constituent un cadre de référence.

L'objectif de cette recherche est d'appréhender le processus de contrôle de l'espionnage industriel dans les organisations en France, particulièrement par la fonction contrôle de gestion.

Cependant, nous avons commencé par la solution de l'exploration des pratiques dans les organisations en France, car il se pourrait que les organisations aient déjà mis en œuvre un processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.
La fonction contrôle de gestion s'adapte en permanence aux mutations de l'environnement, donc l'éventuelle existence d'un processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion dans les organisations semble très probable et nécessite une étude scientifique pour une nouvelle découverte.

Par ailleurs, les concepts et théories, que nous expliciterons, constituent le soubassement commun pour la simple raison suivante : les concepts et théories sur lesquels nous nous sommes adossés pour explorer, sont les mêmes que nous avons utilisés pour la construction du modèle.

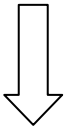
Ainsi, nous allons aborder dans une première section la mobilisation des concepts de référence (comptabilité environnementale, coûts cachés et contrôle de gestion environnemental) pour justifier le cadre de la recherche.

Ensuite, nous explicitons dans une deuxième section la détermination d'un cadre théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Enfin,

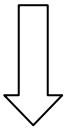
nous allons décortiquer les six dimensions d'analyse de Chiapello revisitées et présenter le modèle théorique.

L'architecture du chapitre est la suivante :

Section 1 **Comptabilité environnementale, coûts cachés et contrôle de gestion environnemental**	
En quoi le contrôle de gestion environnemental, la comptabilité environnementale et les coûts et performances cachés constituent notre cadre de référence ?	Les concepts mobilisés pour appréhender le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion



Section 2 **Cadre théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion**	
Cadre théorique du contrôle de gestion environnemental	Détermination d'un cadre théorique pour appréhender le processus de contrôle de l'espionnage industriel



Section 3 **Les six dimensions d'analyse de Chiapello revisitées et le modèle théorique**			
Les six dimensions d'un mode de contrôle	Une analyse des typologies des modes de contrôle de Chiapello	Les six dimensions de Chiapello réadaptées à l'analyse des outils des systèmes de contrôle	Le modèle théorique

Section 1 : Comptabilité environnementale, coûts cachés et contrôle de gestion environnemental

Afin de clarifier notre démarche d'élaboration d'un cadre théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion, nous avons jugé nécessaire de nous adosser sur des concepts ayant certaines caractéristiques communes avec notre objet de recherche.

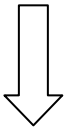
En effet, cette façon d'aborder le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion est novatrice. Par conséquent, une démarche adossée sur des concepts ayant les mêmes caractéristiques semble sûre et probante pour étudier le contour de la question.

D'autant plus que les différents concepts mobilisés ont déjà fait l'objet de plusieurs études scientifiques et possèdent des cadres théoriques. Cela va renforcer scientifiquement notre objet de recherche.

Ainsi, nous allons aborder dans cette section en quoi le contrôle de gestion environnemental, la comptabilité environnementale et les coûts et performances cachés constituent notre cadre de référence (1), pour ensuite détailler les concepts mobilisés permettant d'appréhender le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion (2).

L'architecture de la section est la suivante :

En quoi le contrôle de gestion environnemental, la comptabilité environnementale et les coûts et performances cachés constituent notre cadre de référence ?		
Définitions des éléments du cadre de référence	Cadre de référence	Soubassement commun



Les concepts mobilisés pour appréhender le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion	
Des concepts entrant dans le cadre du développement durable	La justification d'une extension des outils classiques du contrôle de gestion pour appréhender le processus de contrôle de l'espionnage industriel

1. En quoi le contrôle de gestion environnemental, la comptabilité environnementale et les coûts et performances cachés constituent notre cadre de référence ?

Les concepts, que nous avons mobilisés pour appréhender le processus de contrôle de l'espionnage industriel, sont :

- le contrôle de gestion environnemental ;
- la comptabilité environnementale ;
- les coûts et performances cachés.

Ces trois concepts constituent des références du processus de contrôle de l'espionnage industriel et peuvent être regroupés dans le contrôle de gestion environnemental, qui demeurera la base commune.

A. Définitions des éléments du cadre de référence

Henri et Journeault (2010) ont donné le nom d'« éco-contrôle » au contrôle de gestion environnemental. L'éco-contrôle est *« un système de pilotage qui comporte un volet sociétal important, aujourd'hui exacerbé (Pasquero, 2005 ; Capron et Quairel-Lanoizelée, 2004; Igalens, 2004), qui vise à responsabiliser les entreprises à l'égard des impacts environnementaux et de développement durable de leurs activités*[32] *»*.

Cette définition renvoie à une prise de conscience de l'organisation des impacts environnementaux, sans pour autant prétendre à tirer d'autres bénéfices de cette responsabilisation.

Par ailleurs, Renaud (2014) définit le contrôle de gestion environnemental comme : « *un processus par lequel les managers influencent d'autres membres de l'organisation pour mettre en œuvre ou faire émerger les stratégies vertes de l'organisation* ».

Nous retrouvons ici une définition centrée sur la capacité d'influence des managers à la restauration et à l'opérationnalisation des stratégies inhérentes aux aspects environnementaux.

[32] Caron, M. A., Boisvert, H., & Mersereau, A. (2007, May). La comptabilité de management environnementale ou l'écocontrôle : utilité des outils de contrôle de gestion. In *«comptabilité et environnement»*.

Antheaume (2013), dans son état des lieux et état de l'art du contrôle de gestion environnemental, propose la définition suivante[33] :

« *le contrôle de gestion environnemental est un ensemble d'outils qui permettent de collecter des données sur l'état de raréfaction des ressources naturelles liées à l'activité d'une organisation et d'effectuer une allocation de ressources interne, qui pose comme contrainte prioritaire le maintien des capacités de régénération des écosystèmes, et incite les employés à respecter cette contrainte. Les données collectées doivent ainsi permettre l'information des tiers sur la manière dont l'entreprise contribue à maintenir intactes les capacités des écosystèmes* ».

Pour proposer cette définition, l'auteur commence par s'intéresser aux définitions de la comptabilité environnementale, notamment celles de Gray, Owen et Maunders (1987) ; Christophe (1989, 1992) ; Gray, Owen et Adams (1996) ; Gray (1992, 2000, 2002, 2010) ; Antheaume et Christophe (2005) ; Richard (2012).

Antheaume considère que le contrôle de gestion environnemental est une continuité sur les travaux de la comptabilité environnementale, de ce fait proposer une définition revient à clarifier le concept de la comptabilité environnementale.

Gray, Owen et Maunders (1987) définissent la comptabilité sociale et environnementale comme : *« un processus de communication sur les effets sociaux et environnementaux des actions économiques d'une organisation, à destination de certains groupes d'intérêt dans la société et de la société en général ».*

Par ailleurs, Christophe (1989, 1992) définit la comptabilité environnementale comme : *« un système d'information efficient sur le degré de raréfaction des éléments naturels lié à l'activité de l'entreprise, utilisable pour agir sur cette raréfaction et pour informer les tiers »*[34].

Antheaume et Christophe (2005) trouvent que le terme de comptabilité environnementale renvoie aux outils qui permettent : *d'une part de compléter ce que « compte » la comptabilité générale par la prise en « compte » des flux physiques et des coûts que l'entreprise*

[33] Antheaume, N. (2013). Le contrôle de gestion environnemental. État des lieux, état de l'art. *Comptabilité-Contrôle-Audit*, *19* (3), 9-34.
[34] *Ibid.*

occasionne à d'autres du fait de ses actions ; d'autre part d'étendre les catégories d'acteurs à qui l'entreprise rend des « comptes ».

Quant aux coûts et performances cachés, les pionniers tels que Savall et Zardet (2010) définissent les coûts et performances cachés, appelés aussi les coûts cachés par commodité, comme *: « des coûts qui ne figurent pas dans les systèmes d'information d'une organisation ou entreprise (comme le compte de résultat, le budget, la comptabilité générale, la comptabilité analytique, les tableaux de bord...) ».*

Les coûts cachés sont évalués par une méthode d'évaluation des coûts et performances cachés. C'est une méthode d'évaluation qui fait partie, par extension, du domaine de la comptabilité et réside dans le champ de la gestion.

Par conséquent, ce caractère « d'extension » et sa capacité à détecter et à évaluer les coûts invisibles font du concept, un élément susceptible d'entrer dans le cadre de la comptabilité environnementale. D'ailleurs, la méthode est utilisée dans la détermination de certains coûts environnementaux.

En analysant les différentes définitions ci-dessus, nous remarquons des liens entre les différents concepts, notamment entre la définition de la comptabilité environnementale de Bernard Christophe (1989, 1992) et celle du contrôle de gestion environnemental d'Antheaume (2013).

Certains outils de la comptabilité étant des outils utilisés dans le contrôle de gestion classique, l'existence d'un lien entre les deux notions en « version environnementale ou durable » prouve que le contrôle de gestion environnemental résulte d'une continuité des travaux de la comptabilité environnementale, comme le mentionne Antheaume (2013). D'autant plus que les travaux sur la comptabilité environnementale précèdent ceux sur le contrôle de gestion environnemental.

Pour Schaltegger et Burritt (2010), uniquement une partie de la comptabilité[35] touche les côtés liés à l'environnement. Dans ce domaine, Schaltegger et Burritt distinguent particulièrement la comptabilité environnementale de gestion (*Environmental Management Accounting*), qu'ils définissent comme : « *un système destiné à générer, analyser et utiliser des informations*

[35] Ils définissent la comptabilité comme un système de collecte et de mise en forme de données monétaires et physiques.

financières et non financières, de manière à optimiser la performance écologique et économique d'une entreprise, pour assurer sa pérennité. La comptabilité environnementale de gestion se définit à partir de ses utilisateurs principaux et de sa raison d'être prioritaire, qui est de fournir une information pertinente et utile aux managers d'une organisation, distinctement des parties prenantes externes ».

Sachant que la comptabilité de gestion fait partie des outils classiques du contrôle de gestion, la logique voudrait que la comptabilité de gestion environnementale soit un outil du contrôle de gestion environnemental.

B. Cadre de référence

Le contrôle de gestion environnemental, la comptabilité environnementale et les coûts cachés constituent notre cadre de référence, car les trois concepts ont en commun d'être des extensions respectivement du contrôle de gestion, de la comptabilité et « des coûts visibles ».

Les coûts visibles font référence aux données visibles, c'est-à-dire les données issues des systèmes d'information de l'organisation. Comme l'indique le nom, les coûts et performances cachés sont des coûts non visibles. La théorie socio-économique considère qu'un coût peut être qualifié de visible, lorsqu'il comporte trois caractéristiques simultanées à savoir :

- une dénomination usuelle ;
- une mesure ;
- un système de surveillance.

Les coûts et performances cachés, ne possédant pas ces caractéristiques, restent invisibles et ne figurent pas dans les systèmes d'information de l'organisation[36].

Le contrôle de gestion environnemental et la comptabilité environnementale ont la spécificité d'intégrer des aspects environnementaux dans leurs disciplines de base respectives. Quant à la notion des coûts cachés, il s'agit d'appréhender certaines données « invisibles » qui engendrent des coûts imperceptibles et réduisent significativement les performances de l'organisation.

[36] Savall H., Zardet V. (2010). Maîtriser les Coûts et les Performances Cachés. *5ème édition*, Economica.

Au-delà de ce caractère d'extension commun aux trois éléments, ils ont tous pour finalité de rendre meilleure la gestion de l'organisation, en montrant les impacts de certains phénomènes sur celle-ci.

Le contrôle de gestion environnemental et la comptabilité environnementale tiennent compte des effets environnementaux sur la gestion de l'organisation et tirent ainsi profit de cette considération, en améliorant son image, en réduisant sa pollution, en aidant à la prise de décisions…

Selon les différentes expérimentations de l'institut socio-économique des entreprises et des organisations (ISEOR), qui est d'ailleurs le seul institut à avoir abordé de manière approfondie le concept des coûts et performances cachés, une maitrise de ces coûts permettrait aux organisations et aux entreprises non seulement d'accroitre leur performance économique mais aussi d'améliorer leur performance sociale.

Ces deux points relevés (l'extension et l'aboutissement à une meilleure gestion) constituent le soubassement commun à notre objet d'étude, puisque le processus de contrôle de l'espionnage industriel, au travers de la fonction contrôle de gestion, vise à agir sur la gestion de l'organisation en améliorant les performances de celle-ci.

Les outils classiques du contrôle de gestion ne permettant pas d'appréhender l'espionnage industriel, une extension des périmètres de ces outils et une prise en compte de nouveaux outils permettront de cerner le phénomène dans son ensemble[37].

C. Soubassement commun

Pour appréhender le processus de contrôle de l'espionnage industriel (notamment par la fonction contrôle de gestion) dans l'organisation, il sera question d'introduire le contrôle de l'espionnage industriel dans la fonction contrôle de gestion. Pour ce faire, une extension des outils du contrôle de gestion traditionnel est nécessaire, dans le sens où ces outils classiques ne permettent pas d'appréhender l'espionnage industriel.

Le contrôle de gestion environnemental, la comptabilité environnementale et les coûts cachés sont tous des outils de gestion, même si certains peuvent englober d'autres (le contrôle de

[37] Cette affirmation sera justifiée dans le soubassement commun.

gestion environnemental peut contenir des outils de la comptabilité environnementale et des coûts cachés).

Appartenant tous à la discipline de gestion, ces trois outils ont la particularité d'être des élargissements d'autres outils (notamment de leurs outils de base), afin d'assurer la gestion de certains phénomènes échappant à la capacité d'appréhension des outils classiques. Restant toujours dans la même discipline, ceci s'apparente à l'objet de notre recherche et constitue des notions connexes du processus de contrôle de l'espionnage industriel.

L'espionnage industriel, dû à sa nature occulte, fait partie des phénomènes non compris dans les systèmes d'information de l'organisation. Or le contrôle de gestion se nourrit principalement des éléments de ces systèmes d'information de l'organisation.

Par conséquent, les outils classiques du contrôle de gestion ne peuvent cerner l'ensemble des phénomènes extérieurs aux systèmes d'information, car ils n'y sont pas tout simplement préparés.

Cependant, un réajustement de ces outils classiques et le recours à d'autres outils (comme le cas des trois outils de gestion relevés ci-haut) pourraient permettre de cerner l'espionnage industriel.

2. Les concepts mobilisés pour appréhender le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion

La recherche sur l'appréhension de l'espionnage industriel par la fonction contrôle de gestion dans une organisation est une première et constitue une innovation dans la discipline de la gestion.

Les concepts mobilisés ont beaucoup de liens, certain étant même à l'origine d'autre concept. C'est le cas du contrôle de gestion environnemental, qui est la continuité des travaux sur la comptabilité environnementale et sociétale (Antheaume 2013). Dans ce sens, évoquer le contrôle de gestion environnemental serait le point focal, même si la mention de certaines notions de la comptabilité environnementale reste nécessaire à la bonne compréhension de notre processus.

Nous explicitons dans cette partie la question de : comment nous nous inspirerons des spécificités des différents concepts et théories mobilisés pour aboutir au processus de contrôle de l'espionnage industriel ?

A. Des concepts entrant dans le cadre du développement durable

Le contrôle de gestion environnemental et la comptabilité environnementale se situent indéniablement dans le cadre d'une stratégie de développement durable, si l'on se réfère à la définition classique du rapport Brundtland de la Commission mondiale sur l'environnement et le développement de l'Organisation des Nations Unies (définition donnée dans l'introduction générale).

Le concept des coûts et performances cachés peut se situer également dans ce même cadre. Les coûts cachés se définissent comme des coûts qui ne figurent pas dans les systèmes d'information d'une organisation et sont des coûts dilués dans le coût des produits/services ou des coûts d'opportunité, qui par nature ne sont pas enregistrés.

Or, comme indiqué ci-haut, une maitrise de ces coûts permettrait aux organisations et aux entreprises non seulement d'accroitre leur performance économique, mais aussi d'améliorer leur performance sociale. Sachant que ces coûts cachés peuvent aussi bien concerner les coûts liés aux aspects économiques et sociaux que les aspects environnementaux, cela impute le concept dans le cadre du développement durable selon sa définition ci-dessus.

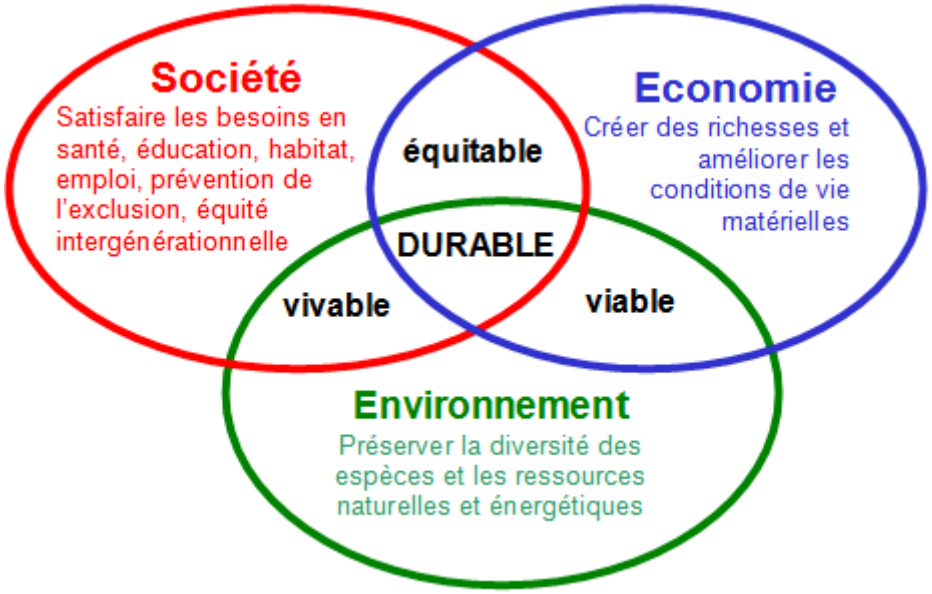
Une question culminante est de savoir, si le contrôle de gestion environnemental permet d'appréhender le processus de contrôle de l'espionnage industriel ?

Pour répondre à cette question, nous allons analyser les trois piliers du développement durable à savoir :

- pilier social ;
- pilier économique ;
- pilier environnemental.

Selon le diagramme du développement durable, une considération des trois piliers constitue une approche globale du développement durable. Cependant, une considération du pilier social et du pilier économique entre dans le cadre d'une approche « équitable » ; une considération du pilier social et du pilier environnemental réside dans le cadre d'une approche « vivable » ; et une considération du pilier environnemental et du pilier économique entre dans le cadre d'une approche « viable ».

Figure b : Diagramme du développement durable, une explication schématique issue du sommet de la terre de Rio 1992



Le contrôle de gestion traditionnel ou classique demeure dans une approche « équitable », car ses outils classiques sont élaborés pour impacter principalement les piliers économique et social.

Par ailleurs, le contrôle de gestion environnemental a la spécificité d'introduire le pilier environnemental, en réadaptant les outils classiques pour appréhender les aspects environnementaux et en ajoutant de nouveaux outils permettant de cerner ledit pilier.

L'apport du contrôle de gestion environnemental est donc l'introduction du pilier environnemental, puisque les deux autres piliers étaient déjà cernés par le contrôle de gestion traditionnel ou classique.

Le contrôle de gestion classique n'appréhende pas tous les processus, Schaltegger (2011) distingue ainsi :

- des processus de marché ;
- des processus hors marché.

L'auteur précise que les processus de marché agissent dans le cadre des relations contractuelles et marchandes, que l'organisation entretient avec certaines parties prenantes (salariés, fournisseurs, clients…) ; tandis que les processus hors marché agissent hors relations contractuelles et marchandes, à travers des éléments comme : l'exposition de

l'entreprise à une couverture médiatique, des sollicitations de divers groupes d'intérêt, le processus législatif…

Selon Antheaume (2013), le contrôle de gestion classique se concentre sur les phénomènes et les processus de marché, et l'auteur ajoute que la spécificité du contrôle de gestion environnemental serait de s'intéresser aux phénomènes et aux processus hors marché.

L'espionnage industriel, qui est un phénomène hors relations contractuelles et marchandes, réside de ce fait dans les phénomènes et processus hors marché, si l'on se réfère à la définition de Schaltegger (2011).

Dans cette optique, la tentation de dire que le processus de contrôle de l'espionnage industriel pourrait être appréhendé par le contrôle de gestion environnemental semble évidente.

Certes, ce raisonnement semble logique, mais pour mieux les différencier et montrer l'incapacité du contrôle de gestion environnemental de cerner le processus de contrôle de l'espionnage industriel, nous allons revenir sur la particularité du contrôle de gestion classique et du contrôle de gestion environnemental, tout en évoquant les trois piliers du développement durable.

Nous montrerons par la suite l'utilité d'une extension des outils classiques du contrôle de gestion, tout en se référant à l'exemple du contrôle de gestion environnemental, pour cerner le processus de contrôle de l'espionnage industriel dans une organisation.

B. La justification d'une extension des outils classiques du contrôle de gestion pour appréhender le processus de contrôle de l'espionnage industriel

L'incapacité du contrôle de gestion environnemental d'appréhender l'espionnage industriel se justifie par l'explicitation du tableau ci-dessous :

Tableau 10 : Les impacts des outils du contrôle de gestion classique et du contrôle de gestion environnemental sur les trois piliers du développement durable

	Impacts des outils classiques du contrôle de gestion	Impacts des outils du contrôle de gestion environnemental
Pilier économique	Oui	Oui
Pilier social	Oui	Oui
Pilier environnemental	Non	Oui

L'espionnage industriel demeure parmi les phénomènes et processus hors marché au même titre que les aspects environnementaux, mais il n'est pas considéré comme un indicateur environnemental. Un indicateur environnemental[38] désigne, dans le dictionnaire environnement 2017, une variable quantitative ou qualitative qui peut être mesurée ou décrite. C'est une représentation simplifiée d'une réalité complexe, qui répond à trois grandes fonctions :

- scientifique : évaluer l'état de l'environnement ;
- politique : identifier les priorités et évaluer les performances de l'action publique ;
- sociétale : faciliter la communication, inciter l'action dans le bon sens.

Les indicateurs environnementaux servent de variables, lorsqu'on étudie par modélisation les changements survenant dans les systèmes environnementaux complexes. L'OCDE (Organisation de Coopération et de Développement Economiques) définit un indicateur

[38] Définition et fonctions issues du dictionnaire environnement 2017, lien ci-dessous : http://www.dictionnaire-environnement.com/indicateur_environnemental_ID767.html

environnemental comme : « *paramètre ou valeur calculée à partir de paramètres donnant des indications sur l'état d'un phénomène, de l'environnement ou d'une zone géographique et d'une portée supérieure aux informations directement liées à la valeur du paramètre* ».

Sachant que les outils classiques du contrôle de gestion ne permettent pas de cerner le processus de contrôle de l'espionnage industriel, pour la simple raison que le contrôle de gestion classique n'appréhende que les phénomènes et processus de marché (Schaltegger, 2011 et Antheaume, 2013).

Les outils du contrôle de gestion environnemental, qui sont à l'origine de l'appréhension des aspects environnementaux, résultent d'une extension des outils classiques du contrôle de gestion (Berland, 2014).

Par ailleurs, cette extension est uniquement une prise en compte des aspects environnementaux et non de tous les phénomènes et processus hors marché. De ce fait, l'espionnage industriel ne peut être appréhendé par le contrôle de gestion environnemental, puisqu'il n'est pas un indicateur environnemental.

Cependant, s'inspirer du contrôle de gestion environnemental (notamment de sa méthode d'extension des outils classiques du contrôle de gestion) serait un bon cadre de référence pour appréhender le processus de contrôle de l'espionnage industriel.

Dans la section suivante, nous allons définir un cadre théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion, en nous adossant sur celui du contrôle de gestion environnemental.

Section 2 : Cadre théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion

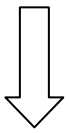
Déterminer un cadre théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion est une première et reste une tâche délicate à cause de l'inexistence de la littérature sur la thématique.

C'est une innovation dans la discipline du contrôle de gestion et en général dans le champ de la gestion. Pour ce faire, nous nous inspirerons du cadre théorique d'un processus connexe pour définir un cadre théorique, permettant de comprendre notre objet de recherche.

Ainsi, nous partirons du cadre théorique du contrôle de gestion environnemental pour définir un cadre théorique permettant d'appréhender le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

L'architecture de la section est la suivante :

Cadre théorique du contrôle de gestion environnemental	
Les quatre leviers de contrôle de Simons	Le contrôle de gestion environnemental : cadre théorique via les leviers de contrôle diagnostic et interactif



Détermination d'un cadre théorique pour appréhender le processus de contrôle de l'espionnage industriel	
Les systèmes de contrôle de Simons et la gestion de l'espionnage industriel	La grille d'analyse des systèmes de contrôle diagnostic et interactif proposée par Renaud

1. Cadre théorique du contrôle de gestion environnemental

Le contrôle de gestion environnemental est un concept, qui prend de plus en plus d'ampleur dans les organisations. Un cadre de référence théorique incontesté du contrôle de gestion demeure celui des leviers de contrôle de Simons.

L'auteur définit le contrôle de gestion moderne comme des : « *processus et procédures formels fondés sur l'information que les managers utilisent pour maintenir ou modifier certaines configurations des activités de l'organisation* » (Simons, 1991), pour ensuite présenter plus tard (1994) quatre leviers de contrôle permettant de concilier le système de contrôle et la stratégie.

Après une présentation des leviers de contrôle de Simons, nous allons voir comment s'articule le contrôle de gestion environnemental au travers de cette grille de lecture ?

A. Les quatre leviers de contrôle de Simons

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)[39].

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.

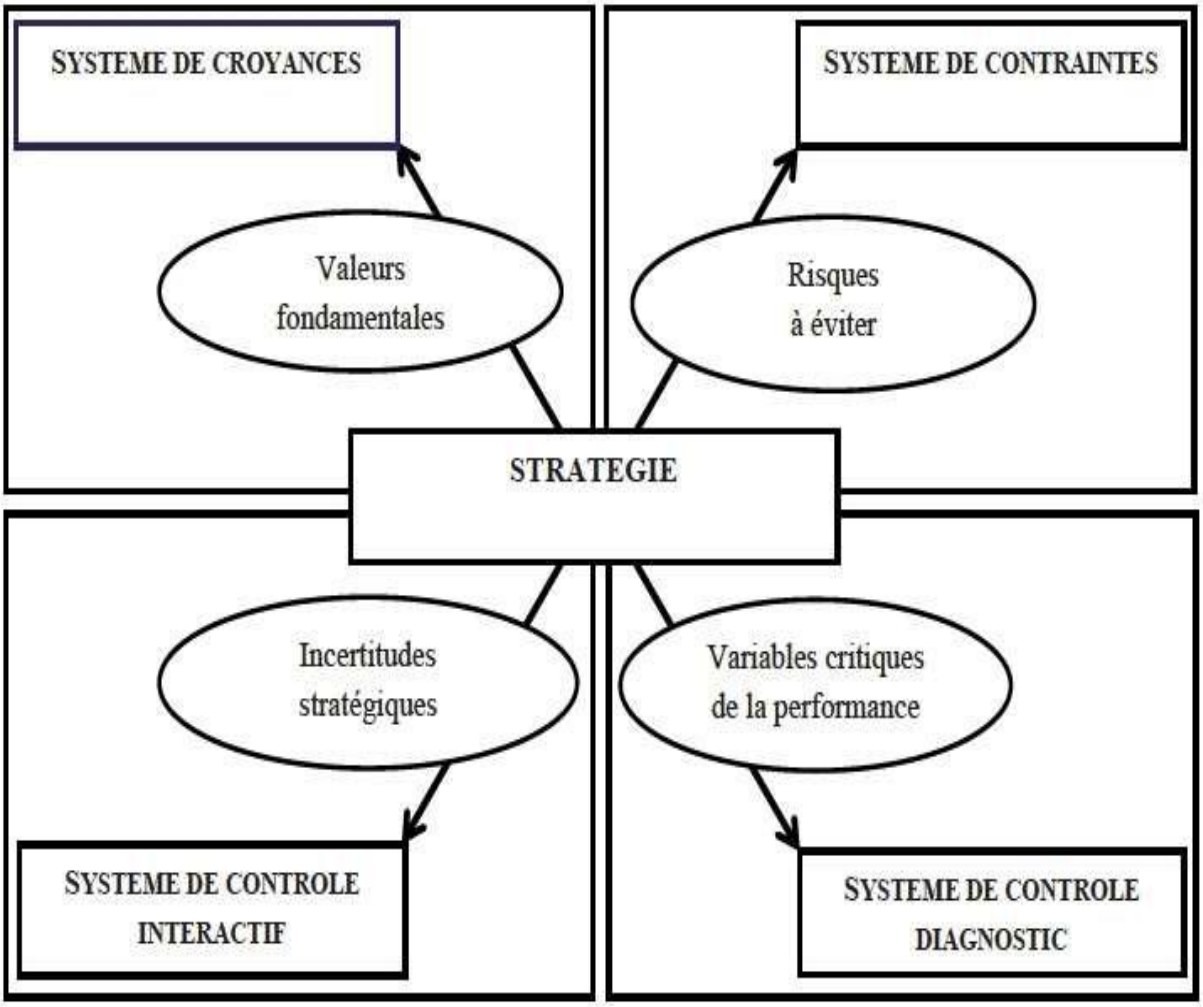
Les variables clés (valeurs fondamentales, risques à éviter, variables critiques de la performance, et incertitudes stratégiques) correspondent respectivement aux systèmes de contrôle ou leviers de contrôle suivants : systèmes de croyances, systèmes de contraintes, systèmes de contrôle diagnostic, et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

[39] Simons, R. (1994). *Levers of control : How managers use innovative control systems to drive strategic renewal*. Harvard Business Press.

Simons ajoute que les organisations peuvent articuler plusieurs systèmes de contrôle à la fois et précise que les meilleures d'entre elles sont celles qui agencent ces leviers de contrôle pour compenser les effets pervers des uns et des autres (Simons, 1999)[40].

La figure ci-dessous illustre les liaisons entre les variables clés et les leviers de contrôle de Simons :

Figure c : Les 4 leviers de contrôle avec les 4 variables clés de Simons[41]



Selon Lepori et Bollecker (2015)[42], les systèmes de contrôle de Simons se caractérisent par :

[40] Nobre, T., & Zawadski, C. (2015, May). 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*.
[41] Figure issue de l'article suivant : Dorbaire, P., Chen, G., & Chen, M. (2012). Le contrôle stratégique des Instituts Confucius. *Management & Avenir*, (5), 272-290.
[42] Lepori, E., & Bollecker, M. (2015, May). Les leviers de contrôle de SIMONS: vers une compréhension des freins à l'équilibrage diagnostic/interactif. In *Comptabilité, Contrôle et Audit des invisibles, de l'informel et de l'imprévisible*.

- 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 (Gibert, 2002).* 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 (Gibert, 2002).

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).

Parmi ces quatre leviers de contrôle de Simons sur le contrôle organisationnel, le contrôle de gestion se trouve principalement dans le cadre du système de contrôle diagnostic et du système de contrôle interactif (Henri, 2006 ; Widener, 2007 ; Essid et Berland, 2011 ; Renaud, 2015 ; Lepori et Bollecker, 2015).

B. Le Contrôle de gestion environnemental : cadre théorique via les leviers de contrôle diagnostic et interactif

Le contrôle de gestion environnemental est un type de contrôle, qui entre dans le cadre du développement durable au travers d'une appréhension des aspects environnementaux ou écologiques.

Par ailleurs, l'insertion de la dimension environnementale ne sous-entend pas seulement une simple prise de conscience des aspects environnementaux sans chercher à engendrer de la valeur ajoutée. C'est aussi un moyen pour les organisations de transformer cette valeur sociale en valeur économique (Acquier, 2008).

Cependant, selon Acquier (2008) cette transformation dans le cadre du développement durable s'opère sur deux catégories de figures initialement proposées par Aggeri et al. (2005), il s'agit :

- d'une part des figures imposées ;
- d'autre part des figures libres.

Arjaliès, Goubet et Ponssard (2011), au travers d'une typologie de stratégies élaborée par Arjaliès et Ponssard (2010), proposent deux types de stratégies dont les conditions de passage d'un type à l'autre y sont différenciées. Une première qualifiée « de conformité » c'est-à-dire des figures imposées et une seconde « d'opportunité » visant les figures libres.

Ces qualifications s'éclaircissent à travers les définitions des deux figures données par Acquier :

- d'une part les figures imposées *désignent un ensemble de pratiques qui se déploient dans des champs d'action déjà cadrés, du point de vue social (elles apparaissent nécessaires et légitimes) et technique (elles sont contrôlables et réalisables). 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 ;*
- d'autre part, *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. Pour l'entreprise, les figures libres constituent un espace potentiel de différenciation et d'exploration, faisant écho à des enjeux sociétaux émergents qui restent à qualifier, et sur lesquels les connaissances et modes d'action restent lacunaires[43].

Il est pertinent de s'intéresser aux définitions des deux cas de figures d'Acquier, parce qu'elles ne se limitent pas uniquement dans un cadre de développement durable, mais visent à étudier de manière plus globale l'interface entre entreprise et société. Cette ouverture permet d'appréhender d'autres phénomènes dans le même cadre théorique.

Selon Antheaume (2013), 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*[44].

Si l'on se réfère aux définitions des deux figures d'Acquier (2008), le contrôle de gestion environnemental semble se caractériser par :

- des variables d'incertitudes stratégiques (compte tenu des réglementations environnementales changeantes en permanence, des incertitudes de marché, d'énormes risques liés à cette fluctuation, etc.) ;
- des variables critiques de la performance (visant la conformité des actions et des résultats vis-à-vis d'un référentiel environnemental, des normes environnementales…).

Cependant, le contrôle de gestion environnemental, s'expliquant par les concepts de figures libres et de figures imposées, peut être confronté aux systèmes de contrôle de Simons, afin d'appréhender son cadre d'appartenance.

De ce fait, il se trouve dans la catégorie de « formulation et de mise en œuvre d'une stratégie ». Par conséquent, les deux leviers de contrôle dans la catégorie d'encadrement d'une stratégie (systèmes de croyances et aux systèmes de contraintes) se voient exclus du

[43] Acquier, A. (2008, May). Développement durable et management stratégique: piloter un processus de transformation de la valeur. In *Actes de la 17e Conférence Internationale de l'AIMS*.
[44] Antheaume, N. (2013). Le contrôle de gestion environnemental. État des lieux, état de l'art. *Comptabilité-Contrôle-Audit*, *19* (3), 9-34.

choix des systèmes de contrôle permettant d'appréhender le contrôle de gestion environnemental.

Ainsi, les deux leviers susceptibles de cerner le contrôle de gestion environnemental sont le système de contrôle diagnostic et le système de contrôle interactif (demeurant les deux leviers de contrôle pour la formulation et la mise en œuvre d'une stratégie), puisqu'en référence *à l'état des lieux et état de l'art du contrôle de gestion environnemental* d'Antheaume (2013), la gestion des figures imposées renvoie au système de contrôle diagnostic et celle des figures libres au système de contrôle interactif.

A ce stade, les auteurs se divisent en deux groupes : ceux qui conçoivent le contrôle de gestion environnemental au filtre des leviers de contrôle diagnostic et interactif « avec articulation simultanée » (Renaud, 2015 ; etc.) ; et ceux qui penchent pour une appréhension du contrôle de gestion environnemental au travers des leviers de contrôle diagnostic et interactif « avec une articulation en glissement » (Tuomela, 2005 ; Essid et Berland, 2011 ; etc.), c'est-à-dire du passage d'un système de contrôle interactif à un système de contrôle diagnostic ou l'inverse.

Ces deux catégories d'auteurs ont tous le mérite de la logique, dans le sens où le contrôle de gestion environnemental se caractérise par la gestion des figures imposées et des figures libres.

A présent, nous allons nous inspirer de cette architecture théorique du contrôle de gestion environnemental pour définir un cadre théorique cernant le processus de contrôle de l'espionnage industriel à travers la fonction contrôle de gestion.

2. Détermination d'un cadre théorique pour appréhender le processus de contrôle de l'espionnage industriel

La question qui se pose à présent est de savoir : quel(s) levier(s) de contrôle de Simons s'articule(nt) avec le processus de contrôle de l'espionnage industriel dans l'organisation ?

A. Les systèmes de contrôle de Simons et la gestion de l'espionnage industriel

L'espionnage industriel faisant partie des phénomènes et processus hors marché, son processus de contrôle peut être confronté aux leviers de contrôle de Simons, si l'on considère la proposition suivante de Schaltegger (2011) : lorsqu'il évoque *la capacité que doit développer le contrôle de gestion environnemental de comprendre comment des éléments et des processus hors marché peuvent se traduire par de la valeur économique pour l'entreprise*[45] ; et que l'auteur préconise, par la suite, la compatibilité entre le contrôle de gestion environnemental et les systèmes de contrôle définis par Simons. Donc, c'est partant de la question « de comprendre comment des éléments et des processus hors marché peuvent se traduire par de la valeur économique pour l'entreprise », que l'auteur a évoqué la compatibilité du contrôle de gestion environnemental avec les leviers de contrôle de Simons.

Le processus de contrôle de l'espionnage industriel entre dans le même cadre, puisqu'il s'agit de mettre en place un ou (des) système(s) de contrôle de gestion dans le cadre d'une stratégie, où l'appréhension de l'espionnage industriel (qui est un phénomène et processus hors marché) se traduirait par de la valeur économique pour l'organisation.

Comme mentionné ci-haut, le cadre définitionnel des figures imposées et des figures libres d'Acquier (2008) ne se statuait pas uniquement dans la limite du développement durable.

Dans cette optique, nous pouvons statuer le processus de contrôle de l'espionnage industriel, en termes de figures imposées et ou de figures libres, avant de le confronter aux leviers de contrôle de Simons. Il s'agit de savoir : **si le processus de contrôle de l'espionnage industriel consisterait à l'appréhension des figures imposées ou des figures libres ? Ou des deux figures à la fois ?**

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

[45] Antheaume, N. (2013). Le contrôle de gestion environnemental. État des lieux, état de l'art. *Comptabilité-Contrôle-Audit*, *19* (3), 9-34.

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.

Ces différents éléments constituent effectivement des figures imposées, si l'on se réfère à la définition d'Acquier (2008) sur le concept. 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 démontré l'incapacité de ces protections et normes juridiques, quant à l'appréhension exhaustive de l'espionnage industriel (dans l'état de l'art 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).

Partant du côté novateur de cette méthode (une première dans la discipline du contrôle de gestion et en général dans le champ de la gestion), le processus de contrôle de l'espionnage industriel constitue logiquement la formulation et la mise en œuvre d'une stratégie. Ceci se justifie de la manière suivante : dans notre cas, il s'agit de la construction d'un modèle de processus de contrôle de l'espionnage industriel, qui fera par la suite l'objet d'une étude empirique.

Au-delà du côté novateur de la méthode, le processus de contrôle de l'espionnage industriel 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.). Il ne peut, par conséquent, être dans un contexte d'encadrement d'une stratégie.

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.

Cependant, la question culminante demeure : quelle articulation des deux systèmes de contrôle serait la plus adaptée au processus de contrôle de l'espionnage industriel ?

Avant de définir les types d'articulation, nous allons présenter la grille d'analyse des deux leviers de contrôle de Renaud (2013), mettant en exergue leurs caractéristiques.

B. La grille d'analyse des systèmes de contrôle diagnostic et interactif proposée par Renaud

Cette grille de lecture établie par Renaud (2013) vise uniquement les deux leviers de contrôle de Simons destinés à la formulation et la mise en œuvre d'une stratégie.

Le tableau ci-dessous met en relief leurs caractéristiques :

Tableau 11 : La grille d'analyse des systèmes de contrôle diagnostic et interactif de Renaud (2013) [46]

[46] Source : Renaud, A. (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).

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

Simons (1995) a affirmé qu'une articulation des leviers de contrôle pourrait permettre aux entreprises d'être plus performantes. Plusieurs auteurs (Sponem, 2004 ; Tuomela, 2005 ; Widener, 2007 ; Naro et Travaillé, 2010 ; Essid et Berland, 2011 ; Gond et Igalens, 2012 ; Renaud, 2015 ; etc.) se sont intéressés à l'articulation des leviers de contrôle[47].

Etant donné que les deux leviers de contrôle, entrant dans le cadre du contrôle de gestion, sont ceux de la formulation et la mise en place d'une stratégie, plusieurs écrits scientifiques ont fait l'objet d'une articulation desdits systèmes de contrôle. Ainsi, les travaux de Renaud (2013) ont porté sur l'élaboration d'une grille d'analyse extériorisant les caractéristiques contradictoires et complémentaires des deux leviers de contrôle.

Cette grille d'analyse est pertinente, car elle donne une vision concise des deux leviers de contrôle, tout en montrant leurs spécificités, que les organisations peuvent considérer lors du choix d'un système de contrôle ou de l'articulation des deux. L'idée n'est pas de mettre en conflit les deux systèmes de contrôle pour en dévaloriser un, mais plutôt de les détailler suffisamment pour que les organisations sachent quel système de contrôle correspondrait le plus efficacement possible à telle étape de leurs stratégies. Elle constitue une lumière permettant de visualiser les différentes interactions entre le système de contrôle diagnostic et le système de contrôle interactif.

Cependant, les différentes possibilités d'y parvenir peuvent être regroupées sous les formes interrogatives suivantes :

- s'agirait-il d'une articulation « en glissement » des deux leviers de contrôle ? (méthode préconisée par Tuomela, 2005 ; Naro et Travaillé, 2010 ; Essid et Berland, 2011 ; etc.), c'est-à-dire d'un passage du système de contrôle diagnostic au système de contrôle interactif, ou l'inverse ;
- ou s'agirait-il d'une articulation « simultanée » des deux systèmes de contrôle ? (méthode préconisée par Renaud, 2015), c'est-à-dire d'un déploiement et l'émergence des stratégies.

[47] Renaud, A. (2015). *Management et contrôle de gestion environnemental*. Éditions EMS.

C. Le processus de contrôle *via* une articulation « en glissement » des leviers de contrôle diagnostic et interactif

Ce processus de contrôle peut s'opérer de deux manières, à savoir : un glissement du levier de contrôle diagnostic au levier de contrôle interactif, et un glissement du levier de contrôle interactif au levier de contrôle diagnostic.

Le premier type de glissement consiste, dans un premier temps, en une veille à la conformité des actions et résultats de l'organisation au travers des variables critiques de la performance (exemple : norme internationale ISO 27001 sur les bonnes pratiques pour la gestion de la sécurité des informations) ; dans un second temps, passer de cette méthode de conformité des objectifs à l'émergence de nouvelles stratégies, au travers d'une méthode de management impliquant fortement l'ensemble du personnel de l'organisation dans la recherche de solutions innovantes.

Contrairement, le deuxième type de glissement consiste à effectuer le même processus de contrôle, mais en commençant cette fois-ci par la méthode d'émergence des nouvelles stratégies, pour ensuite passer dans un système de conformité des actions et résultats, au travers des référentiels et normes existants.

Parmi les études sur l'articulation des leviers de contrôle de Simons (spécifiquement ceux de la formulation et la mise en œuvre d'une stratégie), la quasi-totalité porte sur ce genre d'articulation « en glissement » (De La Villarmois et Stéphan, 2005 ; Tuomela, 2005 ; Widener, 2007 ; Naro et Travaillé, 2010 ; Essid et Berland, 2011 ; Gond et Igalens, 2012 ; etc.). Tous ces auteurs partagent la même vision que Simons, qui demeure la séparation des deux leviers de contrôle. Ainsi pour Simons, « s*i une entreprise dispose de (n) systèmes de contrôle de gestion, (n-1) de ces systèmes seraient utilisés de manière diagnostique, tandis qu'un seul servirait à un usage interactif*[48] *»*.

Toutefois, l'objectif de cette articulation reste la recherche d'une meilleure performance, comme l'a mentionné Simons. Cependant, toutes les organisations ont leurs caractéristiques intrinsèques (objectifs différents, différents usages des moyens et ressources, etc.), et par conséquent il est difficile de plaider en faveur de cette articulation « en glissement » ou de celle « en parallèle ». D'autant plus que les deux types d'articulation convergent vers le même

[48] Renaud, A. (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).

objectif (rendre plus performante l'organisation), seule l'articulation des deux systèmes de contrôle les différencie.

Renaud (2013) remarque que dans les travaux de ces auteurs, *l'accent est mis sur l'évolution des systèmes de contrôle de gestion durant leur cycle de vie, ces derniers passant du levier diagnostic au levier interactif et inversement ; et que dans cette optique, le contrôle de gestion est étudié de façon linéaire par rapport au temps : on distingue alors les phases avant, pendant et après l'action*[49]. Ce qui correspond aux trois phases du processus de contrôle de Bouquin.

Selon Renaud, le contrôle de gestion ne doit pas être appréhendé selon cette linéarité, car il recouvre de son point de vue une réalité beaucoup plus complexe et nécessiterait une exploration plus approfondie de ladite dynamique.

D. Le processus de contrôle *via* une articulation « simultanée » des leviers de contrôle diagnostic et interactif

Ce mode de contrôle met en relief l'usage des leviers de contrôle diagnostic et interactif parallèlement dans un même système de contrôle. Renaud (2013) montre, au travers d'une étude de cas dans une entreprise française de vins et spiritueux, l'existence de ce système de contrôle utilisant simultanément les deux leviers de contrôle.

Cette articulation en parallèle des systèmes de contrôle diagnostic et interactif de Renaud (2013) est une continuité des travaux des auteurs de l'articulation « en glissement ». L'auteur affirme avoir mis en relief ce genre d'articulation, afin de favoriser l'utilisation d'un seul et même système de contrôle de gestion répondant à des objectifs divergents.

Ainsi, il ressort de son étude les points suivants :

- des résultats montrant qu'un seul et même système de contrôle de gestion peut être utilisé pour encadrer parallèlement deux stratégies différentes : le déploiement d'une stratégie délibérée et l'émergence d'une nouvelle stratégie ;
- un élargissement théorique quant à l'articulation des deux leviers de contrôle ;
- sur le plan pratique, l'auteur soulève des questions intéressantes sans toutefois y apporter des réponses. Il s'agit de savoir si ce système d'articulation « en simultanée » permettrait : de réduire le nombre de systèmes de contrôle de gestion

[49] *Ibid.*

dans les entreprises et de ce fait d'éviter la dispersion de l'attention des dirigeants ? ; si l'implantation d'un tel système conduit-elle les entreprises à être plus performantes ? Quels pourraient être les effets pervers d'un tel dispositif ?

Il n'existe pas autant d'écrits et de publications mettant l'accent sur ce type d'articulation « en parallèle », mais notre but était d'exposer les différentes articulations possibles des deux systèmes de contrôle dans la littérature. De ce fait, il nous a semblé nécessaire de les présenter, afin de mettre en évidence leurs caractéristiques.

Conclusion

Après une explicitation des concepts du contrôle de gestion environnemental, de la comptabilité environnementale et des coûts cachés, nous avons pu nous inspirer du cadre théorique du contrôle de gestion environnemental, qui constitue sans doute un processus connexe de notre objet de recherche, pour cadrer théoriquement le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Ainsi, nous avons pu démontrer, à travers les travaux de Simons (1995) et bien d'autres auteurs comme : Acquier (2008), Schaltegger et Burritt (2010), Schaltegger (2011), Antheaume (2013), Renaud (2013, 2015), etc., 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.

Ensuite, après une présentation de la grille d'analyse des systèmes de contrôle diagnostic et inetractif de Renaud (2013) qui met en relief leurs caractéristiques, nous avons exposé les différentes articulations des deux leviers de contrôle.

Cependant, nous ne comparons pas les deux types d'articulation, car nous estimons que les études sur l'articulation « en parallèle » nécessitent scientifiquement beaucoup plus d'éléments justificatifs, c'est-à-dire que l'auteur a mis en évidence des questions et des hypothèses très pertinentes, sans toutefois y apporter des réponses (notamment sur le plan managérial).

Nous ne dévalorisons nullement ses travaux, d'autant plus que sur le plan théorique, nous assistons à un élargissement du mode d'articulation des leviers de contrôle diagnostic et interactif (un nouveau type d'articulation nuançant éventuellement le « one best way » de l'articulation « en glissement »). Nous estimons tout simplement, qu'une multitude d'études sur ce type d'articulation permettrait d'avoir des éléments solides et probants de comparaison.

Par ailleurs, nous avons démontré l'incapacité des outils classiques du contrôle de gestion à appréhender l'espionnage industriel. De ce fait, l'étape suivante va consister à réadapter les outils classiques du contrôle de gestion pour cerner l'espionnage industriel, à ajouter un outil de calcul des coûts de l'espionnage industriel « méthodes d'évaluation des coûts cachés » (côté diagnostic) et à déterminer les outils appréhendant les incertitudes stratégiques liées à l'espionnage industriel (côté interactif).

Une fois les outils des systèmes de contrôle diagnostic et interactif déterminés, nous les analyserons à travers les six dimensions réajustées de Chiapello, dans l'objectif d'exposer sur un plan opérationnel son utilisation dans l'organisation. La section suivante met en relief le réajustement que nous effectuons sur les six dimensions d'analyse de Chiapello.

Section 3 : Les six dimensions d'analyse de Chiapello revisitées et le modèle théorique

Chiapello (1996) définit un mode de contrôle comme : « *une modalité d'exercice du contrôle* ». Cette notion de mode de contrôle est essentielle, car elle permet de détailler les différents processus et dispositifs nécessaires à la mise en œuvre d'une stratégie de contrôle. Ainsi, il consiste à spécifier, planifier et organiser les différentes étapes de contrôle dans l'organisation.

Berland[50] définit le contrôle comme : « *un mécanisme créateur d'ordre dans la mesure où il éclaire le décideur sur la pertinence de ses choix futurs, présents et passés. Il permet au décideur de discerner parmi l'ensemble des alternatives qui s'offrent à lui lesquelles sont les plus performantes. Au-delà d'éclairer les décisions, le contrôle permet de s'assurer que la déclinaison des grandes orientations de l'entreprise se fait de façon logique et cohérente. Le contrôle crée de l'ordre en aidant à prendre des décisions rationnelles et en les déclinant sous forme d'actions concrètes ».*

Dans sa tentative pour présenter le contrôle de gestion, Berland affirme que le contrôle de gestion est créateur de sens d'un double point de vue. Il permet au manager d'apprendre de son environnement et de ses actions passées en créant des boucles d'apprentissage.

Le contrôle est défini par Chiapello, comme : « *toute influence créatrice d'ordre, c'est-à-dire d'une certaine régularité* ». Il s'agit d'influencer les comportements des personnes par quelque chose ou quelqu'un, afin de les guider dans le sens des objectifs attendus de l'organisation.

Cette définition est assez large, si l'on se réfère aux définitions d'autres auteurs comme celles de Berland (définition ci-haut), de Simons (définition donnée dans la détermination du cadre théorique), qui sont plus restreintes.

Par ailleurs, ce caractère d'extension du périmètre définitionnel pourrait s'expliquer par l'objectif de l'auteur, à savoir la réconciliation des différents travaux sur les typologies des modes de contrôle dans la littérature.

[50] Berland, N. (2014). *Le contrôle de gestion : «Que sais-je?» n° 3977*. Presses universitaires de France.

Les typologies proposées par Chiapello reprennent en fait les typologies des modes de contrôle les plus connues dans le champ de la théorie des organisations[51]. Ce qui constitue une référence probante afin d'effectuer une bonne analyse.

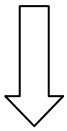
Dans la détermination du cadre théorique, nous avons déjà défini le type de contrôle correspondant à l'appréhension du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion (une articulation des leviers de contrôle diagnostic et interactif de Simons).
A présent, il s'agit de peaufiner la construction de notre modèle, c'est-à-dire le rendre opérationnel, en spécifiant les différents processus et dispositifs nécessaires à sa mise en application.

Ainsi, nous allons aborder dans une première sous-section les six dimensions d'un mode de contrôle proposées par Chiapello ; dans une deuxième sous-section, nous ferons une analyse des typologies des modes de contrôle ; ensuite nous présenterons les six dimensions de Chiapello réadaptées à l'analyse des outils des systèmes de contrôle dans une troisième sous-section ; pour terminer avec notre modèle théorique dans une quatrième sous-section.

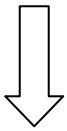
L'architecture de la section est la suivante :

[51] Chiapello, È. (1996). Les typologies des modes de contrôle et leurs facteurs de contingence: un essai d'organisation de la littérature. *Comptabilité-contrôle-audit*, *2*(2), 51-74, p.62.

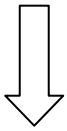
Les six dimensions d'un mode de contrôle



Une analyse des typologies des modes de contrôle de Chiapello



Les six dimensions de Chiapello réadaptées à l'analyse des outils des systèmes de contrôle



Le modèle théorique

1. Les six dimensions d'un mode de contrôle

Chiapello (1996) s'est intéressée aux différentes typologies des modes de contrôle les plus répandues des auteurs et a élaboré un modèle général intégrant l'ensemble des caractéristiques dimensionnelles d'un mode de contrôle.

Pour mieux dissocier le contrôle et les modes de contrôle, Chiapello définit, au travers de l'approche de Hopwood (1974) sur les facteurs d'influence et le contrôle global résultant, le contrôle comme : « *la résultante de l'ensemble des influences à l'œuvre »* et les modes de contrôle *: « pour définir les facteurs d'influence particuliers ».*

Ensuite, l'auteur décrit les six éléments ci-dessous comme étant la description des facteurs d'influence, c'est-à-dire qu'un « *mode de contrôle est toute configuration cohérente intégrant les six éléments suivants »* :

- la source de l'influence (qui ou quoi exerce l'influence) ;
- ce sur quoi elle s'exerce ;
- la réaction de celui qui est soumis à l'influence et son attitude face au contrôle ;
- les moments privilégiés, s'il en est, où le contrôle s'exerce ;
- le processus par lequel l'influence s'exerce ;
- le moyen, ou vecteur, utilisé.

Chiapello a conceptualisé le mode de contrôle à travers les notions de facteurs d'influence qui pèsent sur les comportements du personnel et a commencé à analyser les différentes typologies de contrôle, via les six éléments ci-haut. Les travaux de synthèse de l'auteur aboutirent à la définition de six dimensions d'analyse des modes de contrôle.

Les six dimensions d'un mode de contrôle constituent une grille de comparaison des différents types de contrôle, comme le démontre Chiapello (1996) au travers de son essai d'organisation de la littérature sur les typologies des modes de contrôle.

L'auteur a procédé à une analyse des typologies de contrôle les plus répandues à travers une grille de classification constituée des six dimensions, afin d'identifier leurs points de similitude et de différence.

Pour Chiapello, tout mode de contrôle en organisation doit intégrer les six dimensions suivantes :

Tableau 12 : Les six dimensions d'analyse des modes de contrôle en organisation, Chiapello, 1996

Qui contrôle ?	**Sur quoi s'exerce le contrôle ?**
. L'organisation - machine - administration - structure . Une personne . Un groupe de personnes . Soi-même	. Les actions . Les résultats . Les caractéristiques du personnel . Le contexte affectif . La culture . Les normes . Les objectifs et stratégies
Quelle est l'attitude du contrôlé ?	**Quand le contrôle a-t-il eu lieu ?**
. Implication morale . Relation instrumentale . Aliénation	. Avant l'action . Pendant l'action . Après l'action
Quels sont les processus de contrôle ?	**Quels sont les moyens du contrôle ?**
. Cybernétiques, homéostatiques . Non cybernétiques : - modèle politique - modèle de la poubelle	. Le marché . L'organisation - règlements - contrôle de gestion - structure . La culture - de l'organisation - de la société - des professionnels . Les relations inter-individuelles

En plus de cette aptitude d'analyse des modes de contrôle, nous estimons que les six dimensions d'un mode de contrôle permettent de clarifier l'application concrète d'un système de contrôle dans l'organisation, car ce sont des éléments qui spécifient les processus et

dispositifs d'un système de contrôle comme : les moments du contrôle, sur quoi s'exerce le contrôle, les moyens du contrôle…

L'idée consiste à partir de l'analyse du type de contrôle (dans notre cadre, l'application des leviers de contrôle diagnostic et interactif de Simons sur le processus de contrôle de l'espionnage industriel), via les six dimensions d'analyse réajustées de Chiapello, pour détailler et décortiquer suffisamment lesdits leviers de contrôle.

Cette analyse fractionnera individuellement les deux systèmes de contrôle en six dimensions (éventuellement), et permettra de mettre en exergue les processus et dispositifs détaillés pour une compréhension pratique de leur mise en œuvre dans l'organisation.

Par conséquent, ce fractionnement permettra de clarifier les étapes de contrôle, les tâches à effectuer, les personnes concernées… Ce qui contribuera à donner une vision plus opérationnelle, sur un plan managérial, à la mise en œuvre de notre modèle dans l'organisation.

Nous allons, à présent, procéder à une analyse des typologies des modes de contrôle de Chiapello pour cerner ses apports et limites, afin d'avoir une meilleure exploitation des dimensions d'analyse dans notre étude.

2. Une analyse des typologies des modes de contrôle de Chiapello

Les auteurs et chercheurs (Reeves et Woodward, Hopwood, Ouchi, Anthony, Mintzberg, Etzioni, Bouquin, Hofstede, Flamholtz, Petitjean, Das et Tsui, etc.) ont défini différentes typologies de contrôle dans une organisation. Chiapello a défini une grille de classification des différents modes de contrôle, en fonction des six dimensions élaborées suite à ses travaux d'analyse.

Cependant, chaque auteur se distingue par la mise en avant d'une dimension par rapport à une autre. Cette priorisation constitue la principale différence des différentes typologies de contrôle proposées et permet aux organisations de choisir le mode de contrôle adéquat à leurs structures. Le choix du type de processus de contrôle diffère d'une organisation à l'autre. Cependant, il est difficile d'affirmer que tel processus est approprié à l'ensemble des organisations.

Chaque organisation ayant ses caractéristiques intrinsèques peut s'adapter à une typologie de contrôle, qui l'oriente parfaitement vers ses attendus. Le dessein de Chiapello, lors de la

définition des six dimensions d'analyse des modes de contrôle en organisation, était l'élaboration d'une typologie générale des modes de contrôle, qui intégrerait toutes les autres typologies en prenant en compte le plus grand nombre de dimensions d'analyse.

L'auteur montre, par la suite, comment arriver à ce modèle de synthèse, en analysant les différentes typologies les plus répandues via ses six dimensions, dans le but d'exposer les points de liaison entre elles, au travers de leurs similitudes et différences.

Un des principaux apports de Chiapello demeure cette conceptualisation des modes de contrôle à travers ses six dimensions d'analyse. Théoriquement, cette grille de classification est beaucoup utilisée dans le champ de la gestion.

Sur un plan pratique, elle donne l'occasion aux organisations de choisir le type de contrôle adéquat à leurs attentes. Nos estimons également qu'elle permet de clarifier, sur un plan opérationnel, les mécanismes de contrôle dans l'organisation comme : les étapes de contrôle, les tâches à effectuer, les personnes concernées…

Par ailleurs, il y a des limites qui ont été relevées par Chiapello, comme :

- la médiocre prise en compte des influences externes, que l'auteur explique par le faible degré de maîtrise des managers sur celles-ci ;
- le problème de représentativité des modes de contrôle choisis dans le cadre de ses travaux, vu que leur identification se situe à un niveau assez global (c'est-à-dire le contrôle par la culture choisi dans son étude est-il représentatif des nombreux types de contrôle selon les caractéristiques de la culture ?) ;
- chacun des grands modes de contrôle identifiés au croisement des six axes d'analyse, sur lesquels sont basées les analyses de Chiapello, est sujet de décomposition en différents styles et types…

Malgré ces limites, l'auteur a le mérite d'avoir mis au point une conceptualisation cohérente et efficace à l'analyse des typologies des modes de contrôle. Cette grille d'analyse reste un outil très utile que nous allons confronter à nos deux leviers de contrôle, dans l'objectif de peaufiner la mise en œuvre de notre modèle dans l'organisation.

Conclusion

Nous avons présenté les six dimensions d'analyse des typologies des modes de contrôle élaborées par Chiapello, et nous les avons analysées pour décliner le dessein de l'auteur quant aux objectifs attendus. Ensuite, nous avons fait ressortir quelques apports et limites, afin d'optimiser efficacement l'utilisation de ces dimensions dans notre recherche.

Les six dimensions de Chiapello s'avèrent efficaces pour détailler le processus de mise en œuvre d'un système de contrôle dans l'organisation.

Cependant, nous escomptons confronter nos deux leviers de contrôle aux six dimensions réajustées de Chiapello, sans toutes fois affirmer que lesdites dimensions sont les meilleures, quant à la décortication des étapes et moyens de nos deux systèmes de contrôle. Nous estimons tout simplement qu'elles permettent de bien détailler la mise en œuvre d'un système de contrôle dans l'organisation.

3. Les six dimensions de Chiapello réadaptées à l'analyse des outils des systèmes de contrôle

La mise en application de tout système de gestion doit être suffisamment détaillée dans l'objectif d'une bonne coordination et d'une bonne réussite de sa mise en œuvre. L'utilisation des leviers de contrôle diagnostic et interactif pour cerner la gestion de l'espionnage industriel reste encore théorique.

Pour mettre en œuvre un système de gestion, les entreprises ont besoin de connaitre le mode d'emploi dudit système et le rôle joué par chaque personnel, afin d'envisager son intégration managériale.

Dans la discipline de la gestion, il ne suffit pas de déterminer des outils de gestion sans préciser les modalités d'application desdits outils. Il est important de détailler l'application, la portée et les caractéristiques des outils définis.

Ainsi, l'objectif de cette partie est de finaliser le modèle du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion, en le structurant et en exposant sur un plan managérial son utilisation dans l'organisation.

Pour ce faire, nous faisons passer les différents outils des leviers de contrôle diagnostic et interactif de l'espionnage industriel à la grille des six dimensions d'un mode de contrôle réajustées de Chiapello.

Ces six dimensions d'analyse, qui définissent les personnes à intervenir, l'attitude du contrôlé, les moyens de contrôle, les moments du contrôle, les processus de contrôle et sur quoi s'exerce le contrôle, permettront d'opérationnaliser sur un plan pratique les systèmes de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Nous allons utiliser les six dimensions de Chiapello **sous une vision différente de sa vision initiale**, car en plus de sa capacité d'analyse des modes de contrôle, nous estimons que lesdites dimensions permettent de définir concrètement la mise en œuvre d'un système de contrôle dans l'organisation.

Cette présomption s'explique par les caractéristiques explicatives des éléments desdites dimensions : les moments du contrôle, sur quoi s'exerce le contrôle, les moyens du contrôle…

Au lieu d'analyser les dimensions des modes de contrôle (vision de Chiapello), l'idée consiste plutôt à utiliser **ces six dimensions réajustées sur les outils des leviers de contrôle pour**

détailler et décortiquer suffisamment les étapes des systèmes de contrôle utilisés dans le cadre de cette recherche.

Chiapello (1996) a élaboré son modèle général intégrant l'ensemble des caractéristiques dimensionnelles d'un mode de contrôle, à partir des différentes typologies des modes de contrôle les plus répandues dans le champ de la théorie des organisations.

Dans cette recherche, nous ne prétendons nullement révolutionner les dimensions d'analyse de Chiapello pour caractériser les outils des systèmes de contrôle. Nous voulons réadapter lesdites dimensions d'analyse des modes de contrôle aux outils des leviers de contrôle de notre étude, pour expliquer suffisamment et concrètement la mise en application de ces outils dans l'organisation.

Cette méthode de réadaptation consiste simplement à rediriger les questions d'analyse de Chiapello vers l'utilisation des outils des systèmes de contrôle, sans toutefois s'éloigner sémantiquement des dimensions de l'auteur.

Ce processus scinde individuellement les deux systèmes de contrôle en six dimensions, et permet de spécifier les différentes étapes nécessaires à leur mise en œuvre dans l'organisation. Sur un plan managérial, ça facilite la planification, l'organisation et la coordination des tâches, c'est-à-dire que ça permet aux managers de l'organisation de mieux cerner et se situer sur les travaux à effectuer dans le cadre du processus de contrôle de l'espionnage industriel.

Pour ce faire, les questions d'analyse seront réadaptées aux outils des systèmes de contrôle de la manière suivante :

Tableau 13 : Les six dimensions d'analyse de Chiapello réadaptées à l'analyse des outils des systèmes de contrôle

Les six dimensions d'analyse des modes de contrôle de Chiapello	Les six dimensions de Chiapello réadaptées à l'analyse des outils des systèmes de contrôle
Qui contrôle ? . L'organisation - machine - administration - structure . Une personne . Un groupe de personnes . Soi-même	**Qui utilise cet outil ?**
Sur quoi s'exerce le contrôle ? . Les actions . Les résultats . Les caractéristiques du personnel . Le contexte affectif . La culture . Les normes . Les objectifs et stratégies	**Sur quoi s'utilise cet outil ?**
Quelle est l'attitude du contrôlé ? . Implication morale . Relation instrumentale . Aliénation	**Quelle est l'attitude de l'utilisateur de cet outil ou du contrôlé ?**
Quand le contrôle a-t-il eu lieu ? . Avant l'action . Pendant l'action . Après l'action	**Quand utilise-t-on cet outil ?**
Quels sont les processus de contrôle ? . Cybernétiques, homéostatiques . Non cybernétiques : - modèle politique - modèle de la poubelle	**Quels sont les processus (étapes) d'utilisation de cet outil ?**
Quels sont les moyens du contrôle ? . Le marché . L'organisation - règlements - contrôle de gestion - structure . La culture - de l'organisation - de la société - des professionnels . Les relations inter-individuelles	**Quels sont les moyens d'utilisation de cet outil ?**

Le tableau ci-haut redirige les six dimensions d'analyse réajustées vers les outils des leviers de contrôle. Les différentes étapes d'élaboration de ces outils feront l'objet du chapitre 4. Ainsi, nous estimons que les réponses à ces questions permettront de détailler et de faciliter suffisamment la mise en œuvre du système de contrôle de l'espionnage industriel.

Nous allons maintenant présenter le modèle théorique d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

4. Le modèle théorique

Le modèle théorique de notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion est une représentation schématique montrant la structure globale, les liaisons entre les différents concepts mobilisés et les étapes d'intervention.

Nous avons explicité le contrôle de gestion environnemental, la comptabilité environnementale et les coûts et performances cachés, qui présentent certaines caractéristiques communes avec notre objet de recherche. Ces différents éléments constituent des références connexes.

Ensuite, nous avons pu nous inspirer du cadre théorique du contrôle de gestion environnemental, qui constitue sans doute un processus connexe de notre objet de recherche, pour cadrer théoriquement le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Nous avons pu démontrer, à travers les travaux de Simons (1995) et bien d'autres auteurs comme : Acquier (2008), Schaltegger et Burritt (2010), Schaltegger (2011), Antheaume (2013), Renaud (2013, 2015), 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.

Au cours de ce développement, nous avons démontré l'incapacité des outils classiques du contrôle de gestion à appréhender l'espionnage industriel. Or, les deux leviers de contrôle, permettant d'appréhender le processus de contrôle de l'espionnage industriel, sont les systèmes de contrôle diagnostic et interactif.

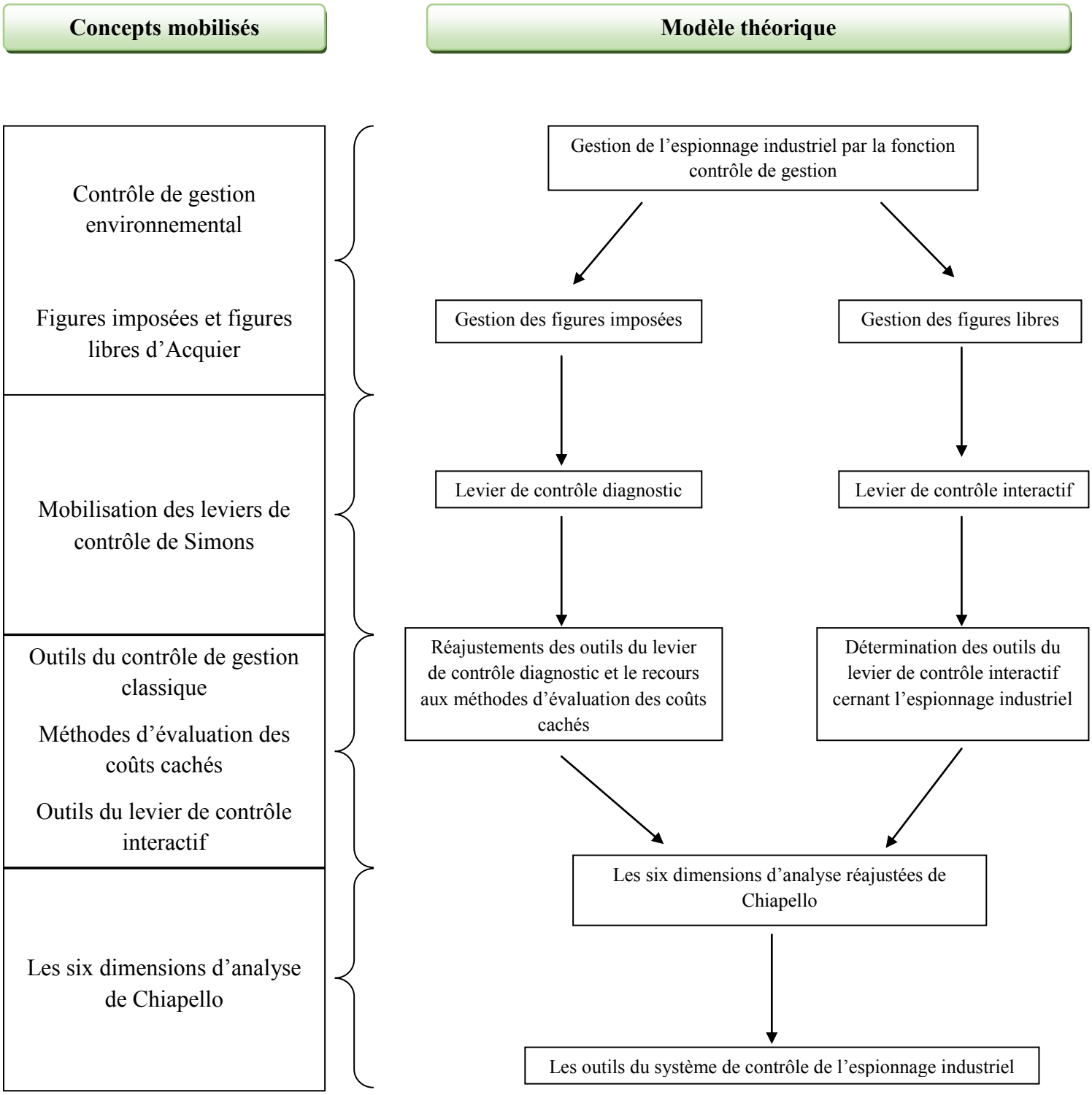
Sachant que les outils du système de contrôle diagnostic correspondent à ceux du contrôle de gestion « classique ou traditionnel », il est nécessaire de réajuster ces outils classiques du

contrôle de gestion, pour cerner l'espionnage industriel (côté diagnostic) et de déterminer les outils appréhendant les incertitudes stratégiques liées à l'espionnage industriel (côté interactif).

Une fois les réajustements effectués sur les outils classiques du contrôle de gestion, l'ajout d'un outil de calcul des coûts de l'espionnage industriel (méthodes d'évaluation des coûts cachés qui seront détaillées dans le chapitre 4) et la détermination de quelques outils du levier de contrôle interactif, nous les analysons à travers les six dimensions réajustées de Chiapello, dans l'objectif d'exposer sur un plan opérationnel la mise en œuvre dans l'organisation.

Ci-dessous le modèle théorique avec les concepts mobilisés :

Figure d : Modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion


Concepts mobilisés
Modèle théorique
Contrôle de gestion environnemental
Figures imposées et figures libres d'Acquier
Mobilisation des leviers de contrôle de Simons
Outils du contrôle de gestion classique
Méthodes d'évaluation des coûts cachés
Outils du levier de contrôle interactif
Les six dimensions d'analyse de Chiapello
Gestion de l'espionnage industriel par la fonction contrôle de gestion
Gestion des figures imposées
Gestion des figures libres
Levier de contrôle diagnostic
Levier de contrôle interactif
Réajustements des outils du levier de contrôle diagnostic et le recours aux méthodes d'évaluation des coûts cachés
Détermination des outils du levier de contrôle interactif cernant l'espionnage industriel
Les six dimensions d'analyse réajustées de Chiapello
Les outils du système de contrôle de l'espionnage industriel

Ce modèle théorique nous semble être une solution adéquate au problème de gestion de l'espionnage industriel dans les entreprises. Il s'articule certainement avec des outils du contrôle de gestion et des outils de gestion en général (outils qui seront présentés dans le chapitre 4), mais il reste transversal et nécessite l'implication de chaque personnel pour sa mise œuvre.

Il part de la problématique de gestion de l'espionnage industriel et aboutit aux outils du système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, en détaillant les différents concepts et théories mobilisés.

Nous n'évoquons nullement la perfection de ce modèle, car il est dynamique et sujet d'amélioration. Cependant, nous nous sommes adossés sur des bases solides dans les règles de scientificité pour construire ce modèle théorique.

Dans les étapes suivantes, nous allons présenter notre organisation méthodologique des travaux de terrain, pour détailler les étapes d'élaboration du système avec ses outils managériaux, et présenter le système complet de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Conclusion du chapitre 2

Dans ce chapitre, nous avons mobilisé plusieurs concepts et théories, qui ont contribué à la construction d'un modèle théorique de gestion de l'espionnage industriel par la fonction contrôle de gestion.

L'espionnage industriel demeure un sujet d'actualité, qui connait un essor sans précédent dans le monde des entreprises. Ces conséquences sont désastreuses et il reste un phénomène mal géré par les entreprises.

Même si des efforts sont effectués, il reste encore énormément à faire. Le contrôle interne (gestion par les entreprises elles-mêmes), les textes de loi et les différentes réglementations contribuent, certes, à atténuer le phénomène, mais présentent des limites qui doivent être analysées et étudiées.

Nous avons démontré que l'appréhension de l'espionnage industriel par la fonction contrôle de gestion pourrait permettre de maîtriser davantage le fléau, voire même empêcher sa survenance.

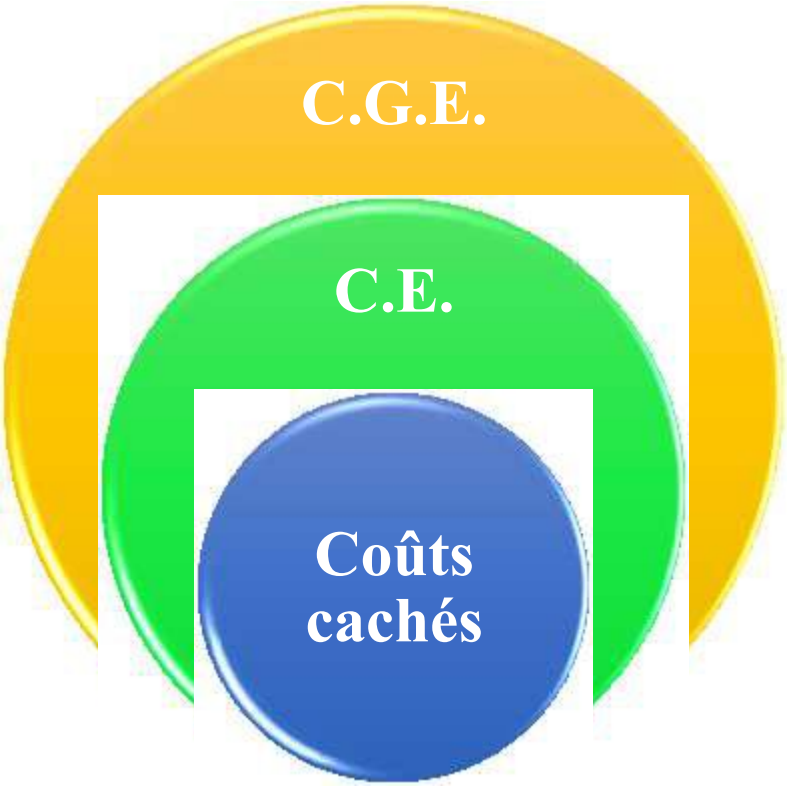
Cependant, il est important de préciser que cette solution par la fonction contrôle de gestion est une continuité sur les travaux du contrôle interne, c'est-à-dire que nous nous sommes proposés d'étudier la question, afin de combler les trous de gestion du contrôle interne, en proposant une nouvelle alternative.

Cette alternative, qui constitue une amélioration de la gestion de l'espionnage industriel par la fonction contrôle interne, s'effectue via un modèle théorique de gestion de l'espionnage industriel par la fonction contrôle de gestion.

Ainsi, nous avons détaillé le contrôle de gestion environnemental, la comptabilité environnementale et les coûts et performances cachés, qui sont des concepts très étudiés et présentant certaines caractéristiques communes avec notre objet de recherche.

Nous avons clarifié les liens qui existent entre les différents concepts, tout en nous focalisant sur le contrôle de gestion environnemental qui semble englober les autres concepts :

Figure e : Le lien entre le contrôle de gestion environnemental, la comptabilité environnementale et les coûts cachés



Partant de ces éléments de référence, nous avons pu nous inspirer du cadre théorique du contrôle de gestion environnemental, pour déterminer un cadre théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

A cet effet, nous avons mobilisé les travaux de Simons (1995) et bien d'autres auteurs comme : Acquier (2008), Schaltegger et Burritt (2010), Schaltegger (2011), Antheaume (2013), Renaud (2013, 2015), pour démontrer 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.

A ce stade, il faut déterminer les outils des deux systèmes de contrôle (objet du chapitre 4) pour compléter le système.

En ce qui concerne le levier de contrôle diagnostic, nous avons démontré dans notre raisonnement l'incapacité des outils classiques du contrôle de gestion à appréhender

l'espionnage industriel dans leur état (car ce sont des outils qui ont pour vocation de cerner les phénomènes et processus de marché).

Par conséquent, des réajustements sont nécessaires pour amplifier les aptitudes des outils classiques du contrôle de gestion. Par ailleurs, les méthodes d'évaluation des coûts et performances cachés présentent certaines caractéristiques, qui leur mettent en première ligne pour l'évaluation des coûts de l'espionnage industriel.

Quant au levier de contrôle interactif, il s'agit de déterminer les outils permettant de cerner les incertitudes stratégiques liées à l'espionnage industriel.

Dans un souci d'une bonne mise en application des outils des deux leviers de contrôle, nous avons revisité les six dimensions d'analyse de Chiapello, pour permettre aux managers de l'organisation de mieux cerner et se situer sur les travaux à effectuer dans le cadre du processus de contrôle de l'espionnage industriel.

Tous ces éléments ont contribué à la structuration d'un modèle théorique de gestion de l'espionnage industriel par la fonction contrôle de gestion.

Le chapitre suivant fait l'objet d'une présentation de notre organisation méthodologique des travaux de terrain.

PARTIE II :
DETERMINATION EMPIRIQUE D'UN SYSTEME DE CONTROLE DE L'ESPIONNAGE INDUSTRIEL PAR LA FONCTION CONTROLE DE GESTION

Chapitre 3 : Posture épistémologique et méthodologie

L'organisation méthodologique d'un travail de recherche scientifique est importante et doit être bien structurée. Elle a pour finalité de tenir compte des éléments empiriques dans 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 terrain de recherche. En effet, la revue de littérature nous a permis de nous interroger sur les raisons qui font que les organisations peinent à mettre en place un processus de contrôle de l'espionnage industriel, qui comblerait l'absence d'un outil d'évaluation des coûts de l'espionnage industriel, l'absence d'un pilotage des outils et moyens de protection contre l'espionnage industriel dans les entreprises…

Cette organisation méthodologique répond à une série de questions, comme :

- Quel type d'informations empiriques allons-nous chercher ?
- Où allons-nous les chercher ?
- Auprès de qui ou de quoi ?
- En posant quelles questions ?
- Sous quelle forme ? Questionnaires ou entretiens dirigés ou semi-dirigés ? Données d'archives ou d'enquête ?
- Quel échantillon ?
- Analyse de discours ? Comment ?
- Analyse d'un courant intellectuel, d'un auteur ? Selon quelles perspectives ?

Ces questions permettent de comprendre l'itinéraire scientifique des travaux de recherche et procurent ainsi une validité à la connaissance, comme le stipulent Perret et Seville (2007) : « *exposer ses réflexions épistémologiques revient à expliciter la conception du monde et*

l'objectif de la recherche qui sous-tendent toute recherche. Cette démarche, indispensable au contrôle de la recherche, permet d'accroître la validité de la connaissance qui en est issue ».

Ainsi, nous allons présenter dans une première section la démarche et la posture épistémologique de cette recherche ; et nous allons aborder dans une deuxième section le mode de recueil et le traitement des données.

L'architecture du chapitre est la suivante :

Section 1 **Démarche de recherche et posture épistémologique**	
Une démarche qualitative	Posture épistémologique

⇩

Section 2 **Recueil et traitement des données**			
Choix de l'échantillon	Mode de recueil des données	Traitement des données	Premiers enseignements empiriques d'une démarche hypothético-inductive

Section 1 : Démarche de recherche et posture épistémologique

La méthodologie de la recherche permet d'avoir une vision globale et claire de l'ensemble des étapes des travaux de recherche.

Nos travaux de recherche sur le terrain se sont déroulés principalement en deux temps :

- un premier travail empirique qui avait pour objectif d'explorer le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion dans les organisations ;
- suite au premier travail de terrain, nous avons opté pour l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, en nous inspirant des concepts connexes, notamment le contrôle de gestion environnemental, la comptabilité environnementale et les coûts et performances cachés. Une fois, le système construit, le deuxième travail empirique a été déclenché dans le dessein de récolter les suggestions de notre échantillon et d'améliorer ledit système.

La méthodologie de recherche et la posture épistémologique déterminent la manière de chercher et adossent le chercheur à des techniques scientifiques spécifiques.

Ainsi, nous allons aborder la démarche qualitative dans une première sous-section (1) et la posture épistémologique adoptée dans une deuxième sous-section (2).

L'architecture de la section est la suivante :

Une démarche qualitative

⇩

Posture épistémologique

1. Une démarche qualitative

Selon Mbengue (2001)[52], la méthodologie d'une recherche représente : « *l'itinéraire de la recherche et englobe à la fois les étapes de choix, de production, de recueil, de traitement, d'analyse (ou traitement) des données, etc.* ».

Les méthodes quantitatives et qualitatives sont les deux démarches utilisées dans le domaine des Sciences de Gestion. Les premières méthodes se basant uniquement sur des données mesurables (numériques ou informations convertibles en chiffres), tandis que les méthodes qualitatives peuvent se baser sur des données non numériques, des informations qui seront ensuite analysées par des procédures bien spécifiques.

Les deux méthodes peuvent être utilisées dans une même recherche en les chevauchant, comme l'utilisation des méthodes qualitatives dans la première partie de la recherche et celle des méthodes quantitatives dans la dernière partie de la recherche.

L'image de la recherche quantitative est beaucoup plus claire par rapport à celle de la recherche qualitative. Cependant, les méthodes qualitatives n'en demeurent pas moins des bonnes méthodes de recherche.

L'exploration est le plus souvent liée à la méthode qualitative et la vérification à la méthode quantitative. Nonobstant, il est important de préciser que les deux méthodes ne sont pas forcément contradictoires, elles sont plutôt complémentaires.

Nous nous inscrivons dans une démarche qualitative avec une approche hypothético-inductive se traduisant par des allers et retours entre le terrain et la littérature théorique, car les caractéristiques de notre cadre théorique influencent largement les choix méthodologiques. Le sujet est novateur et sensible, par conséquent les méthodes qualitatives semblent appropriées pour aborder les questions délicates sur l'espionnage industriel.

Contrairement à la méthodologie quantitative qui s'alimente par des chiffres, notre méthodologie se nourrit principalement des textes et discours (entretiens, documents, rapports nationaux, rapports internationaux, etc.), nous pouvons conclure que la méthodologie adoptée dans cette recherche pour répondre à notre question de recherche est une méthodologie qualitative avec une approche hypothético-inductive (se traduisant par des allers et retours entre le terrain et la littérature théorique).

[52] Mbengue A. (2001), « Posture paradigmatique et recherche en management stratégique », *in Stratégies – Actualités et futurs de la recherche*, sous la dir. D'A.C. Martinet et R.A. Thiétart (Ed.), Vuibert, p.46-47.

Les méthodes qualitatives de recueil des données constituent le moyen le plus pertinent pour avoir des données riches et ciblées touchant les sujets de nature occulte (sans toutefois remettre en cause la méthode quantitative).

Face à la complexité due à la nature occulte de l'espionnage industriel et au manque de littérature, la recherche a été menée au travers des allers-retours entre théorie et terrain dans une démarche qualitative, ce qui a conduit à la construction progressive de l'objet de recherche.

Selon Allard-Poesi et Maréchal (2014), cette interaction entre le chercheur et le sujet d'étude permet de développer une compréhension de la réalité des sujets étudiés et s'inscrit dans une posture interprétative.

2. Posture épistémologique

Le positionnement épistémologique est important à présenter pour valoriser scientifiquement ses travaux de recherche, comme le précisent Mbengue et Vandangeon-Derumez (1999)[53] : « *qu'il soit sur le point de s'engager dans une recherche nouvelle ou qu'il soit en situation d'examiner une recherche déjà effectuée, le chercheur est amené à s'interroger sur un certain nombre de points pouvant porter aussi bien sur les données elles-mêmes que sur la valeur scientifique des résultats attendus ou obtenus. […] toute recherche reflète une position épistémologique, que cette dernière soit affichée et revendiquée ou non par son auteur* ».

Perret et Séville (2007) stipule que *« la réflexion épistémologique s'impose à tout chercheur soucieux d'effectuer une recherche sérieuse car elle permet d'asseoir la validité et la légitimité d'une recherche ».*

C'est à partir de la question de recherche, que se détermine généralement le déroulement de la recherche.

Pour répondre à la question de recherche, il est indispensable de connaitre quelques éléments du terrain, comme :

- quelles sont les données disponibles ou accessibles sur le terrain ?
- quel type d'étude le chercheur peut réaliser dans ce contexte ?

[53] Mbengue A. et Vandangeon-Derumez I. (1999), « Positions épistémologiques et outils de recherche en management stratégique », Huitième conférence internationale de management stratégique de l'AIMS, p. 22.

Piaget (1967) définit l'épistémologie comme « *l'étude de la constitution des connaissances valables* ». Thietart et al. (2014) la définissent à leur tour comme : « *une activité réflexive qui porte sur la manière dont les connaissances sont produites et justifiées* ».

Dans la discipline des Sciences de Gestion, les postures épistémologiques couramment utilisées (Rouleau, 2007 ; Perret, et Seville, 2003 ; Wacheux, 1996) sont :

- le positivisme ;
- l'interprétativisme ;
- le constructivisme.

Certains auteurs opposent deux courants ou deux visions, à savoir le positivisme et la phénoménologie (comprenant l'interprétativisme et le constructivisme).

Le positivisme se définit comme un « *système, qui considère que toutes les activités philosophiques et scientifiques ne doivent s'effectuer que dans le seul cadre de l'analyse des faits réels vérifiés par l'expérience et que l'esprit humain peut formuler les lois et les rapports qui s'établissent entre les phénomènes et ne peut aller au-delà* »[54].

L'interprétativisme s'oppose au positivisme et se dit d'une « *théorie dans la mesure où elle permet de rattacher certains phénomènes visibles à des processus non perceptibles qui les rendent compréhensibles et où elle fournit ainsi une sorte de lecture de ces phénomènes* » (Encyclopédie Universalis, 1995).

Le constructivisme est une « *attitude ouverte de recherche, plutôt qu'avec un paradigme définitif (positiviste). […] le chercheur produit des explications, qui ne sont pas la réalité, mais un construit sur une réalité susceptible de l'expliquer* » (Wacheux, 1996).

Le tableau ci-dessous met en exergue les caractéristiques des trois approches épistémologiques.

[54] Définition Larousse 2018.

Tableau 14 : Regard sur les trois grandes approches épistémologiques *(d'après Allard-Poesi et Maréchal, 2007)*[55]

	Approche positiviste	Approche interprétative	Approche constructiviste
Vision de la réalité	Ontologie du réel	Phénoménologie du réel	
Relation sujet/objet	Indépendance	Interaction	
Objectif de la recherche	Découvrir la réalité	Comprendre les significations que les gens attachent à la réalité sociale, leurs motivations et intentions	Construire une représentation instrumentale et/ ou un outil de gestion utile pour l'action
Validité de la connaissance	Cohérence avec les faits	Cohérence avec le l'expérience du sujet	Utilité/convenance par rapport à un projet
Origine de la connaissance	Observation de la réalité	Empathie	Construction
Nature de l'objet de recherche	Interrogation des faits	Développement d'une compréhension de l'intérieur d'un phénomène	Développement d'un projet de connaissance
Origine de l'objet de recherche	Identification d'insuffisances théoriques pour expliquer ou prédire la réalité	Immersion dans le phénomène étudié	Volonté de transformer la connaissance proposée en élaborant de nouvelles réponses

[55] Bulinge, F. (2010). Renseignement militaire: une approche épistémologique. *Revue internationale d'intelligence économique*, *2*(2), 209-232.

Nous remarquons bien que l'approche positiviste se distingue largement des deux autres approches, qui semblent avoir des points communs. L'interprétativisme et le constructivisme partagent des points, comme :

- ce qui est connaissable relève de l'expérience et du vécu de l'individu ;
- la production de la connaissance dépend de l'environnement, des pensées et les actions des individus guidées par les intentions et les finalités de ces derniers…

Les fondamentaux des deux approches sont quasiment identiques. La différence réside au niveau de l'hypothèse ontologique, comme l'expliquent Gavard-Perret *et al.* (2012) : « *les interprétativistes s'accordent à la fois pour récuser l'hypothèse d'existence d'un réel objectif indépendant de l'observateur et pour poser des hypothèses fondatrices d'ordre ontologique - alors que le constructivisme radical ne nie pas l'existence possible d'un réel extérieur au chercheur, indépendant de lui et de l'attention qui lui accorde. Il conteste seulement la possibilité de connaitre ce réel indépendamment des perceptions qu'il induit* ». Ces affirmations sont corroborées par Von Glaserfeld (2001), qui explique que le constructivisme radical « *nie seulement que nous ne puissions connaître rationnellement un réel au-delà de notre expérience* ».

L'objectif de notre recherche, à savoir l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, a tendance à privilégier la posture constructiviste.

Cependant, nous avons une posture interprétative, car nous élaborons un système de contrôle de l'espionnage industriel, en tenant compte des suggestions et améliorations des professionnels du contrôle de gestion, comme le soulignent Perret et Séville (2007) : « *pour l'interprétativiste, le processus de création de connaissance passe par la compréhension du sens que les acteurs donnent à la réalité. Il ne s'agit plus d'expliquer la réalité mais de la comprendre au travers des interprétations qu'en font les acteurs. Il développe ainsi une démarche qui doit prendre en compte les intentions, les motivations, les attentes, les raisons, les croyances des acteurs, qui porte moins sur les faits que sur les pratiques* ».

Le choix de cette démarche s'est imposé à nous d'une manière légitime, compte tenu de la rareté des théories mobilisables et de l'insuffisance des connaissances sur l'espionnage industriel.

Dans cette recherche, nous avons effectué deux travaux empiriques, dont le premier avait pour objectif d'explorer le processus de contrôle de l'espionnage industriel dans les organisations. Les résultats de cette première exploration ont suscité la naissance d'un second travail de terrain, dont l'objectif était d'évaluer le système de contrôle de l'espionnage industriel par la fonction contrôle de gestion que nous avons construit.

Par ailleurs, chacun des travaux empiriques menés était un processus de création de connaissance passant par la compréhension du sens que les acteurs donnaient à la réalité. Nous avons voulu comprendre la réalité au travers des interprétations qu'en font les acteurs. Cette compréhension prend en compte les intentions, les motivations, les attentes, les raisons, les croyances des acteurs, qui portent moins sur les faits que sur les pratiques.

Ces caractéristiques correspondent à celles de l'interprétativisme, par conséquent nous nous inscrivons dans cette posture épistémologique.

Section 2 : Recueil et traitement des données

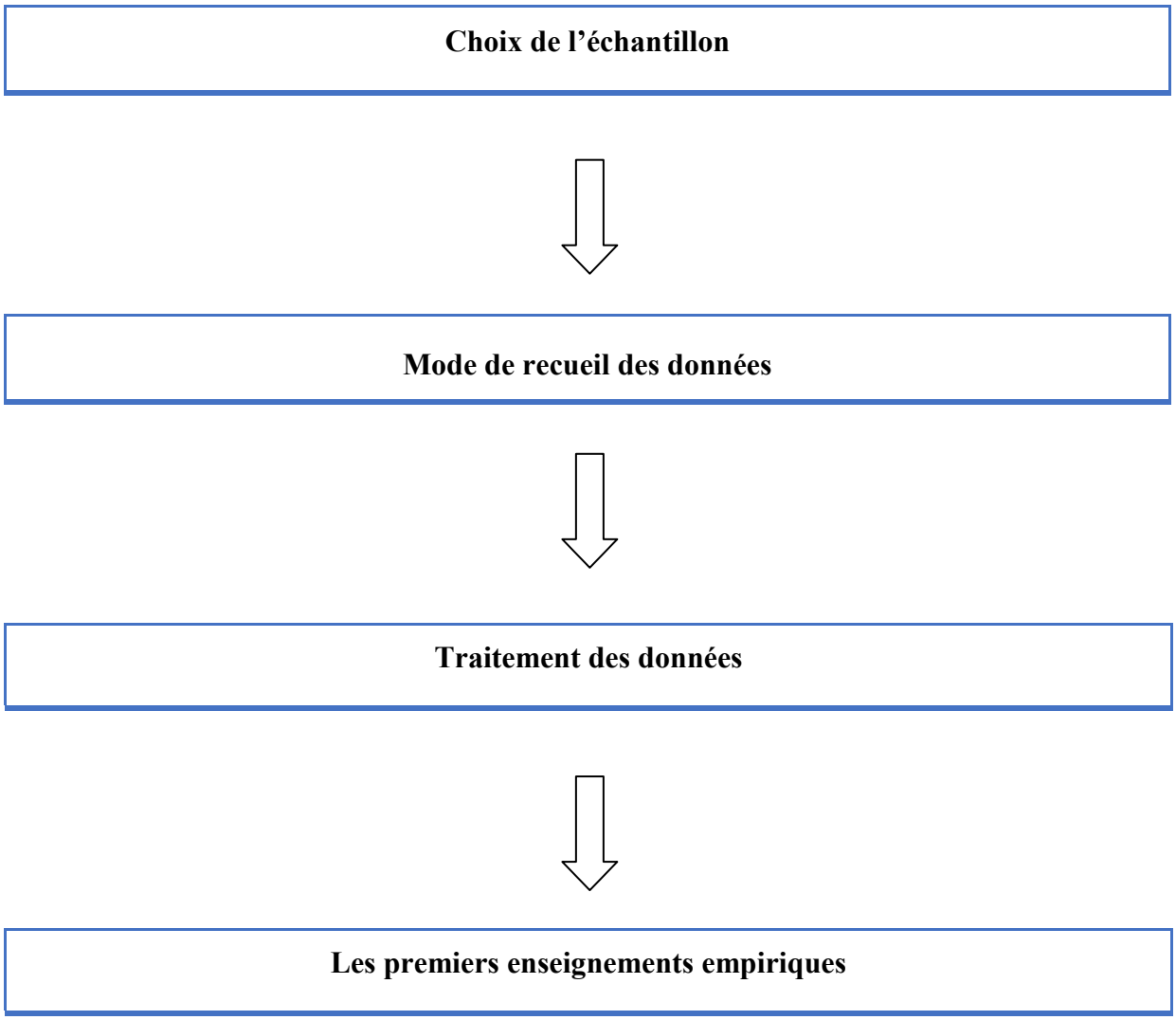
La littérature scientifique propose plusieurs manières de collecter les données d'une recherche, selon qu'il s'agisse des données quantitatives et ou qualitatives. Cependant, collecter des données respecte un certain nombre de règles pour une étude empirique et passe par la précision de certaines étapes, notamment :

- le type de données à collecter ;
- le choix de l'échantillon ;
- le mode de recueil des données…

Une fois les données collectées, l'étape suivante consiste à les analyser et les interpréter afin de présenter les résultats de l'étude. Pour ce faire, nous disposons également d'une panoplie de méthodes de traitement des données recueillies.

Ainsi dans cette section, nous allons expliciter les caractéristiques explicatives du choix de l'échantillon dans une première sous-section (1), ensuite nous allons détailler le mode de recueil des données dans la deuxième sous-section (2), expliciter dans une troisième sous-section le traitement des données (3), et présenter dans une dernière section les premiers enseignements empiriques (4).

L'architecture de la section est la suivante :


Choix de l'échantillon
Mode de recueil des données
Traitement des données
Les premiers enseignements empiriques

1. Choix de l'échantillon

Nous avons effectué deux vagues d'entretiens semi-directifs avec des objectifs différents. La première vague d'entretiens, dont l'objectif était d'explorer le processus de contrôle existant de l'espionnage industriel dans les organisations, est constituée d'un échantillon avec les caractéristiques suivantes :

- entreprises ou organisations ayant un système de contrôle de l'espionnage industriel (système d'intelligence économique, système de sécurité d'information, système de veille…) ;
- entreprises ou organisations ayant un contrôleur de gestion ou un service contrôle de gestion ;
- entreprises ou organisations ayant comme un des objectifs stratégiques « la protection ou la sécurité de l'information ».

Comme exemples, nous pouvons citer les entreprises ou organisations figurant dans l'annuaire des prestataires du SYNFIE (syndicat français de l'intelligence économique), les entreprises ou organisations du portail de l'IE (intelligence économique), etc.

Cet échantillon est large, car nous sommes dans le cadre d'une exploration du processus de contrôle de l'espionnage industriel dans les organisations. Par conséquent, élargir l'échantillon augmente les chances d'avoir plus de réponses.

A cet effet, nous avons contacté plus d'une centaine d'organisations et entreprises par divers moyens :

- par courrier ;
- par téléphone ;
- par mail ;
- par des contacts intermédiaires (indirects)…

Nous avons reçu plusieurs retours des organisations et entreprises sollicitées. Cependant, quatre personnes dans trois organisations différentes ont accepté de faire l'entretien semi-directif.

Les autres réponses étaient négatives, dont 98% des répondants pensaient que :

- leur organisation ne renferme pas des informations confidentielles ou secrètes ;

- leur activité dispose des barrières à l'entrée qui dissuaderaient les espions ;
- l'espionnage industriel ne touche pas leur secteur d'activité, ou domaine d'activité…

Le tableau ci-dessous contient le type d'entité et les fonctions des personnes interviewées de notre première vague d'entretiens. Nous avons assuré l'anonymat total[56] aux différentes personnes interviewées, par conséquent nous présentons uniquement le type d'entité et les fonctions des personnes interviewées.

Tableau 15 : Le type d'entité et les fonctions des personnes interviewées de la première vague d'entretiens

Type d'entité	Fonctions des personnes interviewées
Entreprise privée	Contrôleur de gestion d'un site industriel
Coopérative	Responsable financier et contrôle de gestion
Entreprise privée	Directeur d'un site industriel
Organisation publique	Directeur des Systèmes d'information et des télécommunications

[56] Voir l'annexe 2 (exemple d'une lettre de demande d'entretien du premier guide d'entretien).

Pour la deuxième vague d'entretiens, les caractéristiques de l'échantillon étaient beaucoup plus précises, car l'objectif de l'étude était d'évaluer, au travers des entretiens semi-directifs avec les contrôleurs de gestion professionnels et les spécialistes universitaires en contrôle de gestion, la pertinence du système construit et récolter les suggestions desdits experts, afin d'apporter les améliorations nécessaires.

Cet échantillon requiert un certain niveau d'expertise pour répondre convenablement aux questions techniques de l'étude. Pour se faire, nous avons employé les mêmes moyens pour contacter lesdits experts :

- par courrier ;
- par téléphone ;
- par mail ;
- par des contacts intermédiaires (indirects)…

Pour cette deuxième étude, nous avons choisi d'interviewer des personnes expertes, qui pouvaient émettre des suggestions probantes.

La deuxième vague d'entretiens est une étude plus approfondie, dans le sens où nous avons élaboré un système de contrôle de l'espionnage industriel. Il nous est apparu indispensable d'avoir les différents avis des experts dans le domaine.

Ainsi, le tableau ci-dessous contient le type d'entité et les fonctions des personnes interviewées de notre deuxième vague d'entretiens. Nous avons également assuré l'anonymat total[57] aux différentes personnes interviewées, par conséquent nous présentons uniquement le type d'entité et les fonctions des personnes interviewées.

[57] Voir l'annexe 3 (exemple d'une lettre de demande d'entretien du deuxième guide d'entretien).

Tableau 16 : Le type d'entité et les fonctions des personnes interviewées de la deuxième vague d'entretiens

Type d'entité	Fonctions des personnes interviewées
Entreprise privée	Contrôleur de gestion d'un site industriel
Université	Maître de conférences - HDR contrôle de gestion
Organisation publique	Responsable du service financier, budget et contrôle de gestion
Organisme dédié à la formation professionnelle et à la recherche	Professeur émérite - HDR comptabilité et contrôle de gestion
Entreprise privée	Directeur d'un site industriel
Université	Professeur - HDR comptabilité et contrôle de gestion

2. Mode de recueil des données

Les techniques de recueil des données sont nombreuses, nous pouvons citer celles proposées par Yin (1994) :

- la documentation ;
- les archives ;
- les entretiens ;
- l'observation directe ;
- l'observation participante ;
- la simulation.

Il est nécessaire de préciser que l'utilisation de plusieurs techniques dans une même recherche procure une importance (en qualité de validité) aux résultats obtenus. Yin (1994) a suggéré d'utiliser de multiples sources de données (comme moyen d'assurer la validité du construit).

Cela fait référence à la triangulation et la confrontation des données collectées, pour davantage enrichir les résultats de la recherche.

Néanmoins, la question de recherche, les possibilités du terrain et bien d'autres contraintes influencent le choix des méthodes de recueil des données.

Dans notre recherche, nous avons utilisé deux techniques parmi les six proposées par Yin (1994), il s'agit des analyses documentaires et des entretiens semi-directifs.

Nous avons collecté des données primaires et des données secondaires dans le cadre de cette recherche. Les différentes documentations ont constitué nos premières sources de données. Il s'agit notamment des informations disponibles sur internet, les sites des entreprises, les rapports nationaux, les rapports internationaux, etc.

Ces premières données ont permis de cibler les informations, dont nous avons besoin pour peaufiner notre recherche. Elles ont été un aperçu de ce que nous pouvons chercher dans les organisations.

Ces données primaires nous ont permis de retracer l'ossature de notre cadre de recherche, dans le sens où elles constituent une partie de la revue de littérature, notamment dans le premier chapitre (état de l'art de l'espionnage industriel). Elles ont aussi éclairé le chemin vers d'autres informations plus ciblées (les données secondaires).

Pour collecter ces données primaires, nous avons utilisé la fiche de lecture ci-dessous par document :

Tableau 17 : Fiche de lecture

Auteur / année de publication / discipline	
Question de recherche	
Thèses avancées	
Citations à utiliser	
Remarques personnelles	

Ensuite, nous avons utilisé des outils de collecte des données secondaires. Il s'agit principalement des entretiens semi-directifs.

Les entretiens semi-directifs ont été les principaux outils de collecte des données de cette recherche. En effet, nous avons effectué deux vagues d'entretiens, dont les objectifs étaient différents. Pour chaque vague d'entretiens, nous avons élaboré un guide d'entretien permettant de structurer notre intervention.

Tout entretien dans le cadre d'une recherche scientifique doit être préalablement élaboré, structuré et préparé par le chercheur. Cette structuration passe par l'établissement d'un guide d'entretien, qui permet au chercheur de bien mener son entretien.

Ce guide d'entretien est utilisé lors de l'entretien comme support, afin de conserver constamment sous les yeux les objectifs de l'entretien et de justifier le caractère scientifique de la recherche.

Il a un rôle de rappel des thématiques qui seront abordées lors des échanges, sans toutefois limiter les questions aux seules thématiques du guide.

Ainsi pour la première vague d'entretiens, le guide d'entretien était le suivant :

Figure f : Le premier guide d'entretien semi-directif

Guide d'entretien semi-directif

I. L'objectif de l'étude

L'étude a pour but d'appréhender le processus de contrôle de l'espionnage industriel dans les entreprises en France, à travers les grandes lignes ci-dessous.

Dans le cas échéant, si une telle structure n'est pas mise en place dans votre organisation, les différentes perceptions des professionnels comme vous, nous permettront de construire un modèle de contrôle de l'espionnage industriel.

Elle vise particulièrement à répondre à la question suivante : « pourquoi et comment contrôler l'espionnage industriel dans les entreprises en France ? ».

II. Thématiques de l'étude

A. L'existence d'une politique ou d'une stratégie de l'organisation vis-à-vis de l'espionnage industriel ou de protection / sécurisation de l'information ?
B. Les facteurs explicatifs de ce choix ?
C. Analyse du niveau d'implication des différentes fonctions de l'organisation (Finance, Comptabilité, Contrôle de Gestion, Marketing…)
D. La fonction contrôle de gestion contribue-t-elle au suivi de la protection de l'information ou de lutte contre l'espionnage industriel ?
E. Les outils et moyens du contrôle de gestion utilisés à cet effet
F. Les outils et méthodes de pilotage de l'espionnage industriel

1. Dimension planification
2. Dimension évaluation des coûts
3. Dimension comptabilisation et reporting
4. Autres dimensions

G. Les impacts de ce changement sur la fonction Contrôle de Gestion

Ce guide nous a permis de recueillir empiriquement certaines informations, qui ont été analysées dans l'objectif d'explorer un processus de contrôle de l'espionnage industriel dans les organisations[58].

Après cette première vague d'entretiens, nous avons obtenu des résultats qui ont permis de déterminer l'objectif ultime de cette recherche, à savoir l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Pour atteindre cet objectif, nous avons défini un modèle théorique de gestion de l'espionnage industriel par la fonction contrôle de gestion. Ce modèle nous a permis de déterminer les outils de notre système de contrôle de l'espionnage industriel.

Ensuite, nous avons effectué une deuxième vague d'entretiens avec l'objectif d'évaluer, au travers des entretiens semi-directifs avec les contrôleurs de gestion professionnels et les spécialistes universitaires en contrôle de gestion, la pertinence du système construit et récolter les suggestions desdits experts, afin d'apporter les améliorations nécessaires.

Pour effectuer cette deuxième vague d'entretiens, le guide d'entretien était le suivant :

[58] Les résultats de la première vague d'entretiens sont donnés dans les premiers enseignements empiriques.

Figure g : Le deuxième guide d'entretien semi-directif

Guide d'entretien semi-directif

I. L'objectif de l'étude

L'étude vise particulièrement à évaluer la pertinence du système construit et à récolter vos suggestions, afin d'apporter les améliorations nécessaires.

II. Thématiques et questions de l'étude

A. Selon vous, l'espionnage industriel est-il nuisible pour les entreprises ?
B. Pouvez-vous me citer quelques conséquences de l'espionnage industriel sur les entreprises ?
C. Pensez-vous que les entreprises ont un contrôle sur l'espionnage industriel ?
D. Est-il pertinent de mettre en place un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion ?
E. Examen de la capacité du système construit à contrôler l'espionnage industriel

1. Ce système permet-il de contrôler l'espionnage industriel ?
2. Quels sont les points à améliorer ?

F. Analyse de la pertinence des outils du système construit

1. Quelles sont vos impressions sur les aptitudes de contrôle des outils ?
2. Jugez-vous d'autres outils plus pertinents ? Si oui, lesquels ? Si non, pourquoi ?

G. Détermination des moyens indispensables à la réussite d'un tel système

Quels sont d'après vous les moyens indispensables à la réussite d'un tel système ?

1. Son accueil dans l'organisation ?
2. Les impacts sur les relations entre la fonction contrôle de gestion et les autres fonctions de l'entreprise ?
3. Selon vous, le système doit-il être intégré ou isolé ?
4. Autres moyens ?

Ces deux guides contiennent les thématiques, sur lesquelles les personnes interviewées ont développé leurs arguments. Ils servaient de référentiel pour structurer les échanges, mais aussi pour donner les grandes lignes préalablement aux personnes interviewées.

Pendant le recueil des données, des notes ont été prises et nous avons aussi eu l'autorisation d'enregistrer (en audio) les différents entretiens en entier. Ce qui a été d'une aide considérable, notamment lors du traitement des données.

3. Traitement des données

Pour le traitement des données, nous avons opté pour la technique d'analyse des données qualitatives la plus connue : l'analyse de contenu.

Bardin (2003)[59] définit l'analyse de contenu comme : « *un ensemble de techniques d'analyse des communications visant, par des procédures systématiques et objectives de descriptions du contenu des messages, à obtenir des indicateurs (quantitatifs ou non) permettant l'inférence de connaissances relatives aux conditions de production/réception (variables inférées) de ces messages* ».

Selon Gavard-Perret et al (2012), l'analyse de contenu se place historiquement au cœur des analyses qualitatives et semble trouver ses racines dans les analyses de presse, les analyses d'articles de propagande du début du XX^{ème} siècle. Son champ s'est élargi aux analyses de communications. Ces auteurs stipulent que l'analyse de contenu permet de répondre à de très nombreux objectifs.

Nous retenons les caractéristiques générales des méthodes d'analyse de contenu de Gavard-Perret (2012) pour analyser les données obtenues, il s'agit de :

- la préparation du corpus qui se décompose en :
  - une intervention sur le corpus ;
  - une indexation ;
- la démarche générale qui se subdivise en trois rubriques :
  - la préanalyse ;
  - l'exploitation du matériel ;
  - le traitement des résultats, l'inférence et l'interprétation.

[59] Gavard-Perret *et al.* (2012). *Méthodologie de la recherche en sciences de gestion : Réussir son mémoire ou sa thèse*. Pearson Education France, p.252.

La préparation du corpus :

Après la collecte des données, nous avons effectué une intervention sur le corpus et une indexation sur les différentes données recueillies.

- **L'intervention sur le corpus :**

Les données ont été enregistrées lors des entretiens et le premier travail d'analyse a été un exercice de transcription des données brutes avec certains traitements. Il s'agit principalement des petites corrections sémantiques, orthographiques et grammaticales.

Cette transcription a été effectuée tout en respectant l'ordre des thématiques sur le guide d'entretien. C'était principalement un passage de l'oral à l'écrit avec quelques petits traitements.

- **L'indexation :**

A ce niveau, le travail consistait à structurer et à faciliter la recherche d'un document, d'une donnée quelconque dans les différentes transcriptions. Il s'agit d'indexer, d'étiqueter, de numéroter chaque document. Une transcription par entretien a été effectuée et suivant les thématiques du guide d'entretien, afin de faciliter la comparaison entre les différentes données collectées. Cette indexation permet de visualiser indépendamment les différentes données.

La démarche générale d'analyse de contenu :

Après la préparation du corpus, nous avons suivi les trois phases d'une démarche générale d'analyse de contenu commençant par la préanalyse, ensuite l'exploitation du matériel et le traitement des résultats, l'inférence et l'interprétation.

- **La préanalyse :**

Cette étape a été importante, car elle nous a permis de catégoriser les différentes données collectées, et nous avons défini les règles de découpage du corpus transcrit.

Après lecture des écrits transcrits, nous avons choisi de relever les affirmations communes aux personnes interviewées, c'est-à-dire les points pertinents (par rapport aux thématiques du guide d'entretien) sur lesquels les personnes interviewées avaient une convergence et ou une divergence.

- **L'exploitation du matériel :**

L'exploitation du matériel consiste en une application des règles définies dans la préanalyse, afin de clarifier les points pertinents. A ce stade, nous avons relevé les points pertinents, qui répondent à l'objectif de l'étude.

Ainsi, nous avons identifié les éléments pertinents (convergents et ou divergents) de chaque transcription et nous avons extrait les résultats.

- **Le traitement des résultats, inférence et interprétation :**

Habituellement des traitements statistiques (des simples calculs de fréquences, des analyses factorielles, des graphes, etc.) s'effectuent à ce niveau, par contre nous avons agi manuellement et intellectuellement pour interpréter les différents résultats.

Nous avons effectué un travail de synthèse, à l'instar de Gavard-Perret *et al.* (2012) : « *elle repose sur la réduction des données de manière à exprimer uniquement les idées ou thématiques principales* ».

Nous avons relevé les éléments pertinents selon l'objectif de l'étude et nous avons établi un tableau avec les résultats[60]. Les résultats sont présentés et interprétés dans les parties citées en bas de page.

4. Premiers enseignements empiriques d'une démarche hypothético-inductive

Les premiers enseignements du terrain ont été d'une importance considérable pour cette recherche, car ils ont été l'élément déclencheur d'une redirection vers l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

La dernière rubrique méthodologique d'une recherche scientifique est l'interprétation des résultats. Cette interprétation nécessite l'aptitude du chercheur à détecter les résultats les plus révélateurs.

Les premiers travaux empiriques effectués avaient pour objectif d'appréhender le processus de contrôle existant de l'espionnage industriel dans les organisations. Ces entretiens ont révélé des résultats qui nous alarmaient à ce que nous changions d'angle d'attaque.

[60] Les tableaux des résultats sont dans les premiers enseignements empiriques pour la première vague d'entretiens (sous-section suivante), et dans le chapitre 5 pour la deuxième vague d'entretiens.

Le tableau ci-dessous est une présentation succincte des résultats des différents entretiens menés dans le cadre de la première vague d'entretiens :

Tableau 18 : Les premiers enseignements empiriques

	Objectif de l'étude	Personnes interviewées	Résultats de l'étude
1ère Vague d'entretiens	Appréhender le processus de contrôle existant de l'espionnage industriel dans les organisations	- Directeur des Systèmes d'information et des télécommunications - Responsable financier et contrôle de gestion - Directeur d'un site industriel - Contrôleur de gestion d'un site industriel	• Sujet important et pertinent • La présence d'une volonté de lutter contre l'espionnage industriel • L'absence d'un objectif stratégique prédéfini de lutte contre l'espionnage industriel • L'existence des méthodes et bonnes pratiques pour optimiser la protection sans une concrète formalisation • L'absence d'un pilotage des moyens et méthodes de protection contre l'espionnage industriel

Les résultats de cette étude montrent bien l'absence d'un processus de contrôle de l'espionnage industriel dans lesdites organisations, même si certains efforts ont été effectués pour canaliser le phénomène. Nous ne prenons guère le risque de généraliser ces résultats, car nous ne pouvons effectuer un sondage exhaustif.

Cependant, ces quelques entretiens menés dans les formes nous ont permis d'avoir un petit aperçu de l'appréhension du phénomène dans certaines organisations. D'un autre côté, ces résultats constituent des données concrètes, qui corroborent certaines affirmations d'autres études. Il s'agit notamment des données issues des rapports nationaux, rapports internationaux, des études scientifiques, etc.

Avec cet esprit de triangulation, à l'instar de Yin (1994), certaines affirmations ont pu être vérifiées au travers des différents documents ci-dessous :

- Rapport Martre (1994) ;
- Rapport Carayon (2003) ;
- Rapport de la Commission du droit de l'entreprise et avec la collaboration de l'Institut de Recherche en Propriété Intellectuelle (2014) ;
- Etude de Ponemon (2009).

Nous pouvons citer l'exemple du rapport de la Commission du droit de l'entreprise et avec la collaboration de l'Institut de Recherche en Propriété Intellectuelle (2014), qui stipulait que les entreprises sous-estiment majoritairement l'espionnage industriel et pensent qu'elles ne sont pas des éventuelles cibles des espions. Cette affirmation du rapport est démontrée avec les motifs de refus des 98% des répondants de la première vague d'entretiens[61].

Nous avons remarqué que certains résultats de notre étude corroborent d'autres données des rapports nationaux, des rapports internationaux, des études scientifiques, etc.

[61] Ces motifs se trouvent dans le choix de l'échantillon plus haut dans la même section.

Conclusion du chapitre 3

L'objectif de ce chapitre était de présenter notre démarche de recherche dans son ensemble, à savoir la méthodologie de recherche adoptée, notre posture épistémologique, le choix de l'échantillon, le mode de collecte des données, le traitement des données jusqu'à la présentation des résultats de recherche.

Ainsi, notre recherche s'inscrit dans une démarche qualitative, car les données à recueillir sont des informations et des données non numériques (des mots) des acteurs ou des documents étudiés. L'interprétativisme est la posture épistémologique de notre recherche.

Pour la construction des connaissances, nous avons opté pour une approche hypothético-inductive se traduisant par des allers et retours entre le terrain et la littérature théorique. L'objectif ultime étant d'évaluer le système de contrôle construit de l'espionnage industriel par la fonction contrôle de gestion.

Ces différents choix s'articulent bien avec notre objet de recherche. En fonction du sujet et du type de données, nous avons défini les caractéristiques de notre échantillon. L'entretien (étant la technique favorite de collecte des données qualitatives) et la documentation nous ont permis de collecter des données, qui ont ensuite été analysées et traitées par la méthode d'analyse de contenu.

L'espionnage industriel est un sujet occulte, par conséquent les informations et données qui touchent ce phénomène sont difficilement accessibles. Cela peut être une source d'explication de la réticence des entreprises à accepter l'accueil d'un chercheur traitant le sujet. D'autant plus que notre sujet est sensible et novateur.

Nous rappelons que l'objectif de la première vague d'entretiens était d'explorer le processus de contrôle de l'espionnage industriel dans les organisations.

Suite aux premiers enseignements du terrain, l'objectif de la recherche s'est redirigé vers l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, car les résultats ont révélé l'absence d'un outil d'évaluation des coûts de l'espionnage industriel, l'absence d'un pilotage des outils et moyens de protection contre l'espionnage industriel dans les entreprises, etc.

A cet effet, la fonction contrôle de gestion est apparue comme une alternative pouvant combler ces trous de gestion. Par conséquent, nous avons défini un modèle théorique de

gestion de l'espionnage industriel par la fonction contrôle de gestion[62]. Ce modèle théorique a permis de déterminer des outils qui constituent le système de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Le chapitre suivant explicite les étapes d'élaboration dudit système de contrôle.

[62] Le modèle théorique a été présenté dans le deuxième chapitre.

Chapitre 4 : Les étapes d'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion

Les premiers travaux empiriques effectués avaient pour objectif d'appréhender le processus de contrôle existant de l'espionnage industriel dans les organisations. Nos premiers entretiens ont révélé des résultats, qui nous alarmaient à ce que nous changions d'angle d'attaque. Des rapports avaient noté que les organisations, par méconnaissance ou par ignorance, n'accordaient pas d'intérêt à l'espionnage industriel. Par conséquent, certaines ne voient pas l'utilité de mettre en œuvre un processus de contrôle. Elles semblent sous-estimer majoritairement le problème et ne pensent pas être concernées, or ces rapports internationaux, nationaux et autres études montrent que tout type d'organisation peut être victime d'espionnage industriel, du moment où la structure a des informations qui intéressent les espions.

Les résultats des premiers travaux empiriques ont, certes, révélé des points intéressants et corroboré certaines affirmations, mais ils ne répondent pas totalement à notre question de recherche.

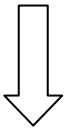
Il y a, certes, des méthodes de prévention mises en place, mais nous n'avons pas pu découvrir la façon dont la fonction contrôle de gestion appréhende l'espionnage industriel dans les organisations.

Cependant, ces résultats ont été des pistes intéressantes qui ouvrent des portes d'exploration à d'autres horizons.
Pour répondre à notre question de recherche, nous avons opté pour l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Ensuite nous allons évaluer empiriquement la pertinence dudit système auprès des spécialistes du contrôle de gestion des universités et des contrôleurs de gestion professionnels des organisations.

Pour ce faire, nous allons détailler les étapes d'élaboration dudit système dans les deux sections suivantes : la première section fera l'objet d'une détermination des outils de contrôle de l'espionnage industriel du système de contrôle diagnostic, dans le but de cerner les figures imposées ; et la deuxième section sera consacrée à l'étude des outils du levier de contrôle interactif, afin d'encadrer les figures libres du processus de contrôle de l'espionnage industriel.

L’architecture du chapitre ci-dessous récapitule les différentes étapes de construction de notre système de contrôle de l’espionnage industriel par la fonction contrôle de gestion :

Section 1 **Système de contrôle diagnostic : détermination des méthodes et outils de contrôle de l'espionnage industriel**		
Méthodes et outils de base du contrôle de gestion	Réajustement des outils et méthodes de base du contrôle de gestion	Autres méthodes et outils : méthodes des coûts cachés



Section 2 **Système de contrôle interactif : détermination des méthodes et outils de contrôle de l'espionnage industriel**	
Méthodes et outils du système de contrôle interactif	Des outils du levier de contrôle interactif cernant l’espionnage industriel

Section 1 : Détermination des outils du levier de contrôle diagnostic

Le système de contrôle diagnostic consiste à s'assurer de la conformité des actions et résultats, au travers d'une définition des variables critiques de performance. Pour Simons et bien d'autres auteurs, ce levier de contrôle diagnostic s'apparente au contrôle de gestion classique. Ses outils et méthodes, qui ont pour vocation de cerner les figures imposées, correspondent à ceux du contrôle de gestion classique.

Pour Simons (1994), on distingue un système de contrôle diagnostic selon trois caractéristiques :

- *la capacité à fixer des objectifs ou des standards de performance ;*
- *la capacité à mesurer les résultats d'un processus ;*
- *la capacité à corriger les déviations par rapport aux standards de performance*.

Or, ces caractéristiques renvoient aux aptitudes du contrôle de gestion classique. Par conséquent, les outils et méthodes du système de contrôle diagnostic sont les outils et méthodes du contrôle de gestion classique.

Par ailleurs, nous savons que le contrôle de gestion est une discipline, qui demande une adaptation permanente de ses outils et méthodes à l'environnement tant interne qu'externe de l'organisation. De ce fait, il existe plusieurs outils et méthodes du contrôle de gestion, qui ne peuvent être traités exhaustivement dans notre étude.

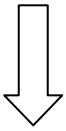
Dans cette optique, nous nous intéresserons uniquement aux outils de base du contrôle de gestion dans le cadre de notre recherche, et nous aurons recours à d'autres outils éventuellement pour une meilleure appréhension de l'espionnage industriel.

Cette section se décompose en trois sous-sections, il s'agit :

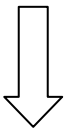
- dans un premier temps, de sélectionner les méthodes et outils de base (ou traditionnels) du contrôle de gestion ;
- ensuite, de les adapter ou les ajuster à ce qu'ils puissent permettre d'appréhender le contrôle de l'espionnage industriel ;
- et de déterminer d'autres outils, notamment les méthodes des coûts cachés.

L'architecture de la section est la suivante :

Les méthodes et outils de base du contrôle de gestion			
La structuration en centres de responsabilité	Les budgets et le contrôle budgétaire	Les tableaux de bord	La comptabilité de gestion



Réajustement des outils et méthodes de base du contrôle de gestion			
Réajustement de la structuration en centres de responsabilité	Réajustement des budgets et du contrôle budgétaire	Un tableau de bord adapté au contrôle de l'espionnage industriel	Réajustement de la comptabilité de gestion



Autres méthodes et outils : méthodes des coûts cachés		
Sources des coûts cachés	Méthodes d'évaluation des coûts cachés	Méthodes d'évaluation des coûts invisibles de l'espionnage industriel

1. Méthodes et outils de base du contrôle de gestion

La phrase introductive de Berland et Simon (2011) résume assez bien le contrôle de gestion actuel : « *le contrôle de gestion est en effet un ensemble de pratiques paradoxales qui ne saurait se limiter à des outils ou à une profession au risque d'en présenter une vision trop caricaturale qui ne permet pas d'en saisir la richesse et le potentiel* »[63].

Les méthodes et outils du contrôle de gestion sont nombreux et se diversifient au fur et à mesure que l'environnement de l'organisation en exige.

Chiapello (1996) définit : « *les outils du contrôle de gestion (plans, budgets, contrôle budgétaire, tableaux de bord) comme des instruments utilisés par les managers afin de mettre sous contrôle les activités des entreprises. Mais ils ne sont assurément pas les seuls moyens disponibles* […] ».

En analysant cette définition, nous pouvons relever la multiplicité des outils du contrôle de gestion et noter que ce ne sont certainement pas des outils immuables. Ce qui écarte toute intention de requérir l'exhaustivité des méthodes et outils à utiliser.

Nous pouvons aussi évoquer le fait que les objectifs à atteindre des différentes organisations privées et publiques soient différents. Le service public recherche la satisfaction de la population et priorise la qualité de service, tandis que les organisations privées cherchent non seulement à satisfaire les clients, mais à optimiser les coûts de revient, tout en cherchant à dégager un bénéfice.

Par conséquent, les objectifs diffèrent selon les spécificités des organisations. Des auteurs comme Alcouffe *et al.* (2013) mentionnent la nécessité d'adapter les méthodes et outils du contrôle de gestion aux spécificités des différentes organisations (industrie, grande distribution, banque, secteur public, culture…)[64].

Ces mêmes auteurs soutiennent qu'un « contrôle de gestion sur mesure »[65] est plus adapté au pilotage de la performance des organisations. Par ailleurs, ils présentent quatre dispositifs et outils de contrôle qui servent au pilotage d'une performance multidimensionnelle, à savoir :

---

[63] Berland, N., & Simon, F. X. (2011). *Le contrôle de gestion en mouvement: Etat de l'art et meilleures pratiques-Regards croisés de professeurs et praticiens*. Editions Eyrolles.

[64] Alcouffe, S., Boitier, M., Rivière, A., & Villesèque-Dubus, F. (2013). *Contrôle de gestion sur mesure: Industrie, grande distribution, banque, secteur public, culture*. Dunod.

[65] Termes utilisés pour le titre de leur ouvrage.

- la comptabilité de gestion ;
- les budgets ;
- les tableaux de bord ;
- la structuration en centres de responsabilité.

Cependant, recourir aux méthodes et outils traditionnels du contrôle de gestion pourrait permettre d'appréhender scientifiquement le processus de contrôle de l'espionnage industriel. Par méthodes et outils traditionnels du contrôle de gestion, nous voulons signifier par là les plus fondamentaux et les plus utilisés.

On peut donc se poser la question, pourquoi partir des méthodes et outils du contrôle de gestion traditionnel ? D'autant plus que ces outils semblent obsolètes selon certains auteurs, comme Lorino (1991)[66].

Ces critiques sont indéniablement pertinentes, car les méthodes et outils du contrôle de gestion connaissent énormément de mutations à cause de l'environnement des organisations. Ils sont, par conséquent, adaptés et réajustés en permanence. De plus, de nouveaux outils et méthodes se créent pour une meilleure gestion.

Nonobstant, ces nouveautés, réadaptations et réajustements sont souvent inspirés des outils du contrôle de gestion traditionnel qui sont le point de départ. L'exemple de la méthode ABC (Activity-Based Costing) est une bonne illustration, car elle est inspirée de la méthode des coûts complets.

Cependant, même énumérer des outils du contrôle de gestion comme les « outils traditionnels » pose des problèmes pour diverses raisons. Berland (2014)[67], dans son approche technique de la discipline, a émis les hypothèses suivantes pour la description du contrôle de gestion au travers de ses outils les plus traditionnels :

> - *Nous adoptons alors une perspective technicienne sans véritable cohérence d'ensemble. Le contrôle se résume à un ensemble de pratiques que l'on ne sait ordonner les unes par rapport aux autres.*

[66] Lorino, P. (1991). *Le contrôle de gestion stratégique: la gestion par les activités* (Vol. 213). Paris: Dunod.
[67] Berland, N. (2014). *Le contrôle de gestion : «Que sais-je?» n° 3977*. Presses universitaires de France.

- *La diversité des pratiques du contrôle de gestion n'est en outre pas immuable. De nouveaux outils apparaissent régulièrement. Le contrôleur de gestion s'en saisit comme par exemple pour les outils de la création de valeur. La liste des outils du contrôle n'est donc pas définie de façon fermée.*
- *En outre, les outils du contrôle de gestion sont implicitement ceux utilisés par le contrôleur de gestion ou ceux présentés dans les ouvrages de contrôle de gestion. Mais le contrôle de gestion, en tant que processus, peut utiliser des outils, comme la gestion de la qualité, qui ne sont pas des outils du contrôleur.*

Ces précisions hypothétiques ont le mérite de donner un cadre ou un périmètre de délimitation aux outils du contrôle de gestion. Cela permet de caractériser la discipline, au travers de ses outils, sans pour autant fermer les portes de toute éventuelle évolution aussi bien de ladite discipline que de ses outils.

Il énumère ainsi les outils suivants, comme les plus traditionnels du contrôle de gestion :

- la définition des centres de responsabilité ;
- la comptabilité de gestion (il évoque des méthodes comme la méthode des coûts complets, les prix de cession internes…) ;
- le budget (et le contrôle budgétaire) ;
- les tableaux de bord.

D'autres auteurs comme Gervais (2009), Grandguillot (2013) et tant d'autres parlent de tableaux de bord, de budgets (et contrôle budgétaire), de comptabilité de gestion (en faisant référence aux écarts, prix de cession internes…) comme des outils inhérents au contrôle de gestion.

Nous pouvons donc considérer ces différents outils parmi les plus fondamentaux et les plus basiques du contrôle de gestion.

En somme, le contrôle de gestion a et ne cesse d'avoir des outils permettant d'atteindre les finalités de la fonction. Ces outils sont aussi bien nombreux que multidisciplinaires, dans le sens où la fonction contrôle de gestion utilise des outils provenant d'autres disciplines.

C'est une fonction, qui s'adapte en permanence à son environnement interne et externe, ce qui écarte toute intention d'affirmer l'efficacité pérenne d'un outil dépourvu de modernité et de perspective dynamique.

Dans un objectif de simplicité, d'avoir des points de repère dans la discipline du contrôle de gestion, et même dans les enseignements magistraux des universités et écoles, les auteurs sont quasiment unanimes sur les outils suivants, comme les plus fondamentaux du contrôle de gestion :

- La structuration en centres de responsabilité ;
- Les budgets (et le contrôle budgétaire) ;
- Les tableaux de bord ;
- La comptabilité de gestion (les méthodes de calcul des coûts, dont la méthode des coûts complets demeure la plus répandue et utilisée).

Nous retiendrons ces 4 éléments comme les plus fondamentaux et nous spécifions tout de même que cet effectif n'est en aucun cas une exhaustivité en soi.

Par ailleurs, des auteurs comme Berland, Burlaud, Simon, Gervais, Chiapello, Lorino et tant d'autres énumèrent au moins ces 4 outils propres au contrôle de gestion traditionnel. Ces outils sont aussi enseignés dans toutes les universités et écoles (dans la discipline contrôle de gestion)[68]. Pour corroborer notre choix, les professionnels du contrôle de gestion (organisations privées et publiques) utilisent aussi ces types d'outils.

Dans le cadre théorique du processus de contrôle de l'espionnage industriel, nous avons évoqué l'incapacité de ces méthodes et outils de base du contrôle de gestion à appréhender l'espionnage industriel dans les organisations (l'espionnage industriel est un phénomène hors marché, ce qui échappe aux aptitudes de perception des outils traditionnels). Cependant, nous allons les définir et les caractériser, pour ensuite les réadapter à la perception de l'espionnage industriel.

[68] Si l'on se réfère aux contenus des nombreux manuels destinés au public académique et aux professionnels des organisations.

A. La structuration en centres de responsabilité

Les centres de responsabilité constituent des véritables méthodes et outils de clarification du contrôle de gestion dans les organisations. Ils consistent en une décentralisation maîtrisée du pouvoir pour une meilleure gestion.

Giraud (2011) définit un centre de responsabilité, comme : « *une entité de la structure que les dirigeants d'un groupe ont placée sous l'autorité d'un manager, à qui ils ont délégué un pouvoir de décision et qui doit rendre compte d'un objectif de contribution aux résultats d'ensemble »*[69]. L'auteur précise que la responsabilité englobe un pouvoir de décision assez large et l'existence d'une marge de manœuvre assez importante.

Burlaud et Simon (2013)[70] quant à eux, définissent un centre de responsabilité comme : *« une entité dotée d'une délégation de pouvoir et soumise à des objectifs contrôlés par un reporting spécifique »*.

Il s'agit d'inculquer des comportements proactifs aux employés des entités. Ces définitions sous-entendent un découpage de l'organisation en entités, afin de responsabiliser ces dernières, en leur accordant les moyens nécessaires à l'atteinte des objectifs préétablis. Ces centres de responsabilité sont intéressants dans le sens où ils constituent un moyen concret pour ses managers de montrer leurs aptitudes au travers des résultats.

Ils demeurent également un moyen de contrôle pour le groupe, qui reçoit un reporting de chaque entité et peut ainsi converger les différentes entités vers les objectifs souhaités. En somme, le groupe garde le contrôle sur ses entités, en leur octroyant une certaine autonomie et leur permet simultanément de s'épanouir en montrant leurs capacités de gestion au travers des résultats.

Cependant le concept de centre de responsabilité a des limites, comme :

- peut-on parler de centres de responsabilité pour les petites organisations ? Les explications ci-dessus concernent, *à priori*, une organisation de grande taille, c'est-à-dire ayant un effectif assez élevé et une structure assez complexe. Qu'en est-il d'une organisation de petite taille ?

[69] Giraud, F. (2011). *Les fondamentaux du contrôle de gestion : principes et outils*. Pearson, p24.
[70] Burlaud, A. & Simon, C. (2013). *Le contrôle de gestion*. 3ème édition. La Découverte, p45.

- Lorino *et al.* (2013) évoquent la nécessité *de concilier décentralisation et cohérence collective*, pour éviter une distanciation inutile des performances entre les centres de responsabilité. Ceux-ci étant liés et interdépendants, ils doivent avancer au même rythme pour une meilleure performance collective (un centre de responsabilité qui engendre des performances supérieures à celles des autres centres ne constitue pas une bonne cohérence et peut nuire à l'organisation).

Pour une meilleure cohérence, Lorino *et al.* (2013) distinguent deux types de contrats[71], à savoir :

- Les contrats « *objectifs-moyens* » (contrats verticaux) : passés entre différents niveaux hiérarchiques, ils spécifient les finalités à atteindre accompagnées des moyens et d'une analyse des actions permettant l'atteinte desdites finalités ;
- Les contrats « *client-fournisseur* » (contrats horizontaux) : passés entre un service prestataire interne et un autre service (absence de lien hiérarchique), c'est un échange de biens ou de service (généralement rémunéré) obéissant à différents critères de coût, délai, qualité, etc.

Les prix de cession internes sont nés de la valorisation des échanges entre les centres de responsabilité. Par ailleurs, quelques problèmes demeurent toujours et nécessitent une bonne entente entre les responsables des différents centres de responsabilité. Parmi ces problèmes, Lorino *et al.* (2013) mentionnent :

- le problème de l'optimisation globale ;
- le problème de motivations individuelles des différents responsables des centres de responsabilité ;
- une gestion purement financière ;
- un risque de cloisonnement entre centres de responsabilité…

Nous pouvons en déduire que la technique des centres de responsabilité est un outil ayant aussi bien des bonnes vertus de gestion que des limites à reconsidérer. Cependant, comment les centres de responsabilité de l'organisation peuvent-ils permettre d'appréhender l'espionnage industriel ?[72]

[71] Lorino, P., Demeestère, R., & Mottis, N. (2013). Pilotage de l'entreprise et contrôle de gestion. *5ème édition, Dunod*, p142.

[72] Cette question sera répondue dans la section suivante (précisément dans le réajustement de la structuration en

B. Les budgets et le contrôle budgétaire

Les budgets et le contrôle budgétaire, appelés aussi système budgétaire selon Gervais (2009)[73], sont des outils de planification des activités opérationnelles des organisations et de pilotage, au travers d'une comparaison entre le réel et le budgété. Ce sont des outils importants du contrôle de gestion à base de chiffres.

Les budgets sont des outils, qui spécifient à court terme toutes les éventuelles charges et tous les produits escomptés d'une organisation. Ils permettent donc d'anticiper la performance des organisations, au travers de ses différents composants (budget des ventes, budget de la production, budget des approvisionnements[74]…).

La construction des différents budgets aboutit à la mise en place des documents de synthèse (compte de résultat prévisionnel, bilan prévisionnel…), sous contraintes de certains facteurs, comme les moyens de production, les capacités de ventes… Ils constituent, de ce fait, des outils pertinents de la gestion déclinant les objectifs stratégiques de l'organisation en plans opérationnels.

Les différents budgets, étant interdépendants, doivent être bien construits[75] pour éviter un écart trop important entre le budgété et le réel. D'où l'intérêt du contrôle budgétaire qui consiste à confronter le réel au budgété pour des raisons spécifiques, comme :

- voir la pertinence des budgets en cas d'écart trop important ;
- cerner les origines des écarts dans l'objectif de les corriger ;
- voir les performances des différents centres de responsabilité…

Cependant, le système budgétaire a des limites qui nécessitent d'être prises en compte. Burlaud et Simon (2013) évoquent sa lourdeur et les rivalités internes, qu'il peut occasionner dans une organisation. Les centres de responsabilité lancés dans l'optimisation de leurs performances peuvent croire à une course aux trésors, et ainsi considérer les autres centres comme des rivaux.

---

centres de responsabilité).

[73] Un système budgétaire est un système de gestion prévisionnelle à court terme, comprenant des budgets et un processus de contrôle de gestion. Gervais, M. (2009). *Contrôle de gestion*, 9ème édition, Economica, p353.

[74] Voir Grandguillot, B. (2013). *L'essentiel du contrôle de gestion 2013*. Gualino éditeur ; et Augé, B., & Naro, G. (2011). *Mini manuel de contrôle de gestion*. Dunod.

[75] Voir les principes de base du système budgétaire de Gervais, M. (2009). *Contrôle de gestion*, 9ème édition, Economica, p355.

Sachant que le but n'est en aucun cas de mettre les centres de responsabilité en conflit, les rivalités peuvent s'avérer néfastes pour l'organisation. S'ajoute à ces limites son inaptitude à ne mesurer qu'une partie des performances de l'organisation : « *celles que traduisent les données monétaires et comptables, c'est-à-dire les flux immédiats au détriment des actions dont les retombées sont plus lointaines (qualité, formation du personnel et d'une façon générale l'ensemble des éléments immatériels favorables), à terme, à la pérennité et au développement de l'entreprise*[76] ». A cette limite, nous pouvons associer son incapacité à appréhender l'espionnage industriel, d'où l'intérêt d'une réadaptation ou un réajustement pour résoudre le problème.

C. Les tableaux de bord

Le concept des tableaux de bord ne cesse de s'adapter à de nombreuses mutations de l'environnement des organisations. De ce fait, de multiples modèles de tableaux de bord ont été mis en place pour une meilleure adaptation des outils de gestion aux fluctuations permanentes de l'environnement des organisations.

Parmi ces modèles, nous pouvons citer en plus du tableau de bord de gestion, la méthode OVAR (objectifs, variables d'action et responsabilités), les Balanced Scorecards ou tableaux de bord prospectifs, la méthode ORAA (objectifs récurrents et axes d'action)…

Selon Gervais (2009), le tableau de bord de gestion correspond *: « à un système d'information permettant de connaître le plus rapidement possible les données indispensables pour contrôler la marche de l'entreprise à court terme et faciliter dans celle-ci l'exercice des responsabilités ».*

D'autres auteurs comme Giraud, Zarloswki et al. (2011) définissent le tableau de bord, comme : « *un ensemble d'indicateurs à caractère non exclusivement financier (KPI : key performance indicators). Il peut prendre des formes très variées, mais se présente de façon générique sous la forme d'une liste d'indicateurs avec différentes valeurs prises par ces indicateurs ».*

Le tableau de bord est un outil, qui alerte le contrôleur de gestion sur les différents éloignements des opérations courantes des objectifs à atteindre. Les deux définitions ci-dessus montrent qu'il peut contenir aussi bien des indicateurs financiers que des indicateurs non

[76] Burlaud, A. & Simon, C. (2013). *Le contrôle de gestion*. 3ème édition. La Découverte, p43.

financiers, ce qui lui octroie une très bonne qualité d'appréhension de plusieurs catégories de variables.

Tant que l'environnement des organisations subit des changements permanents, les dimensions d'appréhension des tableaux de bord ne cesseront de s'élargir. La naissance de la méthode OVAR ou des Balanced Scorecards en est une parfaite illustration.

Ce sont des outils qui peuvent être adaptés à la taille de l'organisation, mais aussi aux types d'organisations (organisations privées ou publiques, organisations industrielles ou de prestations de service, etc.). Les tableaux de bord se construisent de diverses manières[77], mais ont en commun cet objectif d'alerte des managers, afin d'apporter rapidement des actions correctives.

Comme limite, Giraud, Zarloswki et al. (2011) évoquent l'importance (quantité trop élevée) du nombre d'informations quantitatives dans les systèmes d'information, pouvant empêcher une analyse adéquate. Un tableau de bord, contenant beaucoup d'informations, risque de désorienter au lieu d'orienter les managers.

Cependant, on peut s'interroger comme suit : comment les tableaux de bord de gestion peuvent contribuer au processus de contrôle de l'espionnage industriel dans les organisations ?

D. La comptabilité de gestion

La comptabilité de gestion est un outil important, voire indispensable, pour le contrôleur de gestion. Le contrôle de gestion, avant son évolution actuelle, était principalement appréhendé par ce postulat comptable. Au fil du temps, des grandes figures, comme Anthony, Simons et bien d'autres, ont donné un cadre plus élargi au contrôle de gestion, incluant aussi bien des dimensions techniques que des dimensions organisationnelles.

Cependant, le contrôle de gestion ne peut plus être réduit uniquement à ce titre comptable, qui constitue néanmoins un de ses outils fondamentaux.

[77] Pour la construction des différents types de tableaux de bord, voir Augé, B., & Naro, G. (2011). *Mini manuel de contrôle de gestion*. Dunod ; Gervais, M. (2009). *Contrôle de gestion*, 9ème édition, Economica ; Et Giraud, F. (2011). *Les fondamentaux du contrôle de gestion: principes et outils*. Pearson.

Le contrôle de gestion fait intervenir la comptabilité de gestion principalement pour[78] :

- *le calcul de coûts pour l'analyse stratégique ;*
- *l'analyse de coûts pour le pilotage de l'organisation.*

Pour Berland et De Rongé (2013), la comptabilité de gestion remplit trois fonctions[79] :

- *fournir de l'information utile :*
  - *à la mesure et à l'amélioration de la productivité et de l'efficience opérationnelle de l'organisation ;*
  - *à l'orientation du comportement ;*
- *calculer la rentabilité des produits, clients, canaux de distribution d'une entreprise et éventuellement agir dessus en modifiant le prix de vente ou en réduisant les coûts ;*
- *aider à prendre des décisions spécifiques et ponctuelles, par exemple évaluer une décision d'investissement ou d'externalisation, accepter ou non une baisse de prix, lancer ou non une action promotionnelle, etc*.

Le concept de coût est un élément fondamental au cœur de la fonction contrôle de gestion. Maîtriser les coûts (en les réduisant le plus possible tout en conservant l'avantage compétitif) fait partie intégrante des finalités de la fonction. Les arguments du contrôleur de gestion sont essentiellement adossés sur cette notion de coût.

Selon De Rongé et Cerrada (2012)[80], deux définitions du coût sont régulièrement données dans les systèmes de contrôle de gestion, à savoir :

- le coût tel que défini par les comptables ;
- le coût d'opportunité utilisé par les économistes.

Ils définissent le coût, dans l'optique comptable, comme : « *tout regroupement de charges comptables qu'il est pertinent d'opérer pour informer une prise de décision dans l'entreprise ou pour assurer le contrôle d'une partie ou de l'ensemble de l'organisation* ».

[78] De Rongé, Y., & Cerrada, K. (2012). *Contrôle de gestion*. Pearson Education France.
[79] Berland, N., & De Rongé, Y. (2013). *Contrôle de gestion: Perspectives stratégiques et managériales*. Pearson Education France, p152.
[80] De Rongé, Y., & Cerrada, K. (2012). *Contrôle de gestion*. Pearson Education France, p2.

Selon le plan comptable général français de 1982 (PCG 1982), le coût se définit comme : « *une somme de charges relatives à un élément défini au sein du réseau comptable* ». Ils définissent la notion de coût d'opportunité (développée par la théorie économique) comme : « *étant le revenu provenant de la meilleure utilisation alternative possible d'une ressource ou d'un facteur rare, auquel on renonce en affectant cette ressource ou ce facteur à un usage précis* ».

Berland et De Rongé (2013) affirment que le calcul de coûts (appelé également comptabilité de gestion ou comptabilité analytique) a pour vocation de fournir tous les éléments d'information possibles de nature à éclairer la prise de décision et à mesurer la performance de l'organisation et de ses sous-parties[81]. La comptabilité de gestion englobe de nombreuses méthodes de calcul de coûts, qui interviennent spécifiquement dans :

- la fixation des prix des produits ou du service ;
- l'analyse des écarts ;
- la détermination des coûts pour faciliter la prise de décision ;
- l'aide à la définition et à la mise en œuvre de la stratégie ;
- l'établissement des prévisions de charges et de produits…

Parmi les méthodes de calcul de coûts, nous pouvons citer : la méthode classique des coûts complets, la méthode des coûts partiels, la méthode ABC, direct costing[82]…

En somme, la comptabilité de gestion intervient de plusieurs manières dans la fonction contrôle de gestion et reste un de ses outils les plus utilisés et les plus fondamentaux. Cependant, c'est un outil qui a tout de même des limites, parmi lesquelles nous pouvons citer son inaptitude à évaluer certains phénomènes impactant les organisations. Ce qui soulève la question de savoir, si cet outil permet d'appréhender les coûts de l'espionnage industriel ?

[81] Berland, N., & De Rongé, Y. (2013). *Contrôle de gestion: Perspectives stratégiques et managériales*. Pearson Education France, p152.
[82] Pour avoir plus de détails sur les outils de calcul de coûts de la comptabilité de gestion, voir les manuels de De Rongé, Bouquin, Burlaud, Simon…

Conclusion

Nous avons vu que le contrôle de gestion a plusieurs outils, qui sont pluridisciplinaires et nous avons spécifié les quatre outils les plus fondamentaux et les plus utilisés aussi bien dans le monde académique que dans le monde professionnel. Par ailleurs, il est important de mentionner l'apparition, les réadaptations et les réajustements en permanence de nombreux outils pour une meilleure gestion.

Nous avons défini les quatre outils fondamentaux tout en déclinant les objectifs attendus. Sachant que ces différents outils ne constituent pas une perfection en soi, nous avons donc relevé quelques limites, qu'il convient de considérer lors de la construction de notre système. Dans la sous-section suivante, nous allons déterminer précisément les méthodes et outils du levier de contrôle diagnostic du processus de contrôle de l'espionnage industriel, en :

- réadaptant les outils fondamentaux évoqués,
- ayant recours à d'autres méthodes et outils plus adaptés.

Pour ce faire, nous nous adosserons sur des concepts similaires, pour expliciter les différents outils qui permettront d'appréhender le processus de contrôle de l'espionnage industriel.

Un constat remarquable et pertinent est que les trois phases de Bouquin se cloisonnent parfaitement avec les outils classiques et fondamentaux du contrôle de gestion.
Bouquin (1991) s'est intéressé à la dimension temporelle « quand le contrôle a-t-il lieu ? » et propose les trois phases du processus de contrôle dans l'organisation, à savoir :

- la finalisation des objectifs ;
- le pilotage ;
- la post-évaluation.

Les phases de Bouquin correspondent parfaitement au contrôle de gestion classique. Par ailleurs, il a déjà défini ces phases comme suit[83] :

- **La phase de finalisation, en amont de l'action** : *elle consiste à en définir les finalités et à les traduire en objectifs quantifiés sur un horizon déterminé (le plus souvent un à trois ans en contrôle de gestion) associés à la détermination des moyens jugés*

[83] Bouquin, H. (2011). *Les fondements du contrôle de gestion : «Que sais-je ?» n° 2892*. Presses universitaires de France.

nécessaires pour réussir. Cela va de pair avec la définition des rôles des différents intervenants et à celle des critères et normes qui serviront à évaluer la qualité des résultats atteints (performance). Dans le modèle classique du contrôle de gestion, ces finalités sont avant tout économiques et cette phase correspond à une planification budgétaire […].

- **La phase de pilotage, en cours d'action** : *il faut organiser un suivi du déroulement, anticiper, entreprendre les actions correctives que les déviations éventuelles rendent nécessaires pour arriver au but fixé, voire changer de but. […] la démarche classique est dans le suivi budgétaire complété de tableaux de bord.*
- **La phase de post-évaluation, après l'action ou à l'occasion d'une étape, parfois artificielle (la fin du trimestre par exemple)** : *Il s'agit de mesurer les résultats et de juger de la qualité du travail de leurs responsables. […] dans le contrôle de gestion classique, les résultats obtenus sont évalués dans trois domaines : l'économie, l'efficience et l'efficacité.*

Même si l'auteur précise qu'il s'agit d'une « *référence commode et non pas comme un ensemble de phases distinctes* »[84], ce travail a le mérite de simplification et permet d'avoir une vue d'ensemble du processus de contrôle.

Dans notre étude, nous nous baserons sur la définition la plus répandue, à savoir celle des 3 phases du processus de contrôle de Bouquin pour appréhender et modéliser le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Le choix se porte sur les trois phases de Bouquin pour les raisons suivantes :

- Les trois phases de Bouquin englobent l'ensemble des étapes temporelles du processus de contrôle dans une organisation (en amont, en cours et en aval) ;
- Les différentes phases semblent adéquates pour introduire des méthodes et outils de contrôle de l'espionnage industriel, afin d'appréhender le processus de contrôle dans chacune des étapes ;
- La définition reste la plus répandue et a le mérite de simplicité.

Le choix de la définition du processus de contrôle de Bouquin n'est en aucun cas une façon de dire que c'est le meilleur processus de contrôle pour les organisations. Nous n'avançons pas

[84] Bouquin, H. (2011). *Les fondements du contrôle de gestion : «Que sais-je ?» n° 2892*. Presses universitaires de France, p31.

un jugement dans ce sens, sachant que chaque organisation peut trouver le processus de contrôle, qui se combine de la façon la plus adéquate aux caractéristiques spécifiques de sa structure.

L'analyse de Chiapello (1996) est concise sur ce point puisqu'elle affirme, que les différents auteurs ont défini le mode de contrôle, en priorisant les six dimensions de l'organisation les unes par rapport aux autres.

Le tableau ci-dessous illustre le cloisonnement du mode de contrôle de Bouquin avec les outils classiques ou traditionnels du contrôle de gestion :

Tableau 19 : Le cloisonnement des phases du mode de contrôle de Bouquin avec les outils classiques du contrôle de gestion

Phases du mode de contrôle de Bouquin	**Outils fondamentaux du contrôle de gestion correspondants**
La phase de finalisation, en amont de l'action	La structuration en centres de responsabilité ; Les budgets
La phase de pilotage, en cours d'action	Le contrôle budgétaire ; Les tableaux de bord
La phase de post-évaluation, après l'action	Le contrôle budgétaire ; La comptabilité de gestion
Correspondent au levier de contrôle diagnostic de Simons	

Les budgets et le contrôle budgétaire constituent le système budgétaire, par contre les deux éléments se scindent dans les phases du mode de contrôle, en raison de la survenance du rôle des outils en temps voulu (l'un dans la première phase et l'autre dans la deuxième phase et la troisième phase).

2. Réajustement des méthodes et outils de base du contrôle de gestion

Les méthodes et outils de contrôle de l'espionnage industriel du levier de contrôle diagnostic seront les outils de base réajustés ou adaptés du contrôle de gestion et d'autres méthodes et outils, permettant d'effectuer efficacement les opérations de certaines phases du processus de contrôle.

Nous voulons signifier que les outils de base du contrôle de gestion, une fois réajustés ou adaptés, permettront d'effectuer les opérations de contrôle de certaines phases du processus.

Pour ce faire, nous nous inspirerons des concepts et modèles similaires suivants :

- Le contrôle de gestion environnemental ;
- La comptabilité environnementale ;
- Les coûts et performances cachés.

Nous allons, à présent, réajuster individuellement les quatre outils de base du contrôle de gestion, et proposer un autre outil permettant une appréhension de l'espionnage industriel dans l'organisation.

A. Réajustement de la structuration en centres de responsabilité

La structuration en centres de responsabilité reste une pratique des organisations de grande taille (c'est d'ailleurs une des limites), par conséquent les organisations de petite taille demeurent en marge quant à l'utilisation de cet outil. Par ailleurs, l'équivalent de cet outil dans les organisations de petite taille peut être la répartition des responsabilités ou des tâches.

Si l'on se réfère aux différentes définitions de la structuration en centres de responsabilité (données dans les méthodes et outils de base du contrôle de gestion), cet outil se caractérise par une délégation de pouvoir avec des objectifs préétablis, que les managers ou responsables doivent respecter.

L'outil en soi-même ne sera pas remplacé par un autre, par contre son contenu sera réajusté notamment par l'ajout de deux principales actions :

- **la définition des objectifs clairs et cohérents visant le processus de contrôle de l'espionnage industriel ;**

- **la sensibilisation des managers ou responsables vis-à-vis du processus de contrôle de l'espionnage industriel.**

A ce niveau, les deux actions sont des objectifs stratégiques que les managers ou les responsables vont traduire en objectifs opérationnels pour appréhender l'espionnage industriel.

En effet, il s'agirait de définir des objectifs prenant en compte l'appréhension de l'espionnage industriel, et de sensibiliser les managers ou les responsables à ce qu'ils comprennent l'ampleur dudit fléau.

La prise en compte de l'espionnage industriel intervient lors de la définition des objectifs, où il sera spécifié aux managers ou responsables les attendus de l'organisation vis-à-vis du phénomène.

La définition des objectifs est une première étape cruciale dans le processus de contrôle. Celui-ci doit se faire en première ligne, notamment lors des négociations des contrats verticaux (objectifs-moyens) ou des contrats horizontaux (client-fournisseur), à l'instar de Demeestère, Lorino et Mottis (2013).

Par exemple, l'organisation peut exiger comme un de ses objectifs, la stricte application de la norme internationale ISO 27001 sur les bonnes pratiques pour la gestion de la sécurité des informations dans toute l'organisation. Par ailleurs, les responsables des centres de responsabilité doivent disposer des moyens et ressources nécessaires à l'atteinte des objectifs visés, d'où l'importance des négociations pour étudier la faisabilité.

Une fois les objectifs visant l'espionnage industriel définis, l'étape suivante va consister à informer les managers ou les responsables, à ce qu'ils sensibilisent l'ensemble du personnel de leurs centres de responsabilité.

Ce travail de sensibilisation est indispensable au contrôle de l'espionnage industriel, car il permettra d'une part de le prévenir par l'adoption de certains comportements de sécurité, d'autre part de faciliter l'accueil des objectifs préétablis auprès de l'ensemble du personnel de l'organisation.

Par ailleurs, dans les organisations de petite taille, nous assistons à une déclinaison plus directe, c'est-à-dire que les responsables ou les managers auront déjà traduit les objectifs

stratégiques visant l'appréhension de l'espionnage industriel en objectifs opérationnels, voire en tâches à effectuer. Ensuite, ils vont sensibiliser l'ensemble du personnel, en leur expliquant les actions à effectuer pour une meilleure assise du processus de contrôle de l'espionnage industriel.

Nous pouvons remarquer l'indispensabilité de la sensibilisation du personnel aussi bien dans les organisations de grande taille que dans celles de petite taille. Cela montre l'importance de cette étape et elle reste cruciale pour la réussite d'une mise en place du processus de contrôle de l'espionnage industriel dans l'organisation.

L'espionnage industriel est un fléau qui ne se combat pas par une seule personne ou un groupe de personnes de l'organisation, mais par l'ensemble du personnel de l'organisation quel que soit le poste ou le grade de la personne.

Chaque personnel de l'organisation doit se sentir concerné, sensibilisé (informé et formé), afin d'atteindre les objectifs attendus du processus de contrôle de l'espionnage industriel.

A l'issue de cette étape, nous nous retrouvons avec des plans d'actions stratégiques, cohérents, concis et réalisables, constitués des éléments comme :

- les objectifs stratégiques à atteindre ;
- les délais ;
- les moyens et finalités négociés ;
- la désignation des managers ou responsables de pilotage des centres de responsabilité dans l'organisation…

L'étape suivante va consister à chiffrer à court terme les charges prévisionnelles et les éventuels produits. Pour ce faire, nous allons nous intéresser aux budgets et au contrôle budgétaire.

B. Réajustement des budgets et du contrôle budgétaire

Les budgets et le contrôle budgétaire, appelés aussi système budgétaire, sont le plus souvent liés, car ils se succèdent dans les étapes du contrôle de gestion et les mêmes données utilisées dans l'élaboration des budgets sont reprises dans le contrôle budgétaire pour les confronter aux données réelles.

Par ailleurs, nous avons mentionné que les deux éléments se scindent selon les trois phases du mode de contrôle de Bouquin : les budgets se trouvant dans la phase de finalisation (en amont de l'action) et le contrôle budgétaire dans la phase de pilotage (en cours de l'action) et la phase post-évaluation (après l'action).

Nous allons les aborder individuellement pour un meilleur éclaircissement des étapes de notre processus de contrôle de l'espionnage industriel.

a. Les budgets

Une fois les négociations effectuées et les objectifs stratégiques définis dans la structuration en centres de responsabilité, le rôle des budgets consistera en une planification plus opérationnelle des actions, et à chiffrer à court terme les éventuelles charges et les produits escomptés de l'organisation.

Habituellement, l'organisation établit ses budgets dans un ordre précis (commençant par les budgets de ventes, ensuite les budgets de production, etc.[85]), sous contraintes de certains facteurs comme les moyens de production, les capacités de ventes… Sachant que tous ces éléments demeurent prévisionnels, cela aboutit aux différents documents de synthèse.

Par contre, l'espionnage industriel n'est pas un produit (ou service), qui se commercialise et génère des profits, mais plutôt un phénomène qui engendre énormément de pertes à l'organisation (allant des pertes de sommes colossales à la faillite de certaines organisations).

Ces coûts liés à l'espionnage industriel doivent être anticipés et l'idéal serait que l'organisation empêche la naissance desdits coûts. La difficulté d'appréhension de

[85]Voir Grandguillot, B. (2013). *L'essentiel du contrôle de gestion 2013*. Gualino éditeur ; et Augé, B., & Naro, G. (2011). *Mini manuel de contrôle de gestion*. Dunod.

l'espionnage industriel par les budgets classiques réside à ce niveau, puisque ces derniers sont interdépendants et doivent être bien construits[86].

Cependant, l'objectif demeure le combat de l'espionnage industriel pour éviter des pertes colossales (voire la faillite) à l'organisation. Dans cette optique, les produits escomptés de l'organisation peuvent être l'ensemble des coûts évités grâce au processus de contrôle mis en place, voire la survie totale de l'organisation dans le cas où elle devrait être en faillite suite à l'espionnage industriel. Or, cette évaluation échappe aux méthodes classiques de construction des budgets.

Quant aux charges de l'espionnage industriel dans l'organisation, elles peuvent être de deux types :

- **les coûts visibles :** nous avons déjà donné la définition des coûts visibles dans le cadre théorique (définition selon la théorie socio-économique). Dans le cas de l'espionnage industriel, il s'agit des coûts de revient de l'ensemble des actions entrant dans le cadre de la prévention et de la protection contre l'espionnage industriel dans l'organisation (formations du personnel, achats des matériels anti-espionnages, brevets de protection, les frais d'acquisition des droits d'auteur, etc.). S'ajoutent à ces éléments, certains coûts de réparation des dommages provoqués par l'espionnage industriel, tels que les frais de poursuite judiciaire, les honoraires des avocats, etc.

  Le tableau ci-dessous contient les différents coûts visibles provenant du processus de contrôle de l'espionnage industriel :

[86]Voir les principes de base du système budgétaire de Gervais, M. (2009). *Contrôle de gestion*, 9ème édition, Economica, p355.

Tableau 20 : Les coûts visibles de l'espionnage industriel

Coûts visibles de l'espionnage industriel		
Coûts de prévention	Coûts de protection	Autres coûts visibles

- **Les coûts invisibles :** ce sont des coûts cachés qui sont dilués dans les produits ou services et des coûts d'opportunité.
  Les premiers sont des coûts incorporés dans les produits ou services, suite à la résolution des problèmes survenus à cause de l'espionnage industriel.
  Les coûts d'opportunité représentent l'ensemble des produits, que l'organisation aurait dû engendrer si elle n'avait pas été victime d'espionnage industriel. C'est le manque à gagner, qui empêche le bon fonctionnement de l'organisation. S'ajoutent à ces coûts d'autres charges invisibles.

  Le tableau suivant comporte les différents coûts invisibles pouvant être générés par l'espionnage industriel dans l'organisation :

Tableau 21 : Les coûts invisibles de l'espionnage industriel

Coûts invisibles de l'espionnage industriel		
Coûts incorporés dans les produits ou services	Coûts d'opportunité	Autres coûts invisibles

Nous pouvons remarquer que l'organisation ne peut prétendre avoir des produits escomptés, mais plutôt prévenir la naissance des coûts exorbitants pour maintenir sa pérennité. De ce fait, les budgets classiques peuvent cerner une partie des coûts visibles, qui peuvent être budgétés, notamment ceux de la prévention et de la protection.

Quant aux coûts de réparation et les coûts invisibles, ils sont incertains puisqu'ils naissent suite à la survenance de l'espionnage industriel.

Les coûts invisibles de l'espionnage industriel nous renvoient au concept des coûts et performances cachés, et sans une mise en place du processus de contrôle de l'espionnage industriel, les seuls coûts existants seraient ces coûts invisibles si l'organisation est victime du phénomène.

L'enjeu est majeur, puisque la survie de l'organisation en dépend totalement (en se référant aux organisations qui partent en faillite à cause des problèmes d'espionnage industriel selon les rapports nationaux et internationaux).

Etant donné que les produits escomptés sont l'ensemble des coûts évités grâce au processus de contrôle mis en place, nous pouvons remarquer que les produits escomptés correspondent à l'ensemble des coûts invisibles et une partie des coûts visibles notamment les coûts de réparation des dommages provoqués par la survenance de l'espionnage industriel.

Par ailleurs, budgéter des coûts invisibles, dont la survenance est incertaine, n'est pas une chose facile et ne peut jamais être exhaustif. Les coûts visibles, qui sont dépendants de la survenance de l'espionnage industriel, entrent aussi dans ce cadre.

Cependant, le rôle des budgets consiste à chiffrer les besoins de financement des investissements et charges nécessaires au processus de contrôle de l'espionnage industriel. Connaissant la structure des coûts de l'espionnage industriel (coûts visibles et invisibles), nous pouvons budgéter les coûts visibles du processus de contrôle de l'espionnage industriel, grâce aux plans d'actions définis par les managers ou les responsables.

Il s'agit de chiffrer, en octroyant une valeur financière à toutes les actions planifiées dans le cadre du processus de contrôle de l'espionnage industriel, notamment les actions de prévention et de protection (formations du personnel, mise en place des dispositifs anti-espionnages, souscription des brevets, etc.).

Cette partie permettra de connaitre toutes les dépenses, que l'organisation engagerait pour éviter la survenance de l'espionnage industriel.

En ce qui concerne les coûts visibles, qui sont liés à la survenance de l'espionnage industriel (coûts de réparation des dommages) et les coûts invisibles, leur prévision est très incertaine et exhaustivement impossible. Cependant, nous pouvons **attribuer une valeur en fonction des éléments de coûts historiques dus à l'espionnage industriel dans l'organisation, ou**

attribuer une valeur forfaitaire en fonction des coûts moyens relevés des cas d'espionnage industriel dans le secteur, le domaine d'activité, dans la région, etc.

Afin d'atteindre les objectifs d'évaluation et de réduction des coûts de l'espionnage industriel (voire empêcher carrément la naissance desdits coûts), nous avons jugé nécessaire de focaliser l'attention sur les charges du phénomène plutôt que ses produits. Ces différents éléments constituent les raisons pour lesquelles nous n'avons déterminé que le budget des charges de l'espionnage industriel.

Le tableau ci-dessous est un récapitulatif des étapes de construction d'un budget tenant compte de l'espionnage industriel :

Tableau 22 : Les étapes de construction du budget des charges de l'espionnage industriel

<table>
<tr><th colspan="4">Etapes de construction du budget des charges de l'espionnage industriel</th></tr>
<tr><th colspan="2">Charges visibles</th><th colspan="2">Charges invisibles</th></tr>
<tr><td colspan="2">- Déterminer les actions de prévention et de protection du processus de contrôle de l'espionnage industriel ;
- Spécifier en quantité les besoins nécessaires à la réalisation des actions définies ;
- Chiffrer les éléments de coûts, tout en précisant leur période de survenance (mensuellement, trimestriellement, etc.).</td><td colspan="2">- attribuer une valeur en fonction des éléments de coûts historiques dus à l'espionnage industriel dans l'organisation ;
- ou attribuer une valeur forfaitaire en fonction des coûts moyens relevés des cas d'espionnage industriel dans le secteur, le domaine d'activité, dans la région, etc.</td></tr>
<tr><td>Charges visibles</td><td>Total = …….</td><td>Charges invisibles</td><td>Total = ……</td></tr>
</table>

La spécificité de ce budget est qu'il n'appréhende que les charges prévisionnelles de l'espionnage industriel. Cependant, nous pouvons remarquer qu'une partie de ces charges prévisionnelles demeure incertaine et difficile à budgéter (les charges invisibles, comprenant aussi une partie des charges visibles dépendantes de la survenance de l'espionnage industriel dans l'organisation).

Nous n'avons pas déterminé les produits escomptés pour deux raisons :

- l'objectif dans notre modèle est l'évaluation et la maîtrise des coûts de l'espionnage industriel, voire empêcher son apparition. Il s'agit d'évaluer, de prévoir les coûts de l'espionnage industriel, mais aussi d'anticiper la survenance desdits coûts dans l'organisation ;
- la détermination des produits escomptés est très délicate, au vu de son caractère incertain et de sa dépendance à la survenance de l'espionnage industriel. Par conséquent, il serait intéressant de valoriser lesdits « produits » après l'action, c'est-à-dire lors de la phase post-évaluation (à l'instar de Bouquin).

Cependant, nous n'ignorons guère les bénéfices que l'organisation pourrait en tirer, puisque l'évaluation des ces éléments de produits se fera à la phase post-évaluation, c'est-à-dire lors de l'évaluation des coûts réels.

b. Le contrôle budgétaire

A ce stade, il s'agit d'évaluer les coûts réels et les confronter aux coûts budgétés afin d'observer les écarts. Cette étape permet de juger le niveau d'atteinte des objectifs et donne l'occasion aux managers ou responsables de l'organisation de prendre le recul sur leurs stratégies. Cette confrontation se fera une fois que les deux coûts (réels et budgétés) seront calculés.

Ce contrôle budgétaire va permettre de voir l'évolution des charges prévisionnelles par rapport aux dépenses réellement effectuées. Comme expliqué ci-haut, l'objectif recherché avec le processus de contrôle de l'espionnage industriel demeure non seulement l'évaluation des coûts de l'espionnage industriel, mais aussi l'anticipation et l'empêchement de la naissance desdits coûts.

Cependant, sans ignorer les produits, nous nous concentrons sur les charges et appréhendons les stratégies de réduction, voire de suppression de ces coûts.

Ainsi, nous allons montrer comment se calculent les coûts réels de l'espionnage industriel dans la partie de la comptabilité de gestion et des méthodes d'évaluation des coûts cachés.

Une fois ce calcul effectué, le contrôle budgétaire va consister à comparer les charges budgétées aux coûts réels, afin d'exposer les écarts. Ces écarts vont permettre aux managers ou aux responsables de détecter les sources de problème, afin d'apporter des actions correctives. C'est également l'occasion de reconsidérer éventuellement les stratégies préalablement définies.

Ce contrôle budgétaire se fait de la même manière que celui d'un produit ou service de l'organisation. Néanmoins, quelques petites différences subsistent comme :

- la focalisation est accentuée sur les écarts des coûts de l'espionnage industriel, or pour un produit ou service, les écarts de prix et de quantités sont importants à déterminer (les écarts sur les produits) ;
- le calcul des coûts réels d'un produit ou service est assez évident, et peut être cerné par les méthodes de calcul classiques du contrôle de gestion (méthodes d'évaluation des coûts complets, des coûts variables, etc.). Cependant, le calcul des coûts réels de l'espionnage industriel est beaucoup plus complexe et échappe aux aptitudes d'appréhension desdites méthodes classiques…

A présent, nous allons exposer les étapes de construction d'un tableau de bord adapté au contrôle de l'espionnage industriel, avant de présenter des méthodes d'évaluation des coûts réels du phénomène.

C. Un tableau de bord adapté au contrôle de l'espionnage industriel

Les caractéristiques d'un tableau de bord (comme son aptitude à contenir aussi bien des indicateurs qualitatifs que quantitatifs) font de cet outil un véritable « outil-caméléon »[87], dans le sens où son adaptation à l'appréhension des nouveaux phénomènes semble plus facile que d'autres outils.

Le tableau de bord, qui est un outil d'alerte, peut être très utile dans la prévention contre la survenance de l'espionnage industriel.

[87]Nous avons utilisé ce terme pour notifier sa capacité d'adaptabilité.

Pour ce faire, il faudrait définir des indicateurs pertinents, afin d'avoir des clignotants inhérents aux objectifs visés dans le tableau de bord.

Dans cette optique, le seul changement à apporter réside au niveau des composants du tableau de bord de l'organisation.

Le tableau de bord habituel de l'organisation ne subira pas une métamorphose complète, mais plutôt une prise en compte des nouveaux objectifs à atteindre cernant l'espionnage industriel.

Cette prise en compte de l'espionnage industriel passe par les mêmes étapes de construction du tableau de bord de l'organisation, à savoir :

- **définition des objectifs :** il s'agit de **définir clairement, avec cohérence, les objectifs visés qui se rapportent au contrôle de l'espionnage industriel** et ceux-ci doivent être **atteignables** ;
- **détermination des variables d'actions :** à ce niveau, il faut **déterminer les principaux facteurs clés de succès** des objectifs visés se rapportant à l'appréhension de l'espionnage industriel et ces derniers doivent être **contrôlables et mesurables quantitativement et ou qualitativement** ;
- **choix des indicateurs :** suite à la détermination des facteurs clés de succès, **il sera question d'identifier des indicateurs de mesure de la performance représentatifs et pertinents, qui demeureront dans le périmètre d'action des responsables** (c'est-à-dire qu'ils ont les moyens et le pouvoir d'agir sur ces éléments leur permettant ainsi d'apporter des actions correctives) ;
- **responsabilisation :** il consiste à **rattacher les différents indicateurs choisis aux responsables ayant les moyens et le pouvoir de pilotage sur ces derniers** ;
- **mise en place d'un système de normes :** il est important d'avoir un **référentiel à atteindre ou à ne pas dépasser pour chaque indicateur,** afin que l'atteinte des objectifs soit plus probante ;
- **périodicité :** cette partie se caractérise par **la définition de la périodicité de contrôle des indicateurs choisis**, c'est-à-dire que chaque indicateur est relevé à nouveau à cette échéance.

Les mêmes objectifs stratégiques définis, depuis la structuration en centres de responsabilité, et déclinés en objectifs opérationnels peuvent ainsi être pris dans le tableau de bord.

Le tableau ci-dessous est une illustration des éléments du processus de contrôle de l'espionnage industriel dans un tableau de bord :

Tableau 23 : Une illustration des éléments du processus de contrôle de l'espionnage industriel dans un tableau de bord

Objectifs	Variables d'actions ou facteurs clés de succès	Indicateurs	Responsables	Normes de référence	Périodicité
L'adoption des comportements pour prévenir la survenance de l'espionnage industriel via la sensibilisation du personnel.	Formations Contrôles aléatoires	✓ Pourcentage d'employés formés ✓ Nombre d'anomalies relevées lors du contrôle aléatoire	➢ Responsable des ressources humaines ➢ Contrôleur de gestion	✓ 100% ✓ 0	❖ Trimestrielle ❖ Hebdomadaire
La mise en œuvre de la norme ISO/IEC 27001 management de la sécurité de l'information.	Implication du personnel Adoption des principes élémentaires de la norme	✓ Nombre de réunions avec les employés ✓ Nombre d'exigences non respectées de la norme	➢ Responsable du centre de responsabilité ➢ Responsable du centre de responsabilité et contrôleur de gestion	✓ Au moins 2 ✓ 0	❖ Mensuelle ❖ Mensuelle

Le tableau ci-dessus est une illustration prenant en compte l'appréhension de l'espionnage industriel dans le tableau de bord de l'organisation. **Il consiste à introduire les éléments d'appréhension de l'espionnage industriel dans le tableau de bord de l'organisation, en passant par les mêmes étapes de construction d'un tableau de bord**.

A l'instar des étapes du mode de contrôle de Bouquin, nous sommes dans la phase de pilotage, c'est-à-dire que le tableau de bord s'utilise en cours de l'action. L'organisation pourra faire ressortir ses performances vis-à-vis des objectifs préétablis du processus de contrôle de l'espionnage industriel.

En plus de ses objectifs classiques (permettre l'autocontrôle du centre de responsabilité et le reporting à la hiérarchie), ce tableau de bord peut permettre également de revoir l'efficacité des stratégies initialement mises en œuvre et ainsi aider à la prise de nouvelles décisions.

Cependant, les différents tableaux de bord des centres de responsabilité doivent être cohérents avec l'organigramme de l'organisation. Nous voulons signifier qu'il est important de faciliter l'emboitement des éléments des tableaux de bord entre les différents niveaux hiérarchiques, afin de faciliter l'agrégation et la cohérence des informations.

D. Réajustement de la comptabilité de gestion

A ce stade, nous sommes dans la dernière phase de contrôle de l'espionnage industriel par le système de contrôle diagnostic, qui correspond à la phase de post-évaluation de Bouquin (après l'action). Les phases de finalisation et de pilotage sont à présent effectuées et l'objectif actuel est de déterminer les coûts réels de l'espionnage industriel.

L'appréhension de l'espionnage industriel se diffère des autres phénomènes (comme le calcul des coûts d'un produit), parce que le calcul des coûts de l'espionnage industriel est beaucoup plus complexe.

En effet, les coûts de l'espionnage industriel se composent des coûts visibles et des coûts invisibles. Les deux coûts ne se calculent pas de la même manière et ne s'appréhendent pas non plus par les mêmes méthodes d'évaluation des coûts.

Les coûts visibles peuvent être calculés par les méthodes d'évaluation classiques de la comptabilité de gestion, par contre les coûts invisibles, qui sont surtout liés à la survenance de l'espionnage industriel, se déterminent par les méthodes d'évaluation des coûts cachés.

Pour le calcul des coûts visibles, les méthodes classiques comme les coûts complets peuvent cerner lesdits coûts. Il s'agit de tenir compte de l'ensemble des charges engagées dans la prévention et la protection contre l'espionnage industriel dans l'organisation.

Cela se détermine à partir des éléments disponibles tels que : les achats des matériels anti-espionnages, les montants déboursés pour la souscription d'un brevet, les frais de formation, etc.

Quant aux coûts invisibles, ils échappent aux aptitudes d'analyse des outils de calcul classiques du contrôle de gestion se nourrissant principalement des éléments des systèmes d'information de l'organisation. Ainsi, nous allons exposer la méthode d'évaluation des coûts invisibles, à travers les méthodes d'évaluation des coûts cachés.

3. Autres méthodes et outils : méthodes des coûts cachés

Les caractéristiques occultes de l'espionnage industriel exigent certains outils et méthodes plus adaptés, c'est le cas de l'évaluation des coûts de l'espionnage industriel. Les principales méthodes d'évaluation des coûts du contrôle de gestion nécessitent des données comptables « visibles », c'est-à-dire les données issues des systèmes d'information de l'organisation. Le plus souvent nous n'appréhendons pas certaines données « invisibles », qui engendrent des coûts imperceptibles et réduisent significativement les performances des organisations.

L'espionnage industriel entre dans ce cadre, car une fuite d'informations permettra aux concurrents d'exploiter les mêmes activités que l'organisation victime d'espionnage industriel. Ce qui provoquera une perte en termes de chiffre d'affaires (réduction de la part de marché, etc.). Les organisations subissent énormément de pertes de ce genre et cette ignorance (ou méconnaissance) de l'espionnage industriel peut même conduire certaines structures en faillite.

En plus des coûts issus des systèmes d'information, l'espionnage industriel engendre des coûts imperceptibles, qui empêchent les organisations d'être efficacement rentables, compétitives et détériorent leur qualité de fonctionnement (voire conduire en faillite certaines structures).

La question est de savoir : à partir des méthodes d'évaluation des coûts cachés, comment évaluer les coûts invisibles de l'espionnage industriel ?

Pour ce faire, nous allons spécifier les sources et les étapes d'évaluation des coûts cachés, pour ensuite appréhender l'évaluation des coûts invisibles de l'espionnage industriel.

A. Sources des coûts cachés

Le concept a été mis en évidence par la théorie socio-économique des organisations (ISEOR : institut socio-économique des entreprises et des organisations, 1973-1978), issu des courants structuraliste (relation structures-comportements-résultats) et comportementaliste et behavioriste (comportements-résultats). Cette théorie considère l'entreprise, comme un ensemble de structure de travail en interaction avec les comportements du personnel. Le fonctionnement de l'entreprise se décompose en un bon fonctionnement et des dysfonctionnements.

Selon cette théorie, les coûts et performances cachés sont des coûts dus à des irrégularités, des anomalies, des perturbations dans le fonctionnement de l'organisation (dénommées les dysfonctionnements, qui sont à la base des problèmes d'efficacité et d'efficience), qui l'empêchent de réaliser ses objectifs et provoquent un gaspillage de ressources.

Savall et Zardet (2010) montrent que les coûts cachés sont des coûts dilués dans le coût des produits/services (coûts historiques) ou des coûts d'opportunité, qui par nature ne sont pas enregistrés et proviennent des dysfonctionnements issus des structures et des comportements des membres de l'organisation.

Selon nos deux auteurs, les structures et les comportements interférent et engendrent des dysfonctionnements, qui sont à l'origine des coûts cachés. Ils montrent que la cause exacte des coûts cachés provient de cette interférence permanente et complexe, et affirment que ces interférences ne se réalisent pas dans tous les domaines du fonctionnement de l'organisation.

D'une part, Savall et Zardet (2010)[88] définissent les structures comme l'ensemble des éléments relativement permanents de l'organisation, se caractérisant par :

- *la capacité de durée dans le temps de leurs principaux attributs ;*
- *la capacité d'évolution autonome lente et progressive de ces derniers ;*
- *le haut niveau de dépense d'énergie sociale (individuelle ou collective, plus ou moins consciente), matérielle et financière nécessaire à la réalisation d'une évolution plus rapide.*

[88] Savall H. et Zardet V. (2010), « maîtriser les coûts et les performances cachés », Economica, p169 et p171.

Prônant que les structures se caractérisent par les deux propriétés de permanence et de prégnance, ils les classent en cinq catégories de structures à savoir :

- structures physiques ;
- structures technologiques ;
- structures organisationnelles ;
- structures démographiques ;
- structures mentales.

D'autre part, ils définissent les comportements[89] comme étant : « *les manifestations, les réactions, la manière de conduite de l'Homme véritablement observées dans une situation donnée et qui ont un impact sur son environnement financier et social* ».

Ils font la différence entre les attitudes et les comportements, pour éviter toute confusion (les attitudes constituent plus précisément un potentiel de comportement, elles se traduisent au contact des événements par des comportements observables). Les comportements se situent en aval des structures et des attitudes, et se distinguent par leur nature conjoncturelle et leur relative instabilité.

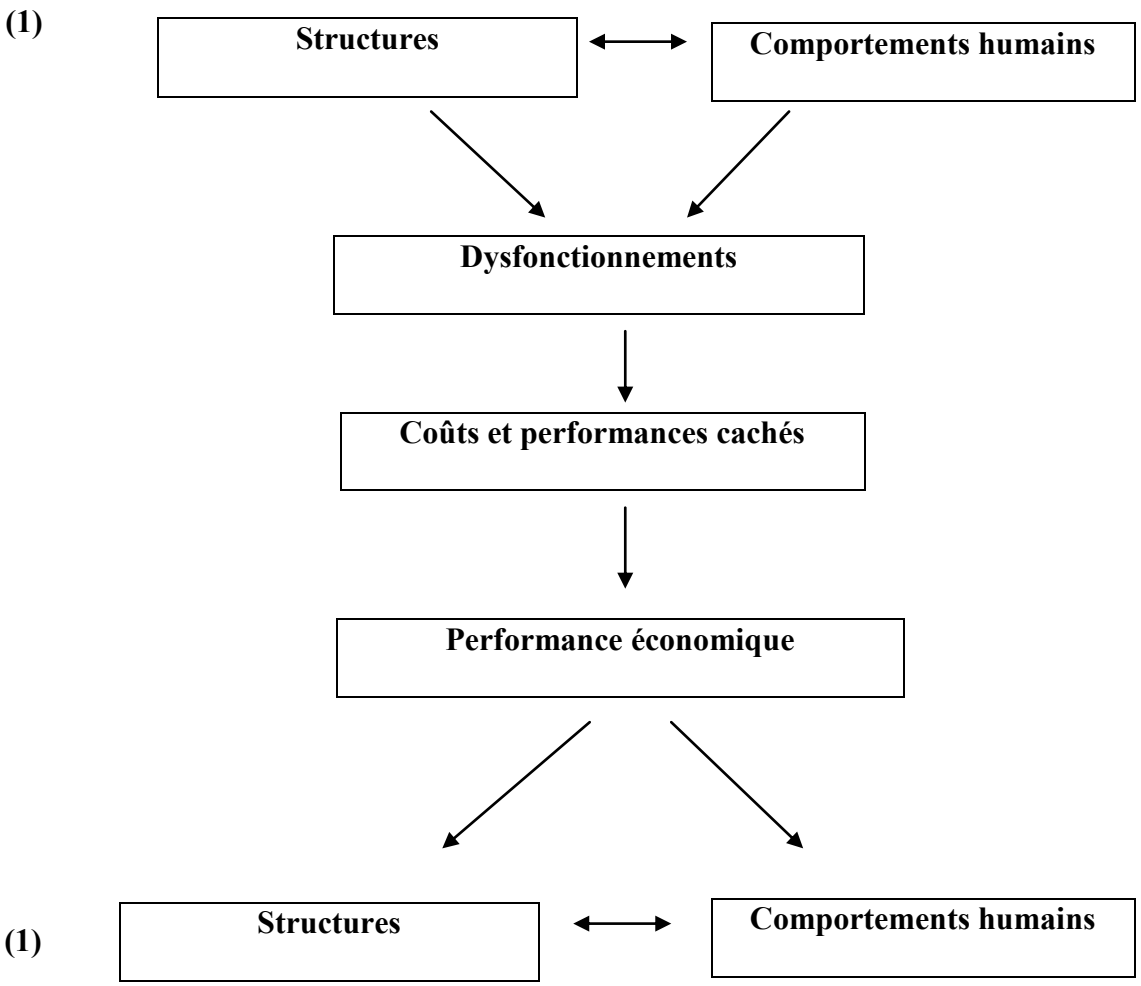
Ils identifient cinq logiques de comportements auxquelles l'individu peut obéir :

- logique individuelle ;
- logique de groupe d'activité ;
- logique catégorielle ;
- logique de groupe d'affinité ;
- logique collective.

La figure ci-dessous représente le cycle des coûts cachés, partant des structures et comportements de l'organisation aboutissant aux mêmes éléments :

[89] Savall H. et Zardet V. (2010), « maîtriser les coûts et les performances cachés », Economica.

Figure h : Cycle des coûts cachés dans une organisation



Les interférences mentionnées ci-haut apparaissent, selon la théorie socio-économique, réalistement dans six domaines :

- les conditions de travail ;
- l'organisation du travail ;
- la communication-coordination-concertation ;
- la gestion du temps ;
- la formation intégrée ;
- la mise en œuvre stratégique.

Il convient de détailler ces différents domaines, afin d'exposer plus clairement la façon dont naissent les coûts cachés[90] :

- **Les conditions de travail :**

Ces conditions de travail sont de façon générale l'environnement dans lequel les salariés effectuent leurs tâches (lieu de travail) et l'ensemble des relations existantes de travail.

- **L'organisation du travail :**

C'est l'attribution des rôles (principales fonctions de l'entreprise), l'imputation des tâches au sein des unités et les différentes corrélations dans le travail.

- **La communication-coordination-concertation :**

C'est l'ensemble des coopérations, des échanges d'informations et autres qui s'effectuent entre les individus de l'organisation ou l'entreprise pour la réalisation de leurs tâches. Selon Savall et Zardet (2010), la communication regroupe tous types d'échanges d'informations entre acteurs : formels ou informels, hiérarchiques ou horizontaux, relatifs à l'activité professionnelle ou non.

La coordination s'applique aux dispositifs d'échanges d'informations entre acteurs, organisés en vue de réaliser un objectif opérationnel ou fonctionnel de l'activité.

La concertation caractérise les types d'échanges d'informations entre acteurs, qui permettent de définir un objectif opérationnel ou fonctionnel commun à réaliser sur une période déterminée.

- **La gestion du temps :**

La technique d'allocation du temps de travail individuel ou collectif, l'imputation du temps de l'individu entre ses principales tâches ou activités.

- **La formation intégrée :**

Ce sont les formations professionnelles faites par l'organisation ou l'entreprise, afin d'améliorer les compétences des individus.

- **La mise en œuvre stratégique :**

[90] Savall H. et Zardet V. (2010), maîtriser les coûts et les performances cachés, Economica.

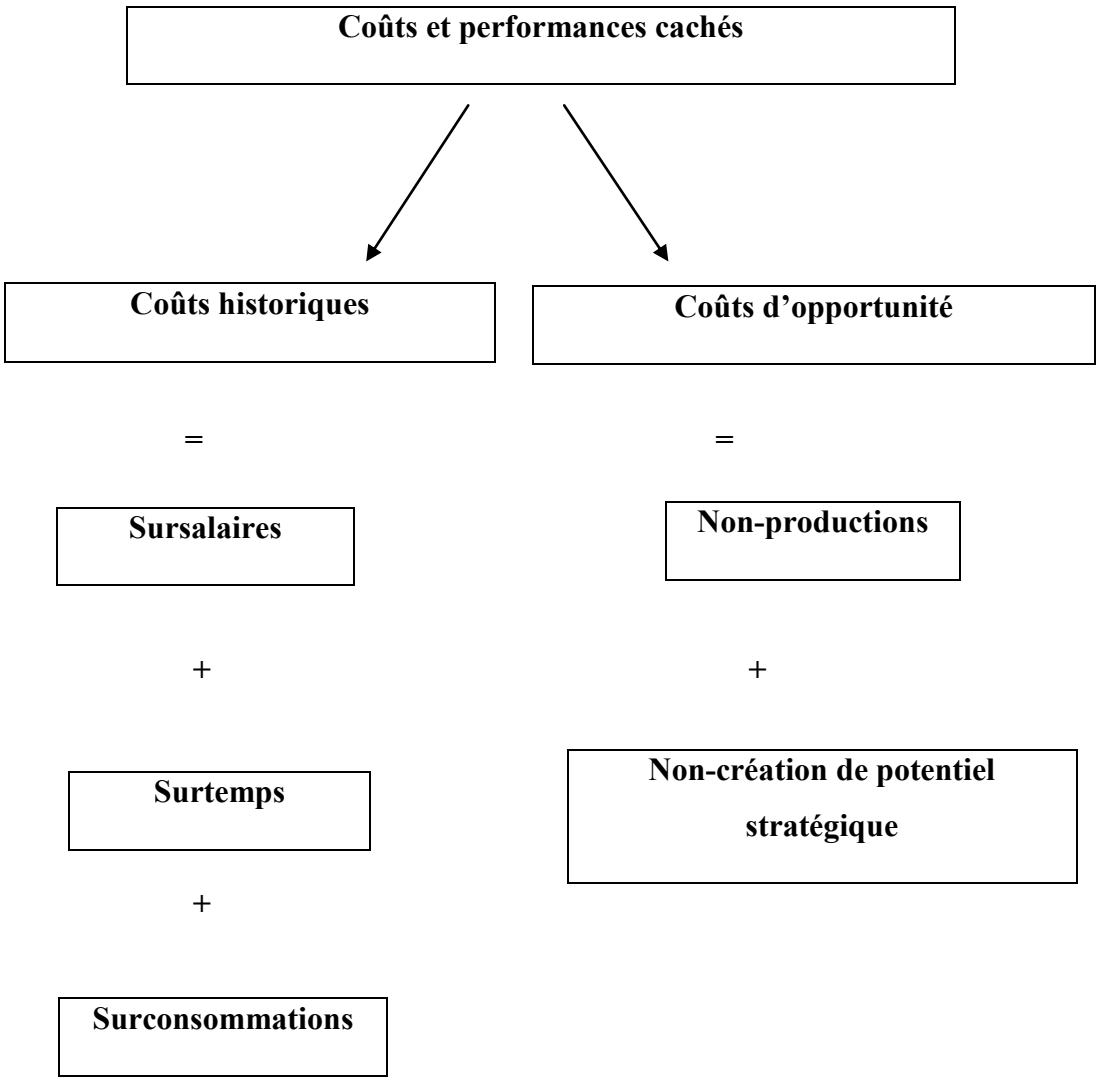
C’est l’ensemble des outils, des démarches, des procédés utilisés par l’organisation ou l’entreprise pour atteindre les objectifs visés (transformation des objectifs managériaux ou stratégiques en actions courantes).

B. Méthodes d’évaluation des coûts cachés

Les méthodes d’évaluation des coûts cachés peuvent être regroupées en deux catégories : celles permettant l’évaluation des coûts historiques (coûts dilués dans les produits ou services) et celles déterminant les coûts d’opportunité.

Ainsi, l’institut socio-économique des entreprises et des organisations a caractérisé ces deux catégories de coûts en cinq familles de coûts regroupant les coûts et performances cachés, il s’agit :

Figure i : Méthodes d'évaluation des coûts cachés



a. *Méthodes d'évaluation des coûts historiques (coûts dilués dans les produits ou services)*

Selon la théorie socio-économique, ce genre de coûts se distingue par son absence d'identification claire par des lignes spécifiques dans les différentes écritures comptables de l'organisation. Le système d'évaluation correspondant est le mode d'évaluation « SOF : Social, Organisationnel, Financier », appelé aussi la méthode « QQFI : qualitative, quantitative, et financière » de l'institut socio-économique des entreprises et des organisations (ISEOR).

Les chercheurs de l'ISEOR ont défini trois composants de coûts, appelés aussi familles de coûts, auxquels les coûts cachés sont liés. Ces différentes familles de coûts constituent les coûts historiques, il s'agit : des surconsommations, des sursalaires et des surtemps.

Le mode d'évaluation SOF consiste à déterminer le gisement de ressources financières affectées à la régulation des dysfonctionnements et des anomalies, et dont une partie peut être mobilisée pour des activités de création de valeur économique.

Les étapes de la méthode SOF pour déterminer les coûts cachés incorporés aux coûts sont :

- **Le module social :**
  - rendre évidents les dysfonctionnements dans l'atelier phosphorique ;
  - répertorier les dysfonctionnements ;
  - rechercher les relations et les liens de causalité existants entre les dysfonctionnements ;
  - ordonner les dysfonctionnements en catégories ;
  - faire un Pareto des dysfonctionnements ou anomalies, en fonction du nombre d'occurrences par catégorie.
- **Le module organisationnel :**
  - mettre en liste les régulations qui ont été mises en œuvre ;
  - chiffrer les impacts des actions mises en œuvre.
- **Le module financier :**
  - valoriser les coûts de chacune des actions.

b. Méthodes dévaluation des coûts d'opportunité

Selon Andreani (1967), le terme des coûts d'opportunité, « opportunity-cost » en anglais, est d'origine américaine et a été employé pour la première fois par Green (1894). Par ailleurs, l'auteur affirme que l'origine de l'idée se trouve dans les écrits de l'école autrichienne, notamment dans ceux de Wieser.

Parler d'opportunity-cost selon lui, c'est : *« évaluer le coût de ce qui est choisi en termes de ce que l'on cède mais aussi en termes de ce que l'on renonce à obtenir, c'est mesurer le coût en occasions perdues »*[91].

A l'instar du même auteur, il est intéressant de parler de coûts d'opportunité pour évaluer les états futurs virtuels entre eux, afin d'aider à la prise de décision en effectuant le bon choix. Cependant, il peut également être intéressant de déterminer les coûts d'opportunité des états passés, actuels et futurs pour certains nouveaux phénomènes, qui ne font pas l'objet d'une priorité pour les organisations.

Ainsi, recourir à l'évaluation des coûts d'opportunité de certains phénomènes, comme l'espionnage industriel, permettrait aux organisations d'une part de reconsidérer l'ampleur et l'enjeu du fléau, d'autre part d'être plus performantes, plus compétitives en tenant compte de ces éléments de coût pour une meilleure prise de décision (fixation des prix, politique de maîtrise des coûts, analyse des responsabilités, etc.).

Il existe plusieurs manières d'évaluer les coûts d'opportunité (approche économique, approche financière, etc.), mais toutes ces différentes méthodes ont le même socle, c'est-à-dire la détermination du manque à gagner.

Les causes de ce manque à gagner sont diverses, allant d'une mauvaise prise de décision, générant un éventuel écart de profit à une perte de clientèle, suite à la survenance d'un phénomène.

Pour évaluer les coûts d'opportunité, les chercheurs de l'ISEOR ont défini **deux composants de coûts ou familles de coûts, il s'agit : des coûts de non-production et de non-création de potentiel stratégique.**

[91] Andreani, E. (1967). Le coût d'opportunité. *Revue économique*, vol. 18, no 5, p. 840-858.

Les **coûts cachés liés à ces composants sont déterminés en multipliant respectivement le temps d'inactivité de non-production et le temps perdu de non-création de potentiel stratégique par un taux horaire « contribution horaire à la marge sur coût variable », qui se note CHMCV**[92] et se calcule de la façon suivante :

$$CHMCV = \frac{\text{Marge sur coût variable de l'année}}{\text{Nombre d'heures d'activité de l'année}}$$

C. Méthodes d'évaluation des coûts invisibles de l'espionnage industriel

Lorsque l'organisation est victime d'espionnage industriel, cela engendre des coûts de réparation (procédures judiciaires, honoraires des avocats, etc.). Ces différents éléments n'ont pas tous forcement une dénomination dans le système comptable, ou ils sont dilués dans les éléments de coût de l'organisation (selon l'ISEOR, il s'agit des coûts historiques).

L'évaluation des coûts invisibles de l'espionnage industriel consiste à déterminer les coûts de réparation dilués dans les éléments de coût et les coûts d'opportunité (manque à gagner).

Le mode d'évaluation SOF ou QQFI de l'ISEOR permet de recenser tous les coûts dilués dans les éléments de coût. En effet, il s'agit de déterminer le gisement de ressources financières affectées à la réparation des dommages de l'espionnage industriel.

Quant à l'évaluation des coûts d'opportunité de l'espionnage industriel, nous pouvons utiliser plusieurs composants de coûts comme : les coûts de non-production, les coûts de non-potentiel stratégique, les coûts liés à des variables de profit impactées par l'espionnage industriel…

Les coûts de non-production seront l'ensemble des occasions de production perdues suite à une perte de clientèle (diminution de la part de marché), tandis que les coûts de

[92] Horngren C., Bhimani A., Datar S. et Foster G. (2009), Contrôle de gestion et gestion budgétaire, Pearson éducation, 425p.

non-potentiel stratégique constitueront le temps perdu par les employés à la résolution des problèmes d'espionnage industriel évalué au taux horaire CHMCV.

L'organisation peut évidemment déterminer d'autres composants de coûts, selon les caractéristiques d'occasions du domaine d'activité, du secteur d'activité, etc.

L'idée consiste à déterminer l'ensemble des coûts d'occasions perdues suite à la survenance de l'espionnage industriel. La détermination des coûts des différents composants est résumée dans le tableau des étapes d'évaluation.

En résumé, l'organisation doit lister les différentes variables impactées (ou pouvant être impactées) par l'espionnage industriel, pour ensuite les quantifier en coûts au travers : des multiplicateurs comme le taux horaire CHMCV pour le temps d'inactivité et le temps perdu, d'une comparaison entre les valeurs de ces variables avant et après espionnage industriel, etc.

Le tableau suivant est un récapitulatif des étapes d'évaluation des coûts historiques et des coûts d'opportunité de l'espionnage industriel :

Tableau 24 : Méthodes d'évaluation des coûts invisibles de l'espionnage industriel

Méthodes d'évaluation des coûts invisibles de l'espionnage industriel	
Etapes d'évaluation des coûts historiques (coûts dilués dans les éléments de coût)	**Etapes d'évaluation des coûts d'opportunité**
Mode d'évaluation SOF ou QQFI : **Etape 1 : le module social** • répertorier les actions de prévention, de protection et de réparation concernant l'espionnage industriel ; • rechercher spécifiquement les causes des différentes actions ; • ordonner les causes en catégories ; • faire un Pareto des causes en fonction du nombre d'occurrences par catégorie. **Etape 2 : le module organisationnel** • mettre en liste les actions de prévention, de protection et de réparation qui ont été mises en œuvre ; • chiffrer les impacts des actions mises en œuvre. **Etape 3 : le module financier** • valoriser les coûts de chacune des actions.	**Coûts de non-potentiel stratégique et autres coûts d'opportunité liés au temps perdu à la résolution des problèmes d'espionnage industriel :** **Etape 1 :** déterminer le temps perdu par les employés à la résolution des problèmes d'espionnage industriel (à l'aide d'un brainstorming ou autres outils de gestion) ; **Etape 2 :** calculer la CHMCV ; **Etape 3 :** évaluer les coûts de non-potentiel stratégique (en multipliant le temps perdu par la CHMCV). **Coûts de non-production et autres coûts d'opportunité liés aux occasions perdues :** **Etape 1 :** identifier les variables de production (ou de profit) impactées par l'espionnage industriel à l'aide d'un Pareto, d'un brainstorming ou autres outils de gestion ; **Etape 2 :** quantifier (historiquement ou de manière prévisionnelle à l'aide des systèmes d'information de l'organisation) ces variables avant la survenance de l'espionnage industriel ; **Etape 3 :** évaluer ces variables après la survenance de l'espionnage industriel ; **Etape 4 :** en déduire les coûts d'opportunité (**variables avant espionnage industriel – variables après espionnage industriel**).

Le tableau ci-dessus n'est en aucun cas exhaustif, il permet juste de déterminer certains coûts invisibles de l'espionnage industriel. Par ailleurs, c'est un modèle qui peut être adapté à plusieurs structures, selon le type d'organisation, le domaine d'activité, etc.

Il permet de repérer les « coûts cachés » engendrés par l'espionnage industriel et expose ainsi sa vraie nature.

4. Conclusion de la section

Dans cette section, nous avons présenté des outils du levier de contrôle diagnostic permettant d'appréhender le processus de contrôle de l'espionnage industriel dans une organisation. Pour ce faire, nous avons identifié et caractérisé quatre outils de base du système de contrôle diagnostic de Simons (levier correspondant au contrôle de gestion classique). Ensuite, nous les avons réajustés, en introduisant les étapes de contrôle de l'espionnage industriel.

Par ailleurs, nous avons ajouté les méthodes d'évaluation des coûts cachés dans la partie de la comptabilité de gestion, car ces méthodes nous semblent plus adéquates pour le calcul des coûts de l'espionnage industriel.

En effet, les coûts de l'espionnage industriel sont composés des coûts visibles et des coûts invisibles, or les méthodes d'évaluation des coûts cachés revêtent des aptitudes probantes permettant de calculer les coûts invisibles.

Nous avons déjà mentionné la non-exhaustivité de ces outils, par ailleurs ils compensent toutes les étapes incontournables du contrôle de gestion classique, passant par les phases de finalisation, de pilotage et de post-évaluation. Ce sont des outils, qui permettent d'appréhender les figures imposées du processus de contrôle de l'espionnage industriel.
Dans la section suivante, nous allons présenter quelques outils du levier de contrôle interactif permettant de cerner les figures libres du processus de contrôle de l'espionnage industriel.

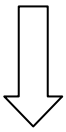
Section 2 : Détermination des outils du levier de contrôle interactif

A partir du cadre théorique, nous savons que le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion s'appréhende via les leviers de contrôle diagnostic et interactif de Simons. Dans la section précédente, nous avons défini les outils du système de contrôle diagnostic nécessaires à cette appréhension.

Cette deuxième section se scinde en deux sous-sections : une première présentant quelques méthodes et outils du levier de contrôle interactif, et une seconde détaillant la capacité des outils du système de contrôle interactif à encadrer les figures libres du processus de contrôle de l'espionnage industriel.

L'architecture de la section est la suivante :

Méthodes et outils du système de contrôle interactif



Des outils du levier de contrôle interactif cernant l'espionnage industriel

1. Méthodes et outils du système de contrôle interactif

Selon Simons (1995)[93], les systèmes de contrôle interactifs se caractérisent par quatre éléments :

- *ils se concentrent sur l'évolution constante de l'information que les gestionnaires de haut niveau ont identifiée comme potentiellement stratégique ;*
- *l'information est suffisamment importante pour exiger une attention fréquente et régulière du fonctionnement à tous les niveaux de l'organisation ;*
- *les données générées par un système interactif sont mieux interprétées et discutées lors de réunions en face à face entre des supérieurs, des subordonnés et des pairs ;*
- *le système de contrôle interactif est un catalyseur pour un débat continu sur les données sous-jacentes, les hypothèses et les plans d'action*.

Ainsi, les outils du levier de contrôle interactif se caractérisent par l'ensemble des méthodes et dispositifs de gestion impliquant l'ensemble du personnel d'une organisation, au travers d'un dialogue ou d'une concertation quelconque, dans la recherche de solutions pour prévenir les variables d'incertitudes stratégiques.

Il s'agit d'identifier et de tenir compte des informations pertinentes du personnel, pour adapter les stratégies préalablement définies aux imprévisibilités incessantes de certains phénomènes fluctuants.

Ce levier de contrôle est une sorte de « système de veille » permettant de chercher, de trouver et d'anticiper certains phénomènes contingents, qui empêchent le bon déroulement d'une stratégie définie.

Nous le qualifions de système de veille, car il doit être utilisé fréquemment dans l'organisation et la hiérarchie fonctionnelle suprême (par exemple la direction générale) doit détecter les éléments potentiellement stratégiques pour améliorer les stratégies définies.

Cette considération des employés, au travers de leur concertation pour la révision des stratégies, accentue leur degré d'appartenance vis-à-vis de l'organisation. Par conséquent, elle facilite l'accueil des nouveaux changements stratégiques ou la mise en application de nouvelles stratégies.

[93] Simons, R. (1995). Control in an age of empowerment. *Harvard business review*, 73 (2), 80-88.

Ce système de contrôle se caractérise par son aptitude à faire émerger de nouvelles stratégies et favorise l'apprentissage (Simons, 1995).

Les outils, pouvant être utilisés dans le cadre du système de contrôle interactif, sont nombreux et les organisations peuvent avoir recours aux outils qu'elles jugent convenables à leur structure.

Par exemple, Simons dans son « control in an age of empowerment (1995) » affirme que lorsqu'il s'agit de petites organisations, les managers clés et les employés peuvent s'asseoir autour d'une table et explorer informellement les impacts des différentes menaces et opportunités émergentes. Par ailleurs, l'auteur précise qu'il est pertinent de définir une méthode de concertation plus formelle, lorsque l'organisation est de grande taille ou devient de plus en plus développée.

Ainsi, nous pouvons retenir quelques outils du système de contrôle interactif, qui ont fait l'objet d'une étude empirique :

Tableau 25 : Quelques outils et études de référence du système de contrôle interactif

Outils / Méthodes	Etudes de référence
Débat et dialogue	Simons (2000), qui est l'instigateur dudit levier de contrôle, affirme que le débat et le dialogue sont les marques de fabrique des systèmes de contrôle interactifs.
Dialogues, formations et de la communication	Berland et Sponem (2007) montrent, au travers d'une étude sur la transformation du budget d'une entreprise chimique en système interactif, l'implication plus forte des managers dans le processus de contrôle, via des dialogues entre les dirigeants, des formations et de la communication.
Réflexion collective	Naro et Travaillé (2010) donnent l'exemple de la formalisation d'une stratégie à la réalisation d'un balanced scorecard dans deux entreprises industrielles et commerciales, à travers la réflexion collective des différents acteurs (dont les fonctions et les niveaux de qualification étaient différents).
Discussions	Fasshauer (2012) évoque dans l'utilisation du forecast au sein d'une division européenne d'un groupe américain les discussions hebdomadaires entre les responsables locaux, les équipes de direction du groupe et de la division, et leurs supérieurs hiérarchiques. Ces révisions hebdomadaires sont effectuées dans le but d'améliorer les prévisions mensuelles.

Les méthodes illustrées[94] dans le tableau ci-haut, les réunions, le brainstorming, les débats organisés et bien d'autres constituent des méthodes et outils utilisés dans le cadre d'un système de contrôle interactif.

[94] Les outils illustrés proviennent de « Dambrin, C., & Löning, H. (2008). Systèmes de contrôle interactifs et théories de l'apprentissage: une relecture des travaux de R. Simons à l'aune des théories

Cependant, la question est de savoir si ces différents outils et méthodes permettent d'appréhender les figures libres du processus de contrôle de l'espionnage industriel ?

2. Des outils du levier de contrôle interactif cernant l'espionnage industriel

Les figures libres du processus de contrôle de l'espionnage industriel se caractérisent par les incertitudes stratégiques liées à l'imprévisibilité des méthodes utilisées par les espions. L'organisation doit permanemment adapter ses stratégies de contre-espionnage pour assurer sa prévention et sa protection.

Ce champ d'action controversé et très changeant, surtout à l'essor des nouvelles technologies, demeure un périmètre d'action, où l'organisation pourra se distinguer compétitivement de ses concurrents, en adaptant ou en améliorant ses stratégies préalablement définies.

Ce potentiel exploitable peut être atteint via l'apport de l'ensemble du personnel de l'organisation. Des chercheurs (comme Berland, Sponem, Naro, Travaillé, Fasshauer, et bien d'autres) ont démontré, au travers des études sur le terrain, l'efficacité de la prise en compte des informations issues des concertations entre les différents employés de l'organisation.

Contrairement aux outils du système de contrôle diagnostic, qui subissent des réajustements pour appréhender les figures imposées du processus de contrôle de l'espionnage industriel, les outils du levier de contrôle interactif permettent de cerner directement les figures libres grâce aux caractéristiques de ses outils, qui rendent possible l'obtention des informations pertinentes auprès du personnel de l'organisation.

En résumé, il s'agit d'impliquer l'ensemble du personnel d'une organisation, au travers d'une concertation constante formellement ou informellement (débat, dialogue, réunion, brainstorming, discussion, etc.), dans la recherche d'informations pour non seulement détecter les failles qui subsistent dans les stratégies mises en place, mais aussi prévenir les variables d'incertitudes stratégiques, en se démarquant de la concurrence et en assurant sa pérennité.

---

piagétiennes. *Comptabilité-Contrôle-Audit*, *14*(3), 113-140. » ; et « Lepori, E., & Bollecker, M. (2015, May). Les leviers de contrôle de SIMONS: vers une compréhension des freins à l'équilibrage diagnostic/interactif. In *Comptabilité, Contrôle et Audit des invisibles, de l'informel et de l'imprévisible*, p5 ».

L'objectif de ce système interactif, à l'instar de Simons (1995), Dambrin et Löning (2008) et bien d'autres chercheurs, est la discussion constante et la remise en cause des stratégies préalablement définies pour faire face aux incertitudes stratégiques.

Ainsi, les outils du système de contrôle interactif, ne nécessitant pas de réajustement pour cerner les figures libres, requièrent néanmoins une définition de certains éléments pour comprendre réellement leur mise en application dans l'organisation, notamment savoir :

- ✓ quand l'utiliser ?
- ✓ qui l'utilise(nt) ?
- ✓ où l'utiliser ?
- ✓ etc.

C'est tout l'intérêt du chapitre suivant, dans lequel nous allons confronter les deux systèmes de contrôle (diagnostic et interactif) aux six dimensions d'analyse réajustées de Chiapello pour comprendre concrètement leur mise en application dans l'organisation.

Conclusion du chapitre 4

L'objectif de ce chapitre était de déterminer les outils et méthodes des leviers de contrôle diagnostic et interactif de notre modèle théorique, car nous avons comme objectif ultime d'élaborer un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Dans la première section de ce chapitre, nous avons déterminé les outils et méthodes du levier de contrôle diagnostic de notre modèle théorique de gestion de l'espionnage industriel par la fonction contrôle de gestion.

Le contrôle de gestion est une fonction, qui demande une adaptation permanente de ses outils et méthodes à l'environnement de l'organisation. Partant de la pluralité de ses outils et méthodes, ne pouvant guère nous permettre d'effectuer une étude exhaustive, nous avons choisi de déterminer les outils fondamentaux du contrôle de gestion et d'effectuer sur ces derniers des réajustements, afin d'appréhender les figures imposées du processus de contrôle de l'espionnage industriel.

Après une revue de littérature, quatre outils et méthodes ressortent comme les plus fondamentaux du contrôle de gestion : la structuration en centres de responsabilité, le système budgétaire (comprenant les budgets et le contrôle budgétaire), les tableaux de bord et la comptabilité de gestion.

Certains outils fondamentaux du contrôle de gestion ont déjà les aptitudes nécessaires à l'appréhension du phénomène, c'est-à-dire que ce sont des outils qui permettent d'appréhender l'espionnage industriel avec des réajustements mineurs. Il s'agit notamment du tableau de bord, qui est un véritable « outil caméléon ».

Cependant, d'autres outils ne permettent point de cerner la gestion de l'espionnage industriel. Il s'agit des méthodes classiques de calcul des coûts du contrôle de gestion, qui ne peuvent évaluer les coûts invisibles du phénomène.

Par conséquent, nous avons également fait intervenir les méthodes d'évaluation des coûts cachés, qui nous semblent parfaites pour évaluer les coûts invisibles de l'espionnage industriel. Nous avons explicité la manière, dont ces méthodes permettent d'évaluer les coûts de l'espionnage industriel.

Dans la deuxième section, nous avons exposé quelques outils et méthodes du levier de contrôle interactif, avant de mettre en exergue leur capacité à appréhender les figures libres du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Ces différents outils et méthodes déterminés des leviers de contrôle diagnostic et interactif de notre processus de contrôle ne constituent en aucun cas une exhaustivité en soi. Sachant que nous nous plaçons dans une perspective dynamique, d'autres outils et méthodes peuvent convenir pour appréhender la gestion de l'espionnage industriel par la fonction contrôle de gestion.

Nous avons juste déterminé des outils et méthodes, qui cernent toutes les étapes de contrôle dans une organisation, à l'instar des trois phases de Bouquin (1991) : avant l'action correspondant à la finalisation des objectifs, au cours de l'action correspondant au pilotage, et après l'action correspondant à la post-évaluation.

Cependant, sur un plan managérial l'utilisation de ces outils dans l'organisation semble floue et nécessite une clarification, afin de faciliter leur usage. Pour ce faire, nous allons faire intervenir les dimensions d'analyse réajustées de Chiapello, et ainsi constituer notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Chapitre 5 : Le système de contrôle de l'espionnage industriel

Les chapitres précédents éclaircissent le cheminement emprunté pour élaborer notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, de l'état de l'art de l'espionnage industriel passant par la détermination d'un cadre théorique à la construction d'un modèle théorique de gestion de l'espionnage industriel.

Comme énoncé dans les parties précédentes, l'objectif de notre première étude sur le terrain était d'explorer le processus de contrôle de l'espionnage industriel dans les organisations. Les résultats de ces études ont révélé des vides de gestion, qui ont redirigé l'objectif vers l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

A partir de notre modèle théorique de gestion de l'espionnage industriel[95], qui montre que le processus de contrôle de l'espionnage industriel peut être appréhendé par les leviers de contrôle diagnostic et interactif, nous avons déterminé les outils et méthodes desdits leviers de contrôle dans le chapitre précédent.

Cependant, le modèle théorique stipule que les dimensions d'analyse réajustées de Chiapello permettent de clarifier la mise en application des différents outils et méthodes des deux leviers de contrôle dans l'organisation.

Pour ce faire, nous avons revisité les dimensions d'analyse de Chiapello, en les orientant vers l'analyse des outils des leviers de contrôle[96].

Une présentation du système de contrôle, après une explicitation de ses outils et méthodes au travers des six dimensions d'analyse réajustées de Chiappello, permettrait d'avoir une vue d'ensemble dudit système.

Une fois le système construit, une deuxième vague d'entretiens sera effectuée pour évaluer la pertinence du système construit. Les résultats de cette étude seront interprétés et discutés pour davantage améliorer le processus de contrôle de l'espionnage industriel.

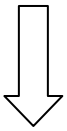
Ainsi, ce chapitre se scinde en deux sections :

[95]Modèle théorique présenté dans le deuxième chapitre.
[96]Voir tableau des six dimensions d'analyse de Chiapello réadaptées à l'analyse des outils des systèmes de contrôle dans le deuxième chapitre, p128.

- la première section fait l'objet d'une présentation de notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion ;
- dans la seconde section, nous allons interpréter et discuter les résultats de la deuxième vague d'entretiens.

L'architecture du chapitre est la suivante :

Section 1 **Le système de contrôle : les outils des leviers de contrôle diagnostic et interactif de l'espionnage industriel via les six dimensions d'analyse réajustées de Chiapello**	
Panorama du système de contrôle de l'espionnage industriel par la fonction contrôle de gestion	Les outils du système de contrôle à la grille d'analyse des six dimensions réajustées de Chiapello



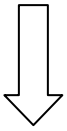
Section 2 **Les enseignements de la deuxième vague d'entretiens**	
Les résultats de la deuxième vague d'entretiens	Discussion des résultats

Section 1 : Le système de contrôle : les outils des leviers de contrôle diagnostic et interactif de l'espionnage industriel *via* les six dimensions d'analyse réajustées de Chiapello

Cette section se scinde en deux sous-sections : la première sous-section fait l'objet de la présentation du panorama de notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion ; et la deuxième sous-section est consacrée à l'explicitation des outils du système de contrôle à la grille d'analyse des six dimensions réajustées de Chiapello.

L'architecture de la section est la suivante :

Panorama du système de contrôle de l'espionnage industriel par la fonction contrôle de gestion



Les outils du système de contrôle à la grille d'analyse des six dimensions réajustées de Chiapello

1. Panorama du système de contrôle de l'espionnage industriel par la fonction contrôle de gestion

Les outils des leviers de contrôle diagnostic et interactif nécessaires au contrôle de l'espionnage industriel par la fonction contrôle de gestion ont été déterminés via les réajustements de certains outils classiques (budget, tableau de bord, etc.), le recours à d'autres outils plus adaptés (méthodes d'évaluation des coûts cachés) et certains outils ayant déjà les caractéristiques adéquates à l'appréhension de l'espionnage industriel (les outils du système de contrôle interactif).

Ainsi, l'objectif de cette sous-section est de finaliser le système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, en le structurant et en exposant sur un plan managérial son utilisation dans l'organisation.

Pour ce faire, nous allons présenter les différents outils des leviers de contrôle diagnostic et interactif de l'espionnage industriel à travers les six dimensions d'analyse réajustées de Chiapello.

Ces dimensions d'analyse, qui définissent les personnes à intervenir, l'attitude du contrôlé, les moyens de contrôle, les moments du contrôle, les processus de contrôle et sur quoi s'exerce le contrôle, permettront, avec les réajustements effectués, d'opérationnaliser sur un plan pratique les systèmes de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Nous allons utiliser les six dimensions de Chiapello sous une vision différente de sa vision initiale, car en plus de sa capacité d'analyse des modes de contrôle, nous estimons que lesdites dimensions d'analyse revisitées ont la capacité de définir concrètement la mise en œuvre d'un système de contrôle dans l'organisation. Cette présomption s'explique par les caractéristiques éclairantes des éléments desdites dimensions : les moments du contrôle, sur quoi s'exerce le contrôle, les moyens du contrôle…

L'idée consiste à utiliser lesdites dimensions réajustées sur les outils des leviers de contrôle, pour détailler et décortiquer suffisamment les étapes des systèmes de contrôle utilisés dans le cadre de cette recherche.

Nous avons déjà présenté dans le deuxième chapitre les six dimensions d'analyse réadaptées à l'analyse des outils des systèmes de contrôle, à savoir :

- Qui utilise cet outil ?
- Sur quoi s'utilise cet outil ?
- Quelle est l'attitude de l'utilisateur de cet outil ou du contrôlé ?
- Quand utilise-t-on cet outil ?
- Quels sont les processus (étapes) d'utilisation de cet outil ?
- Quels sont les moyens d'utilisation de cet outil ?

Ce processus scinde individuellement les deux systèmes de contrôle en six dimensions, et permet de spécifier les différentes étapes nécessaires à leur mise en œuvre dans l'organisation.

Sur un plan managérial, ça facilite la planification, l'organisation et la coordination des tâches, c'est-à-dire que ça permet aux managers de l'organisation de mieux cerner et se situer sur les travaux à effectuer dans le cadre du processus de contrôle de l'espionnage industriel.

Le tableau suivant constitue notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion mettant en interaction les types de figures, les leviers de contrôle diagnostic / interactif et leurs outils, et les six dimensions d'analyse réajustées de Chiapello :

Tableau 26 : Panorama du système de contrôle de l'espionnage industriel par la fonction contrôle de gestion

Figures du processus de contrôle de l'espionnage industriel	**Systèmes de contrôle**	**Outils**		**Les six dimensions réajustées de Chiapello**					
				D1 : Qui utilise cet outil ?	**D2 :** Sur quoi s'utilise cet outil ?	**D3 :** Quelle est l'attitude de l'utilisateur de cet outil ou du contrôlé ?	**D4 :** Quand utilise-t-on cet outil ?	**D5 :** Quels sont les processus (étapes) d'utilisation de cet outil ?	**D6 :** Quels sont les moyens d'utilisation de cet outil ?
Figures imposées	Diagnostic	Structuration en centres de responsabilité réajustée							
		Système budgétaire	Budget réajusté						
			Contrôle budgétaire						
		Tableau de bord réajusté							
		Comptabilité de gestion	Méthodes classiques de calcul des coûts						
			Méthodes d'évaluation des coûts cachés						
Figures libres	Interactif	Débat, dialogue, réunion, discussion, réflexion collective, etc.							

Ce premier tableau du système de contrôle de l'espionnage industriel par la fonction contrôle de gestion est une représentation synthétique qui met en interaction :

- les deux figures (imposées et libres) qui caractérisent le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion ;
- les deux leviers de contrôle (diagnostic et interactif) qui permettent d'appréhender lesdites figures ;
- les outils des deux leviers de contrôle qui ont été déterminés pour cerner les deux figures du processus de contrôle de l'espionnage industriel ;
- les six dimensions d'analyse réajustées de Chiapello.

2. Les outils du système de contrôle à la grille d'analyse des six dimensions réajustées de Chiapello

L'objectif de cette deuxième sous-section est de détailler chaque outil du système de contrôle de l'espionnage industriel à la grille d'analyse des six dimensions réajustées, pour une meilleure mise en œuvre dans l'organisation.

Les tableaux suivants constituent les détails d'utilisation des outils du système de contrôle de l'espionnage industriel sur un plan opérationnel, au travers d'une confrontation entre lesdits outils et les six dimensions réajustées de Chiapello.

Tableau 27 : La structuration en centres de responsabilité et le système budgétaire à la grille d'analyse des six dimensions réajustées de Chiapello

	Structuration en centres de responsabilité réajustée	Système budgétaire	
		Budget réajusté	Contrôle budgétaire
D1	La hiérarchie fonctionnelle suprême (par exemple la direction générale) et le contrôleur de gestion.	Le contrôleur de gestion et les responsables des centres de responsabilité.	Le contrôleur de gestion.
D2	Les objectifs et stratégies ; la répartition des responsabilités.	Les actions à mener.	Les résultats.
D3	Relation instrumentale à l'instar d'Etzioni (1971) : c'est une attitude évaluative et la relation est fondée sur le calcul, c'est-à-dire une dépendance liée aux récompenses permettant un accroissement du bien-être du contrôlé (même relation pour l'utilisateur).	Relation instrumentale.	Relation instrumentale.
D4	Avant l'action, à l'instar des trois phases de Bouquin (1991).	Avant l'action.	Au cours de l'action ; Après l'action.
D5	L'outil intervient dans la répartition en centres de responsabilité via la définition des objectifs clairs et cohérents visant le processus de contrôle de l'espionnage industriel.	Ce sont les étapes de construction du budget des charges de l'espionnage industriel (cf. section 1 du chapitre 4).	Cela consiste à analyser l'écart entre les données budgétées et les données réelles (tâches conférées au contrôleur de gestion).
D6	La sensibilisation des responsables vis-à-vis du processus de contrôle de l'espionnage industriel.	La coopération de tous les responsables de l'organisation (la construction des budgets doit se faire via des concertations collectives).	La coopération de tous les responsables de l'organisation (notamment mettre les données réelles à la disposition du contrôleur de gestion).

Le tableau ci-dessus est un passage de deux outils du système construit (structuration en centres de responsabilité et le système budgétaire) à la grille d'analyse des six dimensions réajustées.

Cette analyse précise les éléments incontournables, qui interviennent dans la gestion de l'espionnage industriel dans l'organisation, à savoir :

- les personnes qui les utilisent ;
- les éléments ciblés par lesdits outils ;
- le type de relation que prône l'utilisation desdits outils ;
- la période d'intervention desdits outils ;
- la précision des étapes d'utilisation desdits outils ;
- les éléments indispensables à l'utilisation desdits outils.

Nous estimons que cette analyse facilite largement la mise en application de notre système de contrôle de l'espionnage industriel dans les organisations.

Le tableau suivant détaille l'analyse de deux autres outils du système : le tableau de bord réajusté et la comptabilité de gestion.

Tableau 28 : Le tableau de bord réajusté et la comptabilité de gestion à la grille d'analyse des six dimensions réajustées de Chiapello

	Tableau de bord réajusté	Comptabilité de gestion	
		Méthodes classiques de calcul de coûts	Méthodes d'évaluation des coûts cachés
D1	Le contrôleur de gestion et les responsables des centres de responsabilité.	Le contrôleur de gestion.	Le contrôleur de gestion.
D2	Les actions ; les résultats.	Les résultats.	Les résultats.
D3	Relation instrumentale.	Relation instrumentale.	Relation instrumentale.
D4	Au cours de l'action.	Après l'action.	Après l'action.
D5	Il s'agit d'utiliser un tableau de bord adapté au contrôle de l'espionnage industriel (cf. section 1 du chapitre 4), via le contrôle périodique des indicateurs par les responsables des centres de responsabilité et le contrôleur de gestion.	Ce sont les étapes des méthodes classiques de calcul des coûts (coûts complets, etc.), pour évaluer les coûts visibles de l'espionnage industriel.	Il s'agit des étapes d'évaluation des coûts invisibles de l'espionnage industriel via les méthodes d'évaluation des coûts cachés (cf. section 1 du chapitre 4).
D6	La coopération des responsables et du contrôleur de gestion (via une communication imminente des variations des indicateurs).	La coopération des responsables (communiquer les charges de prévention et de protection au contrôleur de gestion).	La coopération de l'ensemble du personnel (faciliter la détection des coûts dilués dans les éléments de coût pour le contrôleur de gestion) ; les outils de gestion (brainstorming, Pareto, etc.) pour identifier les variables impactées par l'espionnage industriel.

Le tableau ci-haut explicite les mêmes éléments de compréhension sur l'utilisation concrète, à travers les six dimensions réajustées, de deux autres outils du système (le tableau de bord réajusté et la comptabilité de gestion) dans l'organisation.

Nous nous retrouverons également avec une analyse détaillée de l'utilisation des deux outils dans l'organisation, comme :

- les personnes qui les utilisent ;
- les éléments ciblés par lesdits outils ;
- le type de relation que prône l'utilisation desdits outils ;
- la période d'intervention desdits outils ;
- la précision des étapes d'utilisation desdits outils ;
- les éléments indispensables à l'utilisation desdits outils.

Le tableau suivant explicite l'analyse des différents outils du levier de contrôle interactif de notre système de contrôle de l'espionnage industriel.

Tableau 29 : Les outils du levier de contrôle interactif à la grille d'analyse des six dimensions réajustées de Chiapello

	Débat, dialogue, réunion, discussion, réflexion collective, etc.
D1	La hiérarchie fonctionnelle suprême (par exemple la direction générale) et les subordonnés hiérarchiques (direction de division, les responsables des centres de responsabilité, etc.).
D2	Ces différents outils sont utilisés pour prévenir les incertitudes stratégiques. Par conséquent, ils impactent les objectifs et stratégies de l'organisation.
D3	Relation instrumentale.
D4	Avant l'action ; Au cours de l'action ; Après l'action.
D5	il s'agit d'impliquer l'ensemble du personnel de l'organisation, au travers d'une concertation constante formellement ou informellement (débat, dialogue, réunion, brainstorming, discussion, etc.), dans la recherche d'informations pertinentes pour non seulement détecter les failles qui subsistent dans les stratégies mises en place, mais aussi prévenir les variables d'incertitudes stratégiques, en se démarquant de la concurrence et en assurant sa pérennité.
D6	Les moyens indispensables à l'utilisation de ces outils sont la coopération de tout le personnel de l'organisation, notamment par l'apport des informations pertinentes qui aideront la direction hiérarchique suprême (direction générale) et les subordonnés hiérarchiques (responsables de division ou des centres de responsabilité) à améliorer ou à adapter les stratégies préalablement définies.

Ce dernier tableau met en exergue les modalités d'utilisation des outils du levier de contrôle interactif de notre système dans l'organisation. Il spécifie les mêmes éléments, qui permettent de comprendre l'utilisation managériale, à travers les six dimensions réajustées, des outils du levier de contrôle interactif dans l'organisation.

Nous nous retrouverons également avec une analyse détaillée de l'utilisation des différents outils interactifs dans l'organisation, comme :

- les personnes qui les utilisent ;
- les éléments ciblés par lesdits outils ;
- le type de relation que prône l'utilisation desdits outils ;
- la période d'intervention desdits outils ;
- la précision des étapes d'utilisation desdits outils ;
- les éléments indispensables à l'utilisation desdits outils.

Conclusion

Dans cette section, nous avons exposé, dans une optique de compréhension d'une mise en application concrète, les outils de notre système de contrôle, à travers les six dimensions d'analyse réajustées de Chiapello.

Pour ce faire, nous avons présenté dans un premier tableau une vue d'ensemble synthétique de notre système, qui met en interaction :

- les figures imposées et les figures libres du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion ;
- les leviers de contrôle diagnostic et interactif appréhendant lesdites figures ;
- les outils des deux leviers de contrôle cernant les deux figures du processus de contrôle de l'espionnage industriel ;
- les six dimensions d'analyse réajustées de Chiapello, qui ont décortiqué et explicité l'utilisation des outils de notre système dans l'organisation.

Ensuite, nous avons exposé les différents outils de notre système à la grille des six dimensions réajustées de Chiapello dans trois autres tableaux. Ainsi, nous avons spécifié pour chaque outil :

- la (ou les) personne(s) qui l'utilise(nt) ;
- les éléments ciblés par ledit outil ;
- le type de relation que prône l'utilisation dudit outil ;
- la période d'intervention dudit outil ;
- la précision des étapes d'utilisation dudit outil.

L'étape suivante va consister à soumettre notre système à un échantillon, dans le cadre d'une étude qualitative via des entretiens semi-directifs, afin d'étudier sa pertinence et d'y apporter des améliorations. Cet échantillon se compose principalement des experts universitaires en contrôle de gestion et des contrôleurs de gestion professionnels dans les organisations.

Section 2 : les enseignements de la deuxième vague d'entretiens

Cette section est consacrée à la présentation des résultats des entretiens, que nous avons menés dans le cadre de l'évaluation de notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Les enseignements de cette deuxième étude mettent en lumière la pertinence du système de contrôle de l'espionnage industriel, et permettent de réfuter ou d'approuver notre modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion[97].

Certes, un test sur le terrain est le meilleur moyen de mettre en exergue la pertinence d'un tel système, mais nous avons procédé ainsi pour deux raisons :

- d'un côté, nous avons jugé nécessaire de récolter en amont les suggestions des spécialistes pour mieux consolider le système, en l'améliorant avec l'apport des spécialistes ou experts du contrôle de gestion ;

- d'un autre côté, une étude sur l'espionnage industriel est extrêmement sensible et les entreprises sont très réticentes, quant au test d'un tel système sans étude préalable auprès des spécialistes.

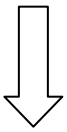
Il est évident que la finalité de cette étude vise une mise à l'épreuve du système de contrôle dans les organisations. Cependant, les raisons évoquées ci-haut et d'autres contraintes[98] nous amènent à évaluer ledit système de contrôle auprès de l'échantillon défini (professionnels et universitaires).

[97]Le modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion est explicité et présenté dans le deuxième chapitre.
[98]Ces contraintes sont liées à la réalisation du travail de recherche dans un temps imparti (c'est une thèse).

Ainsi, nous allons présenter les résultats de la deuxième vague d'entretiens dans une première sous-section (1), et discuter des résultats dans la deuxième sous-section (2).

L'architecture de la section est la suivante :

Les résultats de la deuxième vague d'entretiens



Discussion des résultats

1. Les résultats de la deuxième vague d'entretiens

Les résultats de cette deuxième vague d'entretiens sont issus de la synthèse des données de six entretiens semi-directifs menés avec les spécialistes de notre échantillon. Les différentes données collectées ont été analysées et interprétées comme celles de la première vague d'entretiens.

Les différentes personnes interviewées ont émis leurs avis sur le système de contrôle élaboré, et elles ont également proposé certaines pistes d'amélioration. Nous avons choisi de présenter les résultats par catégorie de spécialistes, à savoir les professionnels d'un côté et les universitaires d'un autre côté. Ce choix est effectué dans le but de visualiser les arguments des deux catégories de spécialistes.

Il est intéressant de confronter les deux visions des spécialistes de notre échantillon, pour tirer une leçon de leurs points de divergence et de convergence.

Les deux tableaux ci-dessous constituent respectivement une présentation succincte des résultats des différents entretiens menés avec les professionnels et les universitaires dans le cadre de cette deuxième vague d'entretiens.

Tableau 30 : Les résultats de l'évaluation du système de contrôle de l'espionnage industriel par la fonction contrôle de gestion « professionnels »

	Objectif de l'étude	Personnes interviewées	Résultats des professionnels
2ème Vague d'entretiens	Evaluer la pertinence du système construit et récolter des suggestions, afin d'apporter les améliorations nécessaires	- Contrôleur de gestion d'un site industriel (Entreprise privée) - Responsable du service financier, budget et contrôle de gestion (Organisation publique) - Directeur d'un site industriel (Entreprise privée)	• L'espionnage industriel est nuisible avec un risque majeur ; • La démarche de construction du système est bien structurée (de la définition des objectifs à l'application des outils) ; • Structurer l'usage de certains outils à cause de la difficile quantification des coûts de l'espionnage industriel, notamment le cadre du brainstorming (pour avoir des coûts assez probants) • Des outils pertinents (surtout les méthodes d'évaluation des coûts cachés pour quantifier les coûts de l'espionnage industriel) • L'implication de tous les employés et une bonne communication sont indispensables à la réussite d'un tel système dans l'organisation • Un système intégré est préférable à un système isolé • Préconisation d'un test dans l'organisation

Tableau 31 : Les résultats de l'évaluation du système de contrôle de l'espionnage industriel par la fonction contrôle de gestion « universitaires »

	Objectif de l'étude	Personnes interviewées	Résultats des universitaires
2ème Vague d'entretiens	Evaluer la pertinence du système construit et récolter des suggestions, afin d'apporter les améliorations nécessaires	- Maître de conférences - HDR contrôle de gestion (Université) - Professeur émérite - HDR comptabilité et contrôle de gestion (Organisme dédié à la formation professionnelle et à la recherche) - Professeur - HDR comptabilité et contrôle de gestion (Université)	• L'espionnage industriel est nuisible avec un risque majeur • La démarche de construction du système est bien structurée (de la définition des objectifs à l'application des outils) • Sujet très large (se concentrer sur un type d'espionnage) • Voir du côté du contrôle interne pour mieux cerner l'espionnage industriel • Sujet trop restreint (il faut élargir le sujet et passer à la fonction sureté pour l'appréhension de l'espionnage industriel) • Des outils pertinents (surtout les méthodes d'évaluation des coûts cachés pour quantifier les coûts de l'espionnage industriel) • L'implication de tous les employés et une bonne communication sont indispensables à la réussite d'un tel système dans l'organisation • Préconisation d'un test dans l'organisation

2. Discussion des résultats

Partant de la revue de littérature, qui présentait peu de travaux scientifiques sur le concept d'espionnage industriel, nous avons voulu explorer dans un premier temps le processus de contrôle de l'espionnage industriel dans les organisations, au travers des entretiens semi-directifs.

Les premiers résultats ont relevé des « trous ou vides » de gestion de l'espionnage industriel dans ces organisations. Ainsi, nous avons redirigé l'objectif de la recherche, en construisant un modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Ce modèle théorique nous a permis d'élaborer un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Dans un second temps, nous avons soumis ce système de contrôle à l'évaluation des spécialistes professionnels et universitaires, au travers des entretiens semi-directifs.

Les résultats de cette deuxième vague d'entretiens présentent des points positifs et des points à améliorer. L'analyse des données de cette étude révèle, selon les avis majoritaires des personnes interviewées, que le système de contrôle de l'espionnage industriel par la fonction contrôle de gestion semble pertinent avec une bonne démarche de construction et de structuration dudit système (de la définition des objectifs à l'application des outils).

Les outils du système semblent pertinents et appréciés, surtout le recours aux méthodes d'évaluation des coûts cachés pour quantifier les coûts de l'espionnage industriel. Cette première analyse montre également la pertinence de notre modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion, qui a permis l'élaboration dudit système.

Le modèle théorique, qui est inspiré des caractéristiques du contrôle de gestion environnemental, de la comptabilité environnementale et des coûts et performances cachés, montre bien que la fonction contrôle de gestion permet de cerner des phénomènes spécifiques (qui échappent aux aptitudes d'appréhension de ses outils classiques), en effectuant des réajustements sur lesdits outils et en ayant recours à certains outils de gestion.

D’un autre côté, certaines personnes universitaires interviewées trouvent l’angle d’attaque trop large ou trop restreint. Ces personnes évoquent la fonction « contrôle interne » et la fonction « sureté » dans les organisations, comme des alternatives plus probantes.

Sans toutefois contester ces remarques pertinentes, nous estimons que la fonction contrôle de gestion est à mieux sujette de combler les « trous ou vides » de gestion de l’espionnage industriel relevés lors de la première vague d’entretiens, qui ont mené à l’élaboration d’un système de contrôle de l’espionnage industriel (issu d’un modèle théorique préalablement construit).

Nous évoquons tout de même qu'il faut être extrêmement prudent dans la généralisation des résultats à l'ensemble des spécialistes professionnels et universitaires, sachant que les personnes interviewées dans le cadre de cette recherche n'ont pas été sélectionnées fortuitement, ce qui rend probablement discutable sa validité externe.

Cependant, les résultats de cette étude montrent bien qu’un test dans l’organisation est faisable, comme le suggèrent les différentes personnes interviewées. Nous en déduisons que l’élaboration du système de contrôle de l’espionnage industriel par la fonction contrôle de gestion est effective, même si celui-ci s’inscrit dans une logique dynamique avec des améliorations possibles.

Conclusion du chapitre 5

L'objectif de ce chapitre était de présenter, d'un côté notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, et d'un autre côté les enseignements de la deuxième vague d'entretiens, dont l'objectif était l'évaluation de la pertinence dudit système de contrôle.

Dans la première section de ce chapitre, nous avons présenté un panorama de notre système de contrôle mettant en interaction les types de figures, les leviers de contrôle diagnostic / interactif et leurs outils, et les six dimensions d'analyse réajustées de Chiapello. Cette présentation a été suivie d'une explicitation, au travers des six dimensions d'analyse réajustées de Chiapello, de l'instrumentation desdits outils dans les organisations.

Ainsi, nous avons détaillé pour chaque outil : la (ou les) personne(s) qui l'utilise(nt) ; les éléments ciblés par ledit outil ; le type de relation que prône l'utilisation dudit outil ; la période d'intervention dudit outil ; et la précision des étapes d'utilisation dudit outil.

Dans la deuxième section, nous avons exposé les résultats de la deuxième vague d'entretiens. Cette exposition a été suivie d'une discussion desdits résultats. Ainsi, les résultats de cette étude montrent bien qu'une expérimentation dans l'organisation est réalisable. Même si notre étude ne constitue point une exhaustivité en soi, elle montre néanmoins la pertinence du modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion et le système de contrôle résultant.

Les répercussions d'un tel système sur la fonction contrôle de gestion peuvent être nombreuses. Cependant, nous allons évoquer les répercussions dudit système sur deux points : notre travail de recherche, étant focalisé sur l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion et la facilitation de son instrumentation dans les organisations, il est intéressant de mettre en exergue les impacts sur le processus et les outils du contrôle de gestion.

Le contrôle de gestion est structuré par un processus, qui permet de visualiser ses étapes d'intervention. Selon Löning et al. (2008), ce processus est une « *boucle qui suppose l'apprentissage par itérations* ». Selon les mêmes auteurs, ce processus, couramment mis en application, correspond au *Plan, Do, Check, Act* de Deming et Gogue (1988) :

- le « Plan » comprend la fixation d'objectifs, la planification et le budget ;
- le « Do » correspond à la mise en œuvre ;
- le « Check » est le suivi des réalisations ;
- « Act[99] » correspond à l'analyse des résultats et la prise d'actions correctives.

Löning et al. (2013) affirment que « *la phase de planification (de la fixation d'objectifs au budget) doit prendre en compte l'environnement et les phénomènes extérieurs (plus ou moins prévisibles) et évoluer de la planification vers la simulation anticipatrice ; la phase de mise en œuvre est soumise de facto à l'environnement et doit rester suffisamment souple pour s'adapter ; le suivi des réalisations et leur analyse ne peuvent plus être menés sans référentiel externe ni sans compréhension de ce qui s'est passé non seulement à l'intérieur mais aussi à l'extérieur de l'entreprise* »[100].

Avec nos différents réajustements sur les outils fondamentaux du contrôle de gestion, le recours aux méthodes d'évaluation des coûts cachés et la détermination des outils interactifs, nous avons élaboré un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, qui entre dans le cadre de l'affirmation ci-dessus.

Nous avons élaboré un système de contrôle en fonction de ce processus, qui tient compte de toutes les étapes de contrôle (avant, pendant et après l'action). Par conséquent, les répercussions sur le processus semblent insignifiantes, car ce sont les mêmes étapes (de la fixation d'objectifs à la prise d'actions correctives).

Quant aux répercussions dudit système sur les outils du contrôle de gestion, elles sont visibles et constituent un apport managérial considérable. Nous avons déjà démontré que les outils classiques du contrôle de gestion ne possédaient pas les aptitudes nécessaires pour appréhender l'espionnage industriel (car c'est un phénomène hors marché).

L'adaptation des outils classiques du contrôle de gestion s'est révélée nécessaire pour cerner le processus de contrôle de l'espionnage industriel. Partant de la pluralité de ses outils et méthodes, ne pouvant guère nous permettre d'effectuer une étude exhaustive, nous avons opté

[99] « Act » est devenu « Analyse » avec les mêmes significations (changement effectué par les mêmes auteurs en 2013).
[100] Löning, H., Malleret, V., Méric, J., & Pesqueux, Y. (2013). *Contrôle de gestion-4e éd: Des outils de gestion aux pratiques organisationnelles*. Dunod, p.13.

pour la détermination des outils fondamentaux du contrôle de gestion et d'y effectuer des réajustements, afin d'appréhender les figures imposées du processus de contrôle de l'espionnage industriel.

Cependant, certains outils fondamentaux du contrôle de gestion nécessitaient juste des réajustements mineurs pour appréhender le phénomène, il s'agit notamment du tableau de bord, qui est un véritable « outil caméléon », des outils et méthodes du levier de contrôle interactif (appréhendant les figures libres du processus de contrôle de l'espionnage industriel).

Par ailleurs, d'autres outils ne permettaient point de cerner la gestion de l'espionnage industriel. Il s'agit des méthodes classiques de calcul des coûts du contrôle de gestion, qui ne peuvent évaluer les coûts invisibles du phénomène. Ce qui justifie l'intervention des méthodes d'évaluation des coûts cachés, qui nous semblent parfaites pour évaluer les coûts invisibles de l'espionnage industriel. Nous avons explicité la manière, dont ces méthodes permettent d'évaluer les coûts de l'espionnage industriel.

Ces réajustements ont accru les aptitudes d'appréhension des outils fondamentaux du contrôle de gestion. Par conséquent, nous sommes face à un élargissement des dimensions d'appréhension des outils du contrôle de gestion.

CONCLUSION GENERALE

Au terme de ce travail, nous allons présenter dans un premier point, une synthèse globale et succincte de l'ensemble des étapes de recherche ; ensuite nous évoquerons dans un deuxième point, les apports sur un plan scientifique, sur un plan managérial et sur un plan méthodologique ; le troisième point fera l'objet d'une énonciation des limites du travail de recherche ; et le quatrième point sera consacré aux perspectives de recherche.

Synthèse globale

Le principal objectif de ce travail de recherche est l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Nonobstant, l'objectif intermédiaire a été d'explorer un processus de contrôle de l'espionnage industriel dans les organisations.

Le travail de recherche a commencé par une revue de littérature sur le concept d'espionnage industriel, qui a malheureusement montré le désintérêt des scientifiques sur le sujet[101], malgré les nombreuses conséquences néfastes du fléau sur les économies et les entreprises.

Cet état de l'art nous a permis de clarifier le concept, en le caractérisant et en précisant le périmètre de délimitation entre l'espionnage industriel et ses concepts connexes (notamment l'intelligence économique, qui demeure le concept le plus proche). Nous nous inscrivons dans une posture défensive de protection contre l'espionnage industriel, c'est-à-dire dans la recherche de solutions de gestion empêchant les espions de nuire. Ce qui exclut de notre travail de recherche toute solution offensive.

La revue de littérature a, certes, révélé des outils et moyens de protection juridiques à la disposition des entreprises, mais ils ont montré des limites. En renfort, les entreprises se protègent par des outils et moyens techniques, qui ont également montré des limites de gestion.

Partant de ce constat, nous avons voulu investiguer sur le sujet, au travers d'une première vague d'entretiens semi-directifs, dans l'objectif d'explorer le processus de contrôle de l'espionnage industriel dans les organisations. Cette première étude, ne constituant guère une exhaustivité en soi, a débouché sur des résultats montrant des vides de gestion appréhensibles par la fonction contrôle de gestion.

[101] Au vu des rares études, articles et communications scientifiques sur l'espionnage industriel.

Ces premiers enseignements empiriques ont redirigé vers l'objectif principal de cette recherche, à savoir l'élaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Une fois le système construit, une évaluation de sa pertinence fera l'objet d'une deuxième étude de terrain, ce qui justifie notre démarche hypothético-inductive, qui se traduit par des allers et retours entre le terrain et la littérature théorique.

Notre recherche s'inscrit dans une démarche qualitative, car les données à recueillir sont des informations et des données non numériques (des mots) des acteurs ou des documents étudiés. L'interprétativisme est la posture épistémologique de notre recherche, car notre processus de création de connaissance passe par la compréhension du sens que les acteurs donnent à la réalité, comme le soulignent Perret et Séville (2007).

Ces différents choix s'articulent bien avec notre objet de recherche. En fonction du sujet et du type de données, nous avons défini les caractéristiques de notre échantillon. L'entretien semi-directif et la documentation nous ont permis de collecter des données, qui ont ensuite été analysées et traitées par la méthode d'analyse de contenu.

L'espionnage industriel est un sujet occulte, par conséquent les informations et données qui touchent ce phénomène sont difficilement accessibles. Cela peut être une source d'explication de la réticence des entreprises à accueillir un chercheur traitant le sujet. D'autant plus que notre sujet est sensible et novateur.

L'espionnage industriel est un sujet peu traité dans la littérature scientifique, par conséquent il n'existe pas de cadre d'analyse pour le concept. De ce fait, nous nous sommes adossés sur des éléments présentant des caractéristiques communes avec notre objet de recherche, il s'agit du contrôle de gestion environnemental, de la comptabilité environnementale et des coûts et performances cachés.

Partant de ces éléments de référence, nous avons pu nous inspirer du cadre théorique du contrôle de gestion environnemental, pour déterminer un cadre théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

A cet effet, nous avons mobilisé les travaux de Simons (1995) et bien d'autres auteurs comme : Acquier (2008), Schaltegger et Burritt (2010), Schaltegger (2011), Antheaume (2013), Renaud (2013, 2015), pour démontrer 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.

Cette mobilisation des concepts et théories a permis la construction d'un modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion, qui met en interaction les figures imposées / libres, les leviers de contrôle diagnostic / interactif et leurs outils, et les six dimensions d'un mode de contrôle réajustées de Chiapello.

Ce modèle théorique a ensuite permis l'élaboration de notre système de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Pour ce faire, nous avons commencé par la détermination des outils des leviers de contrôle diagnostic et interactif.

En ce qui concerne le levier de contrôle diagnostic, nous avons démontré dans notre raisonnement l'incapacité des outils classiques du contrôle de gestion à appréhender l'espionnage industriel dans leur état (car ce sont des outils qui ont pour vocation de cerner les phénomènes et processus de marché).

Par conséquent, des réajustements ont été nécessaires pour amplifier les aptitudes des outils classiques du contrôle de gestion. Par ailleurs, les méthodes d'évaluation des coûts et performances cachés présentent certaines caractéristiques, qui leur mettent en première ligne pour l'évaluation des coûts de l'espionnage industriel. Quant au levier de contrôle interactif, il s'agissait de déterminer les outils permettant de cerner les incertitudes stratégiques liées à l'espionnage industriel.

Dans un souci d'une bonne mise en application des outils des deux leviers de contrôle dans les organisations, ils sont passés à la grille des six dimensions d'analyse revisitées de Chiapello, pour permettre aux managers de l'organisation de mieux cerner et se situer sur les travaux à effectuer dans le cadre du processus de contrôle de l'espionnage industriel. Tous ces éléments ont contribué à l'élaboration dudit système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

A cet effet, une deuxième vague d'entretiens semi-directifs a été effectuée pour évaluer la pertinence dudit système auprès des spécialistes professionnels et universitaires du contrôle de gestion.

Les résultats de cette deuxième vague d'entretiens montrent que le système de contrôle de l'espionnage industriel par la fonction contrôle de gestion semble pertinent avec une bonne

démarche de construction et de structuration dudit système (de la définition des objectifs à l'application des outils).

Les outils du système semblent pertinents et appréciés, surtout le recours aux méthodes d'évaluation des coûts cachés pour quantifier les coûts de l'espionnage industriel. Ce qui montre implicitement la pertinence de notre modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion, qui a permis l'élaboration dudit système.

Tout cela corrobore la capacité de la fonction contrôle de gestion à cerner des phénomènes spécifiques (qui échappent aux aptitudes d'appréhension de ses outils classiques), si nous effectuons des réajustements sur lesdits outils et en ayant recours à certains outils de gestion.

Cependant, certaines personnes interviewées ont trouvé l'angle d'attaque trop large ou trop restreint. Ces personnes évoquent la fonction « contrôle interne » et la fonction « sureté » dans les organisations, comme des alternatives plus probantes.

Sans toutefois négliger ces remarques pertinentes, ni évoquer la généralisation des résultats à l'ensemble des spécialistes professionnels et universitaires, nous estimons que la fonction contrôle de gestion est plus apte à corriger les « trous ou vides » de gestion de l'espionnage industriel relevés lors de la première vague d'entretiens.

Ainsi, les résultats de cette étude montrent bien qu'un test dans l'organisation est faisable, comme le suggèrent les différentes personnes interviewées. Nous en déduisons que l'élaboration du système de contrôle de l'espionnage industriel par la fonction contrôle de gestion est effective, même si celui-ci s'inscrit dans une logique dynamique avec des améliorations possibles.

Apports :

Nous estimons que ce travail de recherche a certains apports sur le plan scientifique, sur le plan managérial et sur le plan méthodologique.

Sur un plan scientifique :

- Clarification d'un périmètre de délimitation entre l'espionnage industriel et ses concepts connexes (notamment l'intelligence économique) : nous estimons avoir apporté un éclaircissement sur les limites de distinction entre l'espionnage industriel et l'intelligence économique (qui demeure le concept le plus proche).

- Mobilisation de plusieurs concepts, dont le contrôle de gestion environnemental, la comptabilité environnementale et les coûts et performances cachés, pour définir un cadre d'analyse du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion : nous avons démontré que ce processus se caractérise par la gestion des figures imposées et des figures libres, qui s'appréhendent par les leviers de contrôle diagnostic et interactif de Simons. L'espionnage industriel est un sujet peu traité scientifiquement, par conséquent mobiliser plusieurs concepts (ayant certaines caractéristiques communes) a contribué à l'appréhension du phénomène. Cela constitue un nouveau regard sur le sujet.

- Détermination d'un modèle théorique de gestion de l'espionnage industriel par la fonction contrôle de gestion : il semble que les outils du contrôle de gestion ne puissent appréhender l'espionnage industriel que de manière limitée, nous avons défini des outils permettant d'appréhender le phénomène à toutes les étapes de contrôle (avant, pendant et après l'action). Le modèle est, certes, basé sur la mobilisation de plusieurs concepts, mais il constitue une nouveauté pour cerner la gestion de l'espionnage industriel par la fonction contrôle de gestion dans les organisations.

- Elargissement de la frontière du contrôle de gestion : ce travail de recherche constitue en soi un élargissement de la frontière du contrôle de gestion, car la fonction ne pouvait appréhender, en l'état actuel de ses outils, le processus de contrôle de l'espionnage industriel. Cela démontre la capacité de la fonction contrôle de gestion à cerner des phénomènes spécifiques (qui échappent aux aptitudes d'appréhension de ses outils classiques), par des réajustements sur lesdits outils et en ayant recours à certains outils de gestion. Notre travail de recherche corrobore cet aspect.

Sur un plan managérial :

- Pilotage des outils et méthodes de protection contre l'espionnage industriel : nous avons défini les fonctionnalités de notre système de pilotage des moyens et outils de protection de l'espionnage industriel. Ce système de pilotage permettra de combler un vide de gestion dans les organisations.

- Un outil d'évaluation des coûts de l'espionnage industriel : nous estimons avoir proposé un outil de mesure des coûts de l'espionnage industriel.

- La protection des compétences et des informations sensibles : ce système de contrôle de l'espionnage industriel par la fonction contrôle de gestion anticipe le vol ou l'expropriation dépourvue d'éthique des informations secrètes et des compétences de l'organisation. Par conséquent, il constitue une barrière de protection pour les organisations.

- Garder son avantage concurrentiel : l'objectif premier de ce système, étant de cerner le processus de contrôle l'espionnage industriel dans les organisations, nous estimons qu'il permettra à celles-ci de se protéger efficacement contre le phénomène et ainsi garder son avantage compétitif.

- Garantir sa réputation auprès des parties prenantes : une organisation bien protégée contre l'espionnage industriel ne peut qu'accroître sa légitimité vis-à-vis de ses parties prenantes.

Sur un plan méthodologique :

Un itinéraire basé sur un aller-retour entre terrain et théories : l'itinéraire de la recherche a été un aller-retour entre terrain et théories, pour élaborer un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Notre échantillon est diversifié et englobe des spécialistes universitaires et professionnels. Cela permet d'avoir les avis et opinions des chercheurs sur un plan théorique et ceux des professionnels sur un plan pratique. Cet agencement constitue une originalité de notre travail de recherche sur le sujet du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Limites :

Une des principales limites de ce travail de recherche est l'absence d'un test dudit système de contrôle sur le terrain, comme il a été également signalé par les différentes personnes interviewées lors de la deuxième vague d'entretiens.

En effet, il est indéniable qu'une expérimentation de ce système de contrôle dans les organisations permettrait d'évaluer concrètement sa pertinence. Les outils définis seraient mis à l'épreuve dans un environnement aussi fluctuant qu'incertain. Les points forts et les points faibles auraient été mis à découvert, pour davantage améliorer le système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Cependant, ce travail de recherche est une thèse s'effectuant dans un temps imparti. Or, une expérimentation de ce système de contrôle pourrait s'allonger sur une ou plusieurs années. Par conséquent, nous avons opté pour le recueil des suggestions et points d'amélioration des spécialistes professionnels et universitaires.

Une autre limite de ce travail de recherche est le petit nombre d'entretiens effectués dans les deux vagues d'entretiens (dix entretiens semi-directifs), même si c'est une méthode qualitative se nourrissant des données non numériques. Ce qui rend la validité externe de cette étude discutable.

Les entreprises ont majoritairement montré une réticence, quant à l'accueil d'un chercheur traitant un sujet sur « l'espionnage industriel ». Nous avons eu énormément de difficultés à nouer une relation avec les organisations. Le sujet est sensible et peut également signifier une mauvaise gestion au sein de l'organisation. Par conséquent, rares sont les organisations qui se prêtent à l'étude.

Cependant, les données collectées ont enrichi le travail de recherche, d'autant plus que les personnes interviewées sont des spécialistes de leur domaine. Etant donné que notre processus de création de connaissance se conforme à une posture épistémologique spécifique, c'est-à-dire sur la compréhension du sens que les acteurs donnent à la réalité (l'interprétativisme), cela crédibilise davantage le travail de recherche.

Toutefois, nous n'évoquons guère une généralisation, sachant que les enseignements que nous tirons de ce travail de recherche ne prétendent aucunement à un statut de loi, ni de règle (plusieurs conditions et expérimentations sont nécessaires à cet effet).

Perspectives :

Les différentes limites citées ci-haut constituent des pistes de recherche, pour approfondir la question du processus de contrôle de l'espionnage industriel.

Une des perspectives incontournables de cette étude s'enregistre dans un cadre de mise en application dudit système de contrôle dans les organisations. Sachant qu'une expérimentation d'un système de contrôle dans les organisations fournit une preuve étayée, il serait intéressant d'élargir notre recherche par la réalisation des études au sein des organisations, pour mettre en exergue les points forts et les points faibles dudit système de contrôle.

D’un autre côté, il serait intéressant d’étudier une expérimentation de notre système contrôle de l’espionnage industriel par la fonction contrôle de gestion dans une grande entreprise, dans une moyenne entreprise et dans une petite entreprise. Une confrontation des différents résultats nous apprendrait davantage sur la pertinence dudit système de contrôle.

BIBLIOGRAPHIE

Abderrahim, N. (2015). *L'intelligence économique et ses répercussions sur le contrôle de gestion (Cas des EPE de la wilaya de Tlemcen)* (Doctoral dissertation).

Acquier, A. (2008, May). Développement durable et management stratégique: piloter un processus de transformation de la valeur. In *Actes de la 17e Conférence Internationale de l'AIMS*.

Aggeri, F., Pezet, E., Abrassart, C., & Acquier, A. (2005). *Organiser le développement durable : Expériences des entreprises pionnières et formation de règles d'action collective* (p. 278). Paris : Vuibert.

Alcouffe, S., Boitier, M., Rivière, A., & Villesèque-Dubus, F. (2013). *Contrôle de gestion interactif: Commercial. Supply Chain. RH. Environnement*. Dunod.

Alcouffe, S., Boitier, M., Rivière, A., & Villesèque-Dubus, F. (2013). *Contrôle de gestion sur mesure: Industrie, grande distribution, banque, secteur public, culture*. Dunod.

Alexandre-Leclair, L. (2001). La sûreté économique comme stratégie de contre intelligence économique. In *Veille stratégique scientifique et technologique. Colloque* (Vol 2 pp. 123 - 134).

Allard-Poesi, F., Maréchal, G. (2007). Construction de l'objet de la recherche. In *Méthodes de recherche en management* (Dir. Thietart, R.-A.). Paris, Dunod, pp. 34-57.

Allard-Poesi, F., & Maréchal, G. (2014). *Construction de l'objet de la recherche* (No. hal-01123768).

Andreani, E. (1967). Le coût d'opportunité. *Revue économique*, vol. 18, no 5, p. 840-858.

Antheaume, N. (2012, May). Essai sur la spécificité du contrôle de gestion environnemental. In *Comptabilités et innovation*.

Antheaume, N. (2001, May). La diffusion volontaire d'informations environnementales: le cas de la Cogema. In *22ÈME CONGRES DE L'AFC*.

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

Antheaume, N., & Christophe, B. (2005). *La comptabilité environnementale: des outils pour évaluer la performance écologique, E-theque. com*. ISBN 2-7496-0099-5.

Anthens G. H. (Sept. 21, 1998). Lotsa Talk, Little Walk. *Computer World*, pp. 70-75.

Anthony, R. N. (1965). *Planning and Control Systems: A Framework for Analysis [by]*. Division of Research, Graduate School of Business Administration, Harvard University.

Anthony, R. N. (1988). *The management control function*. Harvard Business School Press.

Arjaliès, D. L., Goubet, C., & Ponssard, J. P. (2011). Approches stratégiques des émissions CO2. *Revue française de gestion*, (6), 123-146.

Asseman, A. (2009). Vol et fuites de données : le cas interne. Note de recherche N°3. Chaire de recherche du Canada en sécurité, identité et technologie de l'Université de Montréal, 16p.

Augé, B., & Naro, G. (2011). *Mini manuel de contrôle de gestion*. Dunod.

Barry R. S. (1998). Economic espionage. *Marketing Management*, 7 (1), 56-58.

Bartolomeo, M., Bennett, M., Bouma, J. J., Heydkamp, P., James, P., & Wolters, T. (2000). Environmental management accounting in Europe : current practice and future potential. *European Accounting Review*, *9* (1), 31-52.

Baud, J. (1998) Encyclopédie du renseignement et des services secrets. Lavauzelle, Paris.

Berland, N. (1999). A quoi sert le contrôle budgétaire ? *Finance Contrôle Stratégie*, *2* (3), 5-24.

Berland, N. (2014). *Le contrôle de gestion : «Que sais-je?» n° 3977*. Presses universitaires de France.

Berland, N., & De Rongé, Y. (2013). *Contrôle de gestion: Perspectives stratégiques et managériales*. Pearson Education France.

Berland, N., & Simon, F. X. (2011). *Le contrôle de gestion en mouvement: Etat de l'art et meilleures pratiques-Regards croisés de professeurs et praticiens*. Editions Eyrolles.

Besson B. et Possin J.C. (1996). Du renseignement à l'intelligence économique. Editions Dunod, Paris.

Boulanger, P. M. (2004). Les indicateurs de développement durable: un défi scientifique, un enjeu démocratique. *Les séminaires de l'Iddri*, *12*, 24.

Bouquin, H. (1991). Contrôle de gestion : le temps réel implique un retour aux sources. *Revue Française de gestion*, 17-26.

Bouquin, H. (1994). *Les fondements du contrôle de gestion*. Presses universitaires de France.

Bouquin, H. (2011). *Les fondements du contrôle de gestion : «Que sais-je ?» n° 2892*. Presses universitaires de France.

Bouquin, H. & Kuszla, C. (2014). *Le contrôle de gestion*. 10ème édition, Presses universitaires de France.

Bouquin, H., & Pesqueux, Y. (1999). Vingt ans de contrôle de gestion ou le passage d'une technique à une discipline. *Comptabilité-Contrôle-Audit*, *5*(3), 93-105.

Bourguignon, A., & Jenkins, A. (2004). Changer d'outils de contrôle de gestion? De la cohérence instrumentale à la cohérence psychologique. *Finance Contrôle Stratégie*, *7*(3), 31-61.

Bouroubi, M. (2014). L'intelligence économique / de la pratique au concept : Une étude conceptuelle sur l'intelligence économique et les concepts en relation. *Les cahiers du mecas*, *10*(1), 42-55.

Bournois, F., Romani, P. J., & Pierret, C. (2000). L'intelligence économique et stratégique dans les entreprises françaises.

Bouyeure, C. (2009). Guide des bonnes pratiques en matière d'intelligence économique. *Ministère de l'Economie, de l'Industrie et de l'Emploi, France*.

Breillat, J. (2010). L'intelligence économique en PME/PMI : De l'intention stratégique au bricolage de l'informel. *Communication présentée dans la journée d'IE et gouvernance stratégique des entreprises, ENSIAS, Rabat*, *3*.

Bruté De Rémur, D. (2016). Intelligence économique et pôles de compétitivité. VA Press Editions.

Bruté De Rémur, D. (2006). *Ce que intelligence économique veut dire*. Éditions d'Organisation.

Bruté De Rémur, D. (2009). Point de vue : pour une épistémologie de l'IE. *Revue internationale d'intelligence économique*, 1(1), 9-11.

Bulinge, F. (2010). Renseignement militaire : une approche épistémologique. *Revue internationale d'intelligence économique*, *2*(2), 209-232.

Bulinge, F., & Pepin, J. F. (2013). Intelligence économique: l'information au cœur de l'entreprise. Editions Nuvis.

Bulinge, F. (1992). *Pour une culture de l'information dans les petites et moyennes organisations: un modèle incrémental d'intelligence économique* (Doctoral dissertation, Université de Toulon et du Var).

Burlaud, A. & Simon, C. (2013). *Le contrôle de gestion*. 3ème édition. La Découverte.

Burritt, R. L., Hahn, T., & Schaltegger, S. (2002). Towards a comprehensive framework for environmental management accounting—Links between business actors and environmental management accounting tools. *Australian Accounting Review*, *12*(27), 39-50.

Burritt, R. L., & Saka, C. (2006). Environmental management accounting applications and eco-efficiency : case studies from Japan. *Journal of Cleaner Production*, *14*(14), 1262-1275.

Callot, P. (2006). Intelligence Economique et PME. *La Revue des Sciences de Gestion*, (2), 61-71.

Carayon, B. (2003). Intelligence économique, compétitivité et cohésion sociale, rapport remis au Premier Ministre. *France*. La Documentation française, 176 p.

Carlton, S. A. (1992). Industrial espionage: reality of the information age. *Research-Technology Management*, *35*(6), 18-24.

Caron, M. A., Boisvert, H., & Mersereau, A. (2007, May). La comptabilité de management environnementale ou l'écocontrôle : utilité des outils de contrôle de gestion. In *«comptabilité et environnement»*.

Chiapello, È. (1996). Les typologies des modes de contrôle et leurs facteurs de contingence : un essai d'organisation de la littérature. *Comptabilité-contrôle-audit*, *2*(2), 51-74.

Christophe, B. (1989). Comptabilité et environnement. *Prise en compte des activités environnementales dans les documents financiers des entreprises. Doctorat en sciences de gestion. Paris: Université Paris*, *12*.

Christophe, B. (1992). L'expert comptable face à la comptabilité environnementale. *Revue Française de Comptabilité*, *235*, 51-57.

Cohen, C. (2007). Intelligence et Performance mesurer l'efficacité de l'Intelligence Economique et Stratégique (IES) et son impact sur la Performance de l'Organisation. *Vie & sciences de l'entreprise*, (1), 15-50.

Coissard, S., Delhalle, L., & Seiglie, C. (2010). Guerre économique et sécurité internationale. *Revue internationale d'intelligence économique*, *2*(2), 233-250.

Collins, J. M. (2005). *Preventing identity theft in your business: how to protect your business, customers, and employees*. John Wiley & Sons.

Comai, A. (2003). Global code of ethics and competitive intelligence purposes: an ethical perspective on competitors. *Journal of Competitive Intelligence and Management*, *1*(3).

Commission européenne (novembre 2013). La Commission propose des règles pour la protection du secret d'affaires. Date de mise à jour : 19/2/2018. Consulté le 09/08/2018. Disponible sur : http://europa.eu/rapid/press-release_IP-13-1176_fr.htm?locale=fr.

Continuity Central Archive (décembre 2011). How to detect and stop corporate espionage. Date de mise à jour 2/12/2011. Consulté le 9/8/2018. Disponible sur : http://www.continuitycentral.com/feature0938.html.

Corbel, P. (2006). Hypercompétition, rentes et brevet. *La Revue des Sciences de Gestion*, (2), 45-51.

Coskun Samli, A., & Jacobs, L. (2003). Counteracting global industrial espionage : a damage control strategy. *Business and society review*, *108*(1), 95-113.

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

Curtis, J. (2001). Behind enemy lines. Marketing, 24 May Donaldson-Briggs, A.L. (2001) Competitive intelligence and industrial espionage. Consulté le 21/11/2018. Disponible sur : http://www.managementfirst. com/articles/espionage.htm.

Dambrin, C., & Löning, H. (2008). Systèmes de contrôle interactifs et théories de l'apprentissage : une relecture des travaux de R. Simons à l'aune des théories piagétiennes. *Comptabilité-Contrôle-Audit*, *14*(3), 113-140.

De La Villarmois, O., & Stéphan, O. (2005). Quand l'outil de diagnostic devient interactif. *L'Expansion Management Review*, (4), 60-65.

De Rongé, Y., & Cerrada, K. (2012). *Contrôle de gestion*. Pearson Education France.

Delbecque, É., & Harbulot, C. (2011). Les formes de la guerre économique. *Que sais-je?* 42-80.

Delmas, M. A. (2002). The diffusion of environmental management standards in Europe and in the United States : an institutional perspective. *Policy Sciences*, *35*(1), 91-119.

Deming, W. E., & Gogue, J. M. (1988). *Qualité : la révolution du management*. Economica.

Diversified Risk Management Inc. (2014). Industrial Espionage Prevention, Investigation and Awareness. Disponible sur : http://www.diversifiedriskmanagement.com/workshops/esp.

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

Dorbaire, P., Chen, G., & Chen, M. (2012). Le contrôle stratégique des Instituts Confucius. *Management & Avenir*, (5), 272-290.

Dreveton, B. (2009). Les outils de contrôle de gestion à l'épreuve de la RSE. Le cas de l'organisation publique. *Revue de l'organisation responsable*, *4*(2), 30-44.

Dumenil M. (2014). *Le contrôle de gestion : 200 questions sur le pilotage, la stratégie, l'analyse des coûts.* GERESO Edition.

Dupré, J. (2001). Espionnage économique et droit : l'inutile création d'un bien informationnel. Consulté le 21/11/2018. Disponible sur : https://www.lex-electronica.org/files/sites/103/7-1_dupre.pdf.

Dupuis, J-C. *(2011).* Le management responsable. *Revue française de gestion*, (6), 69-85.

Enterprise Risk Management, Inc. (2008). Fighting Corporate Espionage Starts with the Basics. Consulté le 24/11/2018. Disponible sur :

https://www.bloomberg.com/profiles/companies/1024777D:US-enterprise-risk-management-inc.

Essid, M., & Berland, N. (2011). Les impacts de la RSE sur les systèmes de contrôle. *Comptabilité-Contrôle-Audit*, *17*(2), 59-88.

Evrad Samuel, K. (1998). Les freins à l'intelligence économique dans la culture française. *Revue d'intelligence économique*, (2).

Executive, C. (1996). Annual Report to Congress on Foreign Economic Collection and Industrial Espionage 1996.

Frantz J. (2014). La protection des secrets d'affaires dans l'Union européenne : 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, 41p.

Gavard-Perret, M. L., Gotteland, D., & Haon, C. (2012). *Méthodologie de la recherche : réussir son mémoire ou sa thèse en sciences de gestion*. Pearson.

Gervais, M. (2009). *Contrôle de gestion*, 9ème édition, Economica.

Gibert, P. (2002). L'analyse de politique à la rescousse du management public ? Ou la nécessaire hybridation de deux approches que tout, sauf l'essentiel, sépare. *Politiques et management public*, *20*(1), 1-14.

Giraud, F. (2009). *L'art du contrôle de gestion: Enjeux et pratiques*. Gualino.

Giraud, F. (2011). *Les fondamentaux du contrôle de gestion: principes et outils*. Pearson.

Gond, J. P., & Igalens, J. (2012). *Manager la responsabilité sociale de l'entreprise*. Pearson Education France.

Gotteland, D., Haon, C., & Jolibert, A. (2012). *Méthodologie de la recherche en sciences de gestion : réussir son mémoire ou sa thèse*. Pearson Education France.

Grandguillot, B. (2013). *L'essentiel du contrôle de gestion 2013*. Gualino éditeur.

Gray, R. (1992). Accounting and environmentalism : an exploration of the challenge of gently accounting for accountability, transparency and sustainability. *Accounting, Organizations and Society*, *17*(5), 399-425.

Gray, R. (2000). Current developments and trends in social and environmental auditing, reporting and attestation : a review and comment. *International journal of auditing*, *4*(3), 247-268.

Gray, R. (2002). The social accounting project and Accounting Organizations and Society Privileging engagement, imaginings, new accountings and pragmatism over critique?. *Accounting, organizations and society*, *27*(7), 687-708.

Gray, R. (2010). Is accounting for sustainability actually accounting for sustainability… and how would we know ? An exploration of narratives of organisations and the planet. *Accounting, organizations and society*, *35*(1), 47-62.

Gray, R., Owen, D., & Adams, C. (1996). *Accounting & accountability : changes and challenges in corporate social and environmental reporting*. Prentice Hall.

Green, D. I. (1894). Pain-cost and opportunity-cost. *The Quarterly Journal of Economics*, *8*(2), 218-229.

Greenberg, L., & Barling, J. (1996). Employee theft. *Trends in organizational behavior*, *3*, 49-64.

Guarnieri, F., & Przyswa, E. (2009). Cybercriminalité-contrefaçon : les interactions entre « réel et virtuel ». *Revue internationale de droit économique*, vol. *23 n*°1, p.12.

Halligan, R. M. (2008). Protection of US Trade Secret Assets : Critical Amendments to the Economic Espionage Act of 1996, 7 J. Marshall Rev. Intell. Prop. L. 656 (2008). *The John Marshall Review of Intellectual Property Law*, *7*(4), 2.

Harbulot, C., & Baumard, P. (1997). Perspective historique de l'intelligence économique. *Intelligence économique*, *1*, 1-17.

Hejazi, W., Lefort, A., Etges, R., & Sapiro, B. (2011). The 2009 Rotman-TELUS Joint Study on IT Security Best Practices: Compared to the United States, How Well is the Canadian Industry Doing ? In *Corporate Hacking and Technology-Driven Crime : Social Dynamics and Implications* (pp. 228-265). IGI Global.

Henri, J. F. (2006). Management control systems and strategy : A resource-based perspective. *Accounting, organizations and society*, *31*(6), 52.

Henri, J.-F., & Journeault, M. (2010). Eco-control : The influence of management control systems on environmental and economic performance. *Accounting, Organizations and Society* 35 (1) : 63-80.

Hopwood, A. G. (1974). Leadership climate and the use of accounting data in performance evaluation. *The Accounting Review*, *49*(3), 485-495.

House, W. (février 2013). Administration strategy on mitigating the theft of US trade secrets. Disponible en version PDF sur : https://www.justice.gov/criminal-ccips/file/938321/download.

House, W. (1995). Annual Report to Congress on Foreign Economic Collection and Industrial Espionage. *Washington, DC: Government Printing Office*.

Igalens, J., Joras, M., & Manenc, B. (2013). La sûreté éthique. Du concept à l'audit opérationnel. *Sécurité et stratégie*, *15*(4), 76-78.

Incident Management Group (2012). 10 Strategies for Preventing Corporate Espionage, Disponible sur : http://www.imgsecurity.net/10-strategies-for-preventing-corporateespionage/.

Juillet, A. (2013). L'éthique et la sécurité sont-elles conciliables ? *Sécurité et stratégie*, *15*(4), 1-3.

Juillet, A. (2005). Référentiel de formation en intelligence économique. *Secrétariat général de la défense nationale*.

Juillet, A. (2004). Intelligence économique ou renseignement. *Du renseignement à l'intelligence économique, paru dans : revue Défense Nationale*.

Kalitka, P. F. (2000). Do They Know What You Know ? *Security Management*, *44*.

Lamberton, G. (2005, March). Sustainability accounting—a brief history and conceptual framework. In *Accounting Forum* (Vol. 29, No. 1, pp. 7-26). Elsevier.

Larivet, S. (2001, June). Intelligence économique : acception française et multidimensionnalité. In *10th Conference of AIMS, Laval, Quebec Larivet S. & Brouard F. (2007). Faire de l 'intelligence économique au quotidien : application à la gestion des réclamations, Market Management* (Vol. 8, No. 4, pp. 5-25).

Lauriol, J. (2004). Le développement durable à la recherche d'un corps de doctrine. *Revue française de gestion*, (5), 137-150.

Lepori, E., & Bollecker, M. (2015, May). Les leviers de contrôle de SIMONS : vers une compréhension des freins à l'équilibrage diagnostic/interactif. In *Comptabilité, Contrôle et Audit des invisibles, de l'informel et de l'imprévisible*.

Lesca, H. (1997). *Veille stratégique: concepts et démarche de mise en place dans l'entreprise*. Association des professionnels de l'information et de la documentation.

Löning, H., Pesqueux, Y., Chiapello, E., Malleret, V., Méric, J., Michel, D., & Solé, A. (1998). *Le contrôle de gestion* (Vol. 20). Paris : Dunod.

Löning, H., Malleret, V., Méric, J., Pesqueux, Y., Chiapello, E., Michel, D., & Sole, A. (2008). *Le contrôle de gestion-3ème éd.: Organisation, outils et pratiques*. Dunod.

Löning, H., Malleret, V., Méric, J., & Pesqueux, Y. (2013). *Contrôle de gestion-4e éd. : Des outils de gestion aux pratiques organisationnelles*. Dunod.

Lorino, P., Demeestère, R., & Mottis, N. (2013). Pilotage de l'entreprise et contrôle de gestion. *5ème édition, Dunod.*

Lorino, P. (1991). *Le contrôle de gestion stratégique : la gestion par les activités* (Vol. 213). Paris : Dunod.

François, L., Bruté de Rémur, D. & Menguy, N. (2009). Éditorial : Trois dimensions de l'intelligence économique. *Revue internationale d'intelligence économique*, vol 1, (2), 151-153.

Marcon, C. (2009). Réseaux d'intelligence économique. L'éthique au centre des problématiques organisationnelles. *Revue internationale d'intelligence économique*, *1*(2), 197-211.

Marquet-Pondeville, S. (2003). Le contrôle de gestion environnemental. *Doctorat en sciences de gestion, Louvain: UCL, Presses Universitaires de Louvain*.

Martre, H., Clerc, P., & Harbulot, C. (1994). Intelligence économique et stratégie des entreprises. *Rapport du Commissariat Général au Plan, Paris, La Documentation Française*, volume *17*.

Martinet, A., & Savall, H. (1978). Dysfonctionnements, coûts et performances cachés dans l'entreprise. *Revue d'économie industrielle*, *5*(1), 82-94.

Massé, G., & Thibault, F. (2001). Intelligence économique : un guide pour une économie de l'intelligence. Editions De Boeck Université, Bruxelles.

Mbengue A. (2001), « Posture paradigmatique et recherche en management stratégique », *in Stratégies – Actualités et futurs de la recherche*, sous la dir. D'A.C. Martinet et R.A. Thiétart (Ed.), Vuibert.

Mbengue, A., & Vandangeon-Derumez, I. (1999, May). Positions épistémologiques et outils de recherche en management stratégique. In *communication à la conférence de l'AIMS*, p22.

Memheld, P. (2012). Intelligence économique, déontologie, conformité et anticipation des risques. *Revue internationale d'intelligence économique*, *4*(2), 125-137.

Menuet C. & Boloh Y. (2012). Espionnage industriel. Les PME doivent se protéger. Le journal des entreprises. Consulté le 9/8/2018. Disponible sur : https://www.lejournaldesentreprises.com/maine-et-loire-sarthe/article/espionnage-industriel-les-pme-doivent-se-proteger-59146.

Moinet, N. (2009). L'épistémologie de l'intelligence économique face au défi de la communication. *Revue internationale d'intelligence économique*, *1*(2), 159-173.

Moinet, N. (2010). Petite histoire de l'intelligence économique, une innovation « à la française ». L'harmattan.

Moisdon, J. C., & Hatchuel, A. (1997). Du mode d'existence des outils de gestion. *Actes du séminaire Contradictions et Dynamique des Organisations-CONDOR-IX*, 6.

Mongin, P., & Tognini, F. (2015). *Petit manuel d'intelligence économique au quotidien. 2ème éd. : Comment collecter, analyser, diffuser et protéger son information*. Dunod.

Naef. W. E. (2003). Economic and Industrial Espionage: a Threat to Corporate America. Consulté le 10/8/2018. Disponible sur : http://www.iwar.org.uk/infocon/economic-espionage.htm.

Naro, G. (1998). La dimension humaine du contrôle de gestion : la recherche anglo-saxonne sur les aspects comportementaux de la gestion budgétaire. *Comptabilité-Contrôle-Audit*, *4*(2), 45-69.

Naro, G., & Travaillé, D. (2010). Construire les stratégies avec le Balanced Scorecard : vers une approche interactive du modèle de Kaplan et Norton. *Finance Contrôle Stratégie*, *13*(2), 33-66.

Ng Kwet Shing, M., & Spence, L. J. (2002). Investigating the limits of competitive intelligence gathering : is mystery shopping ethical ? *Business Ethics : A European Review*, *11*(4), 343-353.

Noailly J. (1997). L'espionnage industriel au cœur de la guerre mondiale du renseignement économique, Mémoire de maitrise, p. 87.

Nobre, T., & Zawadski, C. (2015, May). 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*.

Nobre, T. (2001). Méthodes et outils du contrôle de gestion dans les PME. *Finance contrôle stratégie*, *4*(2), 119-148.

Nséké L. (2012). Espionnage industriel : Des coûts importants. Afrique Expansion Magazine. Revue des affaires et des partenariats Nord-Sud. Consulté le 23/11/2018. Disponible sur : https://afriqueexpansionmag.com/.

OCDE (2014). Approaches of protection of undisclosed information (trade secrets). Consulté le 9/8/2018. Disponible en version PDF sur : https://read.oecd-ilibrary.org/trade/approaches-to-protection-of-undisclosed-information-trade-secrets_5jz9z43w0jnw-en#page1. 328p.

Office of the National Conterintelligence Executive (2009-2011). Report to Congress on Foreign Economic Collection and Industrial Espionage. Consulté le 9/8/2018. Disponible sur : https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/20111103_report_fecie.pdf. 31p.

Owen, D., Gray, R., & Maunders, K. (1987). Researching the information content of social responsibility disclosure : a comment. *British Accounting Review*, *19*(2), 169-176.

Payne, H. J. (1971). Model of freeway traffic and control. *Mathematical Model of Public System*, 51-61.

Perret V. et Seville M. (2007), Fondements épistémologiques de la recherche, *in* R.A. Thietart, *Recherche en management*, Dunod, p. 13-33.

Piaget, J. (1967). *L'épistémologie et ses variétés*. In Logique et connaissance scientifique, Enclyclopédie de la Pléiade. Paris : Gallimard, 3-61.

Plane, J. M. (2012). *Théorie et management des organisations-3ème éd*. Dunod.

Ponemon Institute (février 2009). Data Loss Risks During Downsizing : As Employees Exit, so does Corporate Data. White-paper. Consulté le 9/8/2018. Disponible sur : https://fr.slideshare.net/constantk/data-loss-during-downsizing. 40p.

Renaud, A., & Berland, N. (2007, May). Mesure de la performance globale des entreprises. in *«comptabilité et environnement»*.

Renaud, A. (2010, May). Le concept d'interactivité de Simons revisité à l'aune des systèmes de contrôle environnemental. In *Crises et nouvelles problématiques de la Valeur*.

Renaud, A. (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).

Renaud, A. (2014). Le contrôle de gestion environnemental : quels rôles pour le contrôleur de gestion?. *Comptabilité-Contrôle-Audit*, *20*(2), 67-94.

Renaud, A. (2015). *Management et contrôle de gestion environnemental*. Éditions EMS.

Richard, J. (2012). *Comptabilité et développement durable* (No. hal-01651227).

Rouleau, L. (2007). *Théories des organisations : approches classiques, contemporaines et de l'avant-garde*. Puq.

Savall H., Zardet V. (2010). Maîtriser les Coûts et les Performances Cachés. *5ème édition*, Economica.

Savall, H. (1979). Reconstruire l'entreprise: Analyse socio-économique des conditions de travail [Reconstructing the enterprise: Socio-economic analysis of working conditions]. *Paris : Dunod*.

Savall, H., & Zardet, V. (2001, May). Evolution des outils de contrôle et des critères de performance, face aux défis de changement stratégique des entreprises. In *22ème congres de l'AFC*.

Schaltegger, S., & Hahn, T. (2000). Environmental management accounting : Overview and main approaches. *Center for Sustainability Management*.

Schaltegger, S., & Burritt, R. L. (2010). Sustainability accounting for companies : Catchphrase or decision support for business leaders ? *Journal of World Business*, *45*(4), 375-384.

Schaltegger, S. (2011). Sustainabilty Management Control. In *Environmental Management Accounting and Supply Chain Management* (Eds, Burrit, R.L., Schaltegger S., Bennett M., Pohjola, T., Csutora, M.). Dordrecht, Heidelberg, London, New-York : Springer, 337-353.

Shanley, A., & Crabb, C. (1998). Corporate Espionage : No Longer a Hidden Threat. Chemical Engineering, 105 (13), 82-91.

Simons, R. (1987). Accounting control systems and business strategy : an empirical analysis. *Accounting, organizations and society*, *12*(4), 357-374.

Simons, R. (1991). Strategic orientation and top management attention to control systems. *Strategic management journal*, *12*(1), 49-62.

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

Simons, R. (1995). Control in an age of empowerment. *Harvard business review*, 73 (2), 80-88.

Simons, R. (2005). Levers of organization design. *Boston : Harvard Business School Publishing*.

Sponem, S. (2004). Contrôle budgétaire diagnostic ou interactif ? Proposition d'un instrument de mesure. In *25ème congrès de l'Association Francophone de Comptabilité* (pp. 1-20).

Stedman, M. J. (1991). Industrial espionage: what you don't know can hurt you. *Business and Society Review* 76, 25-32.

Teagarden, E. M. (1997). James Bond and George Smiley Go into Business—Teaching about Business Espionage. *Journal of Education for Business*, *72*(4), 250-252.

Terry, G. R., & Franklin, S. G. (1968). *Principles of management*. RD Irwin.

Thiétart, R. A. (2007). *Méthodes de recherche en management. 3ème édition*. Dunod.

Thietart, R. A. *et al* (2014). *Méthodes de recherche en management. 4ème édition*. Dunod.

Thonnard, O., Bilge, L., O'Gorman, G., Kiernan, S., & Lee, M. (2012, September). Industrial espionage and targeted attacks : Understanding the characteristics of an escalating threat. In *International workshop on recent advances in intrusion detection*(pp. 64-85). Springer, Berlin, Heidelberg.

Tuomela, T. S. (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.

Von Glasersfeld, E. (2001). The radical constructivist view of science. *Foundations of science*, *6*(1-3), 31-43.

Wacheux, F. (1996). *Méthodes qualitatives et recherche en gestion*. Economica.

Widner, J. (2007). Constitution writing in post-conflict settings : An overview. *Wm. & Mary L. Rev.*, *49*, 1513.

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

Yin, R. K. (1994). Case Study Research: Design and Methods (Applied Social Research Methods, Vol. 5). *Sage Publications, Beverly Hills, CA. Rick Rantz Leading urban institutions of higher education in the new millennium Leadership & Organization Development Journal*, *23*(8), 2002.

ANNEXES

TABLE DES ANNEXES

Annexe 1. Charte d'éthique du SYNFIE

LES ENGAGEMENTS CI-DESSOUS CONSTITUENT LE CODE DE BONNE CONDUITE DES MEMBRES DE LA PROFESSION ET LEUR RESPECT PERMET A LEUR SIGNATAIRE DE SE PRESENTER EN QUALITE DE « MEMBRE DU SYNFIE ».

ARTICLE 1 – OBJECTIF DE LA CHARTE

1.1. L'intelligence économique se définit comme étant l'activité professionnelle qui vise à collecter, analyser, diffuser et protéger l'information économique stratégique. Outil d'aide à la décision, au profit de l'ensemble des acteurs économiques, elle se décline en plusieurs axes :

- Un volet pédagogique, permettant de former et de sensibiliser les acteurs concernés sur les objectifs et les méthodes de l'intelligence économique ;
- Un volet anticipation, connaissance de l'environnement économique et accompagnement des évolutions, notamment par la pratique de la veille et de la collecte informationnelle et stratégique ;
- Un volet sécurité économique à travers le management et la prévention des risques, notamment immatériels et la protection des renseignements économiques non divulgués (secrets d'affaires) ;
- Un volet travail d'influence, afin de fournir un cadre favorable et nécessaire au développement des acteurs économiques sur les marchés stratégiques.

1.2. Le Syndicat des Professionnels de l'Intelligence Economique (« LE SYNFIE ») a notamment pour vocation et pour objet de fédérer et de regrouper en son sein les professionnels indépendants et/ou salariés dont les activités habituelles relèvent à titre principal ou exclusif de la définition ci-dessus.
Le SYNFIE se donne comme objectif de faire connaître, de promouvoir, de défendre et de représenter la profession auprès des acteurs économiques et/ou étatiques et des institutions.

1.3. La présente convention (ci-après « la Charte ») a pour objet de proposer et de conférer un cadre éthique aux activités professionnelles de ses membres. Chaque adhérent du SYNFIE s'oblige par voie de conséquence à respecter et à faire respecter à ses salariés et représentants les termes et engagements découlant de la présente Charte.

ARTICLE 2 – ENGAGEMENTS DEONTOLOGIQUES DES ADHERENTS

2.1. Tout adhérent du SYNFIE, signataire de la présente charte éthique, déclare solennellement réaliser à titre principal et/ou habituel des activités relevant de la définition visée sous l'article 1.1. et en faire sa profession ou en tirer l'essentiel de ses ressources (en ce compris en qualité de salarié d'une entreprise pour laquelle il effectue des missions relevant de l'article 1).

2.2. Les signataires de la Charte, et les personnes morales, groupements ou institutions qu'ils représentent, s'engagent à n'employer dans le cadre de leurs activités professionnelles d'intelligence économique que des moyens légaux ou qui ne seraient pas contraires aux normes et règles de la profession, et ce en toutes circonstances et quel que soit le lieu de leur pratique.

2.3. Les signataires de la Charte s'interdisent de nuire ou de porter atteinte à l'image de la profession en général et au SYNFIE en particulier.

2.4. En cas de médiatisation ou de communication sur une affaire rendue publique ou dans l'exercice d'un mandat relevant d'une autre institution, le signataire de la Charte s'oblige à indiquer qu'il ne représente en aucune façon le SYNFIE, sauf mandat ou délégation expresse.

ARTICLE 3 – CONFORMITE A L'ORDRE PUBLIC ET A L'INTERÊT SUPERIEUR DE LA NATION

3.1. Les signataires de la Charte s'interdisent expressément de porter atteinte, par quelque moyen ou procédé que ce soit, et quelle que soit la raison, aux intérêts fondamentaux de la nation, tel que définis sous l'article 410-1 du Code pénal. De même, lorsque le client est le représentant d'une entreprise, d'une institution ou d'une autorité étrangère, le signataire de la Charte doit veiller et s'assurer du respect des dispositions de la Loi n°68-538 du 28 juillet 1968, dite « loi de blocage ».

3.2. Pour l'exécution du présent article, il appartient aux signataires de la Charte de veiller et d'informer leur client que la prestation demandée est susceptible de porter atteinte aux intérêts de la nation. Le cas échéant, les signataires de la Charte doivent refuser la mission sollicitée, ou en modifier le périmètre.

ARTICLE 4 – RESPECTS DES ENGAGEMENTS ET DES METHODES

4.1. Les signataires déclarent n'accepter que des missions d'intelligence économique pour lesquelles ils disposent des moyens (le cas échéant des diplômes), de l'expérience, de la formation et des compétences requises pour agir conformément aux pratiques et aux règles de l'art de la profession.

Ils s'engagent à recourir, si nécessaire, aux partenaires et/ou sous-traitants répondant aux qualifications et aux critères de la présente Charte.

4.2. Les signataires de la Charte s'obligent à ne communiquer à leur client que des informations librement accessibles par des moyens légaux. Les renseignements transmis doivent être préalablement recollés, vérifiés et recoupés. Les professionnels de l'intelligence économiques membres du SYNFIE doivent vérifier la fiabilité et la véracité de la source utilisée.

ARTICLE 5 - CONFIDENTIALITE – GESTION DES CONFLITS D'INTERÊT - DISCIPLINE

5.1. Les signataires de la Charte s'obligent à soumettre un contrat écrit à leur client, comprenant notamment la nature de leur mission, et une clause de confidentialité ou de discrétion portant sur les informations susceptibles d'être communiquées par le client ou à destination du client.

5.2. Les signataires de la Charte s'interdisent de travailler pour deux sociétés concurrentes, ou ayant des intérêts divergents, sur des problématiques similaires risquant d'entraîner un conflit d'intérêt. Sauf accord des parties, l'adhérent du SYNFIE s'abstient de réaliser la mission lorsque surgit un conflit d'intérêt ou lorsque la confidentialité risque d'être violée ou lorsque son indépendance risque de ne plus être entière. Il ne peut accepter la mission de la part d'un nouveau client si le secret des informations données par un ancien client risque d'être violé ou lorsque la connaissance des affaires de l'ancien client favoriserait le nouveau.

5.3. Toute infraction constatée aux règles de la profession ou toute méconnaissance des règles et dispositions énoncées par la présente Charte sera soumise à l'appréciation du Comité

d’éthique appelé à statuer et le cas échéant à sanctionner le signataire de la Charte en application de l’article 6 du Règlement intérieur du SYNFIE.

La présente charte a été adoptée par l'Assemblée Générale du SYNFIE le 15 Avril 2014.

Annexe 2. Lettre du premier guide d'entretien

UNIVERSITÉ DE REIMS CHAMPAGNE-ARDENNE

Faculté des Sciences Economiques, Sociales et de Gestion

Reims, le 13 février 2017.

Bonjour,

Doctorant en Sciences de Gestion et rattaché au laboratoire REGARDS à l'Université de Reims Champagne-Ardenne, je sollicite vivement la participation de votre organisation dans cette recherche innovante.

Dans le cadre de ma thèse de doctorat intitulée : « Processus de contrôle de l'espionnage industriel » sous la direction du Professeur MBENGUE Ababacar, je mène une étude scientifique.

L'objectif de l'étude :

L'étude a pour but d'appréhender le processus de contrôle de l'espionnage industriel dans les entreprises en France, à travers les grandes lignes ci-dessous. **Dans le cas échéant, si une telle structure n'est pas mise en place dans votre organisation, les différentes perceptions des professionnels comme vous, nous permettront de construire un modèle de contrôle de l'espionnage industriel.**

Elle vise particulièrement à répondre à la question suivante : « pourquoi et comment contrôler l'espionnage industriel dans les entreprises en France ? ».

Les personnes à interviewer :

L'étude étant qualitative, il apparait nécessaire d'avoir des données qualitatives diversifiées. Par conséquent, 2 responsables des fonctions seront interviewées : le Contrôleur de gestion et 1 autre responsable (par exemple : le Directeur ou le Responsable administratif et financier ou

le Responsable des Ressources humaines ou le Comptable ou le responsable des systèmes d'information…).

Durée de l'entretien :

Le temps de l'entretien par responsable, pour ne pas abuser de votre temps, serait **court**.

Date et lieu de l'entretien :

La date et le lieu de l'entretien **sont à définir à votre convenance**. Par ailleurs, dans un souci d'achèvement de ma thèse dans le temps imparti, je vous serais reconnaissant si l'entretien pouvait se dérouler dans un bref délai.

Je tiens à vous rassurer que l'anonymat sera maintenu à votre convenance et seront divulguées dans la thèse que les informations que vous jugerez diffusables.

En espérant avoir de vos nouvelles, je vous remercie d'avance de votre considération et je reste entièrement à votre disposition pour tout renseignement supplémentaire.

Pièce jointe : Guide d'entretien.

Oumar FANE
06 65 15 25 27
fanos41@yahoo.fr
Doctorant en Sciences de Gestion
Carte d'étudiant N° : 21113891
Laboratoire REGARDS
Université de Reims Champagne-Ardenne.

Annexe 3. Lettre du deuxième guide d'entretien

Reims, le 23 janvier 2018.

Bonjour,

Doctorant en Sciences de Gestion et rattaché au laboratoire REGARDS à l'Université de Reims Champagne-Ardenne, je sollicite vivement votre expertise dans cette recherche innovante.

Dans le cadre de ma thèse de doctorat intitulée « **Elaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion** » sous la direction du Professeur MBENGUE Ababacar, je mène une étude scientifique.

L'objectif de l'étude :

L'objectif de cette recherche est d'élaborer un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

A cet effet, nous avons construit un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion, et nous voudrions le soumettre aux critiques de deux échantillons d'experts, à savoir : les spécialistes universitaires en contrôle de gestion et les contrôleurs de gestion professionnels.

L'étude vise particulièrement à évaluer, au travers des entretiens semi-directifs avec lesdits experts, la pertinence du système construit et à récolter vos suggestions, afin d'apporter les améliorations nécessaires.

Durée de l'entretien :

La durée de l'entretien, pour ne pas abuser de votre temps, **serait courte**.

Date et lieu de l'entretien :

La date et le lieu de l'entretien **sont à définir à votre convenance**. **Je tiens à vous assurer que l'anonymat de vos réponses sera total.**

En espérant avoir une réponse positive, je vous remercie d'avance de votre considération et je reste entièrement à votre disposition pour tout renseignement supplémentaire.

Pièces jointes :

- Guide d'entretien ;
- Modèle théorique et outils du système construit (mentionnant les étapes de construction) ;
- Les outils réajustés du système (exposant les réajustements effectués).

Oumar FANE
06 65 15 25 27
fanos41@yahoo.fr
oumar.fane@etudiant.univ-reims.fr
Doctorant en Sciences de Gestion
Carte d'étudiant N° : 21113891
Laboratoire REGARDS
Université de Reims Champagne-Ardenne.

Modèle théorique et les outils du système de contrôle de l'espionnage industriel

I. Modèle théorique

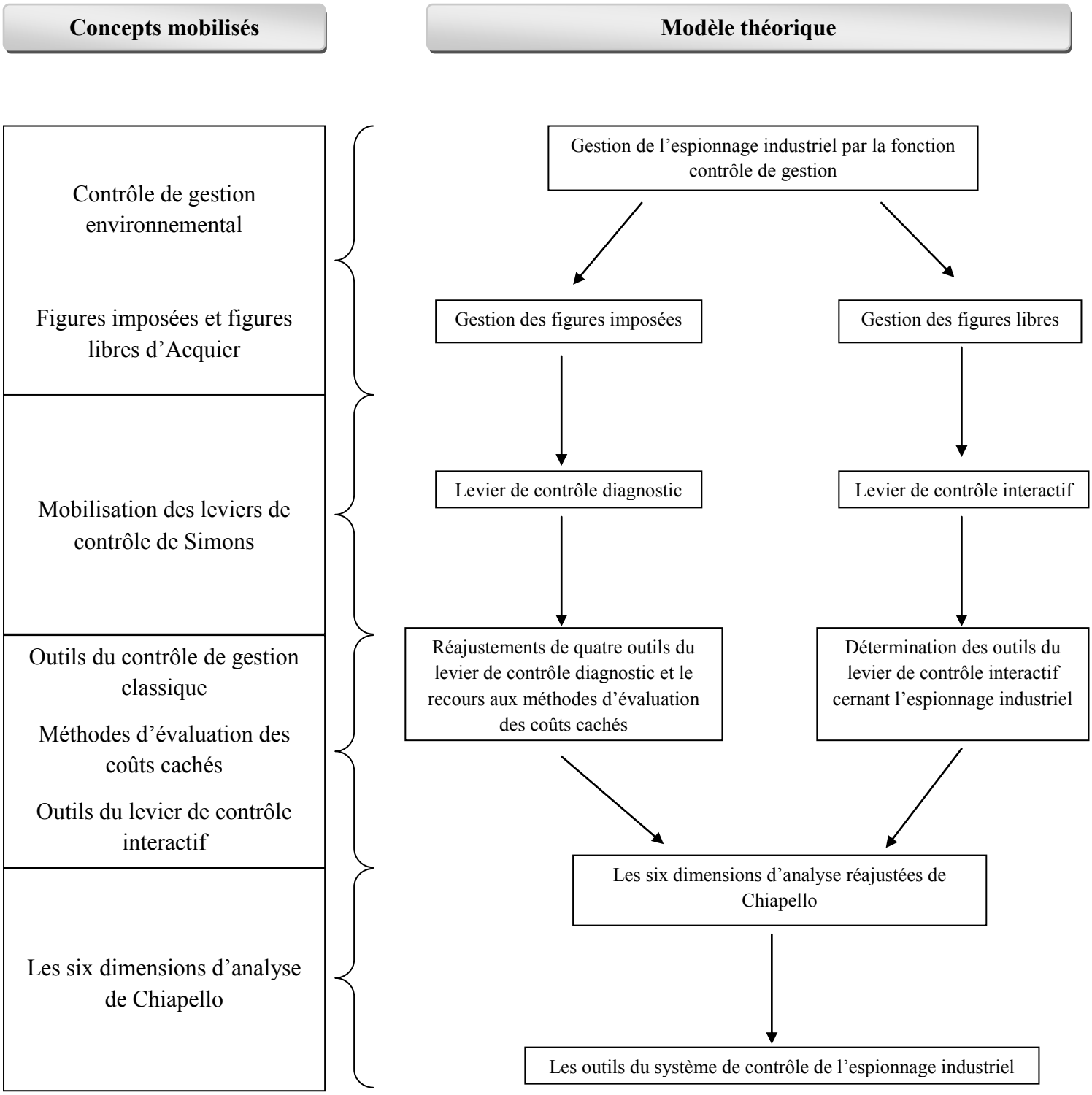
Après une explicitation des concepts du contrôle de gestion environnemental, de la comptabilité environnementale et des coûts cachés, nous avons pu nous inspirer du cadre théorique du contrôle de gestion environnemental, qui constitue sans doute un processus connexe de notre objet de recherche, pour cadrer théoriquement le processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion.

Ainsi, nous avons pu démontrer, à travers les travaux de Simons (1995) et bien d'autres auteurs comme : Acquier (2008), Schaltegger et Burritt (2010), Schaltegger (2011), Antheaume (2013), Renaud (2013, 2015), etc., 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.

Par ailleurs, nous avons démontré l'incapacité des outils classiques du contrôle de gestion à appréhender l'espionnage industriel. De ce fait, il était nécessaire de réajuster certains outils classiques du contrôle de gestion, notamment ses quatre outils fondamentaux, pour cerner l'espionnage industriel (côté diagnostic) et de déterminer les outils appréhendant les incertitudes stratégiques liées à l'espionnage industriel (côté interactif).

Après les réajustements desdits outils, l'ajout d'un outil de calcul des coûts de l'espionnage industriel (méthodes d'évaluation des coûts cachés) et la détermination de quelques outils du levier de contrôle interactif, nous les avons analysés à travers les six dimensions réajustées de Chiapello, dans l'objectif d'exposer sur un plan opérationnel son utilisation dans l'organisation.

Ci-dessous le modèle théorique avec les concepts mobilisés :


Concepts mobilisés
Modèle théorique
Contrôle de gestion environnemental
Figures imposées et figures libres d'Acquier
Mobilisation des leviers de contrôle de Simons
Outils du contrôle de gestion classique
Méthodes d'évaluation des coûts cachés
Outils du levier de contrôle interactif
Les six dimensions d'analyse de Chiapello
Gestion de l'espionnage industriel par la fonction contrôle de gestion
Gestion des figures imposées
Gestion des figures libres
Levier de contrôle diagnostic
Levier de contrôle interactif
Réajustements de quatre outils du levier de contrôle diagnostic et le recours aux méthodes d'évaluation des coûts cachés
Détermination des outils du levier de contrôle interactif cernant l'espionnage industriel
Les six dimensions d'analyse réajustées de Chiapello
Les outils du système de contrôle de l'espionnage industriel

II. Les outils du système de contrôle de l'espionnage industriel

Le modèle construit ci-haut nous a permis de déterminer les outils du système de contrôle de l'espionnage industriel tout en détaillant, sur un plan opérationnel, leur utilisation dans l'entreprise.

Les tableaux ci-après sont :

- le premier tableau est général et contient une représentation synthétique de tous les outils de notre système construit avec les types de figures à appréhender, les leviers de contrôle mobilisés et les six dimensions réajustées de Chiapello ;
- les 3 autres tableaux contiennent les éléments facilitant l'utilisation des outils du système de contrôle de l'espionnage industriel sur un plan opérationnel, au travers d'une confrontation entre lesdits outils et les six dimensions réajustées de Chiapello.

Figures du processus de contrôle de l'espionnage industriel	**Systèmes de contrôle**	**Outils**		**Les six dimensions réajustées de Chiapello**					
				D1 : Qui utilise cet outil ?	**D2 :** Sur quoi s'utilise cet outil ?	**D3 :** Quelle est l'attitude de l'utilisateur de cet outil ou du contrôlé ?	**D4 :** Quand utilise-t-on cet outil ?	**D5 :** Quels sont les processus (étapes) d'utilisation de cet outil ?	**D6 :** Quels sont les moyens d'utilisation de cet outil ?
Figures imposées	Diagnostic	Structuration en centres de responsabilité réajustée							
		Système budgétaire	Budget réajusté						
			Contrôle budgétaire						
		Tableau de bord réajusté							
		Comptabilité de gestion	Méthodes classiques de calcul des coûts						
			Méthodes d'évaluation des coûts cachés						
Figures libres	Interactif	Débat, dialogue, réunion, discussion, réflexion collective, etc.							

	Structuration en centres de responsabilité réajustée	Système budgétaire	
		Budget réajusté	Contrôle budgétaire
D1	La hiérarchie fonctionnelle suprême (par exemple la direction générale) et le contrôleur de gestion.	Le contrôleur de gestion et les responsables des centres de responsabilité.	Le contrôleur de gestion.
D2	Les objectifs et stratégies ; la répartition des responsabilités.	Les actions à mener.	Les résultats.
D3	Relation instrumentale à l'instar d'Etzioni (1971) : c'est une attitude évaluative et la relation est fondée sur le calcul, c'est-à-dire une dépendance liée aux récompenses permettant un accroissement du bien-être du contrôlé (même relation pour l'utilisateur).	Relation instrumentale.	Relation instrumentale.
D4	Avant l'action, à l'instar des trois phases de Bouquin (1991).	Avant l'action.	Au cours de l'action ; Après l'action.
D5	L'outil intervient dans la répartition en centres de responsabilité via la définition des objectifs clairs et cohérents visant le processus de contrôle de l'espionnage industriel.	Ce sont les étapes de construction du budget des charges de l'espionnage industriel (cf. section 2 du même chapitre).	Cela consiste à analyser l'écart entre les données budgétées et les données réelles (tâches conférées au contrôleur de gestion).
D6	La sensibilisation des responsables vis-à-vis du processus de contrôle de l'espionnage industriel.	La coopération de tous les responsables de l'organisation (la construction des budgets doit se faire via des concertations	La coopération de tous les responsables de l'organisation (notamment mettre les données réelles à la disposition du

		collectives).	contrôleur de gestion).

	Tableau de bord réajusté	Comptabilité de gestion	
		Méthodes classiques de calcul de coûts	Méthodes d'évaluation des coûts cachés
D1	Le contrôleur de gestion et les responsables des centres de responsabilité.	Le contrôleur de gestion.	Le contrôleur de gestion.
D2	Les actions ; les résultats.	Les résultats.	Les résultats.
D3	Relation instrumentale.	Relation instrumentale.	Relation instrumentale.
D4	Au cours de l'action.	Après l'action.	Après l'action.
D5	Il s'agit d'utiliser un tableau de bord adapté au contrôle de l'espionnage industriel (cf. section 2 du même chapitre), via le contrôle périodique des indicateurs par les responsables des centres de responsabilité et le contrôleur de gestion.	Ce sont les étapes des méthodes classiques de calcul des coûts (coûts complets, etc.), pour évaluer les coûts visibles de l'espionnage industriel.	Il s'agit des étapes d'évaluation des coûts invisibles de l'espionnage industriel via les méthodes d'évaluation des coûts cachés (cf. section 2 du même chapitre).
D6	La coopération des responsables et du contrôleur de gestion (via une communication imminente des variations des indicateurs).	La coopération des responsables (communiquer les charges de prévention et de protection au contrôleur de gestion).	La coopération de l'ensemble du personnel (faciliter la détection des coûts dilués dans les éléments de coût pour le contrôleur de gestion) ; les outils de gestion (brainstorming, Pareto, etc.) pour identifier les variables impactées par l'espionnage industriel.

	Débat, dialogue, réunion, discussion, réflexion collective, etc.
D1	La hiérarchie fonctionnelle suprême (par exemple la direction générale) et les subordonnés hiérarchiques (direction de division, les responsables des centres de responsabilité, etc.).
D2	Ces différents outils sont utilisés pour prévenir les incertitudes stratégiques. Par conséquent, ils impactent les objectifs et stratégies de l'organisation.
D3	Relation instrumentale.
D4	Avant l'action ; Au cours de l'action ; Après l'action.
D5	il s'agit d'impliquer l'ensemble du personnel de l'organisation, au travers d'une concertation constante formellement ou informellement (débat, dialogue, réunion, brainstorming, discussion, etc.), dans la recherche d'informations pertinentes pour non seulement détecter les failles qui subsistent dans les stratégies mises en place, mais aussi prévenir les variables d'incertitudes stratégiques, en se démarquant de la concurrence et en assurant sa pérennité.
D6	Les moyens indispensables à l'utilisation de ces outils sont la coopération de tout le personnel de l'organisation, notamment par l'apport des informations pertinentes qui aideront la direction hiérarchique suprême (direction générale) et les subordonnés hiérarchiques (responsables de division ou des centres de responsabilité) à améliorer ou à adapter les stratégies préalablement définies.

Les outils du système de contrôle de l'espionnage industriel

I. Les outils du levier de contrôle diagnostic pour cerner les figures imposées de l'espionnage industriel

1. Réajustement de la structuration en centres de responsabilité

L'outil en soi-même ne sera pas remplacé par un autre, par contre son contenu sera réajusté notamment par l'ajout de deux principales actions :

- **la définition des objectifs clairs et cohérents visant le processus de contrôle de l'espionnage industriel ;**
- **la sensibilisation des managers ou responsables vis-à-vis du processus de contrôle de l'espionnage industriel.**

A ce niveau, les deux actions sont des objectifs stratégiques que les managers ou les responsables vont traduire en objectifs opérationnels pour appréhender l'espionnage industriel. En effet, il s'agirait de définir des objectifs prenant en compte l'appréhension de l'espionnage industriel et de sensibiliser les managers ou les responsables à ce qu'ils comprennent les attendus de l'organisation vis-à-vis du phénomène.

2. Réajustement des budgets et du contrôle budgétaire

Habituellement, l'organisation établit ses budgets dans un ordre précis (commençant par les budgets de ventes, ensuite les budgets de production, etc.) sous contraintes de certains facteurs comme les moyens de production, les capacités de ventes… Sachant que tous ces éléments demeurent prévisionnels, cela aboutit aux différents documents de synthèse.

Par contre, l'espionnage industriel n'est pas un produit (ou service) qui se commercialise et génère des profits, mais plutôt un phénomène qui engendre énormément de pertes à l'organisation (allant des pertes de sommes colossales à la faillite de certaines organisations). Ces coûts liés à l'espionnage industriel doivent être anticipés et l'idéal serait que l'organisation empêche la naissance desdits coûts. La difficulté d'appréhension de l'espionnage industriel par les budgets classiques réside à ce niveau, puisque ces derniers sont interdépendants et doivent être bien construits.

Quant aux charges de l'espionnage industriel dans l'organisation, elles peuvent être de deux types : les charges visibles (coûts de prévention, coûts de protection, et autres coûts visibles)

et les charges invisibles (coûts incorporés dans les produits ou services, coûts d'opportunité, autres coûts invisibles). Par ailleurs, budgéter des coûts invisibles, dont la survenance est incertaine, n'est pas une chose facile et ne peut jamais être exhaustif.

Connaissant la structure des coûts de l'espionnage industriel (coûts visibles et invisibles), nous pouvons budgéter ainsi :

<table>
<tr><th colspan="4">Etapes de construction du budget des charges de l'espionnage industriel</th></tr>
<tr><th colspan="2">Charges visibles</th><th colspan="2">Charges invisibles</th></tr>
<tr><td colspan="2">

Déterminer les actions de prévention et de protection du processus de contrôle de l'espionnage industriel ;
Spécifier en quantité les besoins nécessaires à la réalisation des actions définies ;
Chiffrer les éléments de coûts, tout en précisant leur période de survenance (mensuellement, trimestriellement, etc.).

</td><td colspan="2">

attribuer une valeur en fonction des éléments de coûts historiques dus à l'espionnage industriel dans l'organisation ;
ou attribuer une valeur forfaitaire en fonction des coûts moyens relevés des cas d'espionnage industriel dans le secteur, le domaine d'activité, dans la région, etc.

</td></tr>
<tr><td>Charges visibles</td><td>Total = …….</td><td>Charges invisibles</td><td>Total = ……</td></tr>
</table>

Ce contrôle budgétaire se fait de la même manière que celui d'un produit ou service de l'organisation. Néanmoins, quelques petites différences subsistent comme :

- la focalisation est accentuée sur les écarts des coûts de l'espionnage industriel, or pour un produit ou service, les écarts de prix et de quantités sont importants à déterminer (les écarts sur les produits) ;

- ❖ le calcul des coûts réels d'un produit ou service est assez évident, et peut être cerné par les méthodes de calcul classiques du contrôle de gestion (méthodes d'évaluation des coûts complets, des coûts variables, etc.), cependant le calcul des coûts réels de l'espionnage industriel est beaucoup plus complexe et échappe aux aptitudes d'appréhension desdites méthodes classiques.

3. Un tableau de bord adapté au contrôle de l'espionnage industriel

Il consiste à introduire les éléments d'appréhension de l'espionnage industriel dans le tableau de bord de l'organisation, en passant par les mêmes étapes de construction d'un tableau de bord.

Cette prise en compte de l'espionnage industriel passe par les mêmes étapes de construction du tableau de bord de l'organisation, à savoir :

- **définition des objectifs :** il s'agit de **définir clairement, avec cohérence, les objectifs visés qui se rapportent au contrôle de l'espionnage industriel** et ceux-ci doivent être **atteignables** ;
- **détermination des variables d'actions :** à ce niveau, il faut **déterminer les principaux facteurs clés de succès** des objectifs visés se rapportant à l'appréhension de l'espionnage industriel et ces derniers doivent être **contrôlables et mesurables quantitativement et ou qualitativement** ;
- **choix des indicateurs :** suite à la détermination des facteurs clés de succès, **il sera question d'identifier des indicateurs de mesure de la performance représentatifs et pertinents qui demeureront dans le périmètre d'action des responsables** (c'est-à-dire qu'ils ont les moyens et le pouvoir d'agir sur ces éléments leur permettant ainsi d'apporter des actions correctives) ;
- **responsabilisation :** il consiste à **rattacher les différents indicateurs choisis aux responsables ayant les moyens et le pouvoir de pilotage sur ces derniers** ;
- **mise en place d'un système de normes :** il est important d'avoir un **référentiel à atteindre ou à ne pas dépasser pour chaque indicateur** afin que l'atteinte des objectifs soit plus probante ;
- **périodicité :** cette partie se caractérise par **la définition de la périodicité de contrôle des indicateurs choisis**, c'est-à-dire que chaque indicateur est relevé à nouveau à cette échéance.

Le tableau ci-dessous est une illustration des éléments du processus de contrôle de l'espionnage industriel dans un tableau de bord :

Objectifs	Variables d'actions ou facteurs clés de succès	Indicateurs	Responsables	Normes de référence	Périodicité
L'adoption des comportements pour prévenir la survenance de l'espionnage industriel via la sensibilisation du personnel.	Formations Contrôles aléatoires	✓ Pourcentage d'employés formés ✓ Nombre d'anomalies relevées lors du contrôle aléatoire	➢ Responsable des ressources humaines ➢ Contrôleur de gestion	✓ 100% ✓ 0	❖ Trimestrielle ❖ Hebdomadaire
La mise en œuvre de la norme ISO/IEC 27001 management de la sécurité de l'information.	Implication du personnel Adoption des principes élémentaires de la norme	✓ Nombre de réunions avec les employés ✓ Nombre d'exigences non respectées de la norme	➢ Responsable du centre de responsabilité ➢ Responsable du centre de responsabilité et contrôleur de gestion	✓ Au moins 2 ✓ 0	❖ Mensuelle ❖ Mensuelle

4. La comptabilité de gestion

Les coûts visibles et invisibles de l'espionnage industriel ne se calculent pas de la même manière et ne s'appréhendent pas non plus par les mêmes méthodes d'évaluation des coûts.

Pour le calcul des coûts visibles, les méthodes classiques comme les coûts complets peuvent cerner lesdits coûts. Il s'agit de tenir compte de l'ensemble des charges engagées dans la prévention et la protection contre l'espionnage industriel dans l'organisation. Cela se détermine à partir des éléments disponibles tels que : les achats des matériels anti-espionnages, la souscription d'un brevet, les frais de formation, etc.

Quant aux coûts invisibles, ils échappent aux aptitudes d'analyse des outils de calcul classiques du contrôle de gestion se nourrissant principalement des éléments des systèmes d'information de l'organisation. Ainsi, nous allons exposer la méthode d'évaluation des coûts invisibles à travers les méthodes d'évaluation des coûts cachés.

5. Autres méthodes et outils : méthodes des coûts cachés

Les caractéristiques occultes de l'espionnage industriel exigent certains outils et méthodes plus adaptés, c'est le cas de l'évaluation des coûts de l'espionnage industriel. Le plus souvent nous n'appréhendons pas certaines données « invisibles » qui engendrent des coûts imperceptibles et réduisent significativement les performances des organisations. Ces coûts imperceptibles empêchent les organisations d'être efficacement rentables, compétitives et détériorent leur qualité de fonctionnement.

Le tableau suivant est un récapitulatif des étapes d'évaluation des coûts historiques et des coûts d'opportunités de l'espionnage industriel :

***Contribution horaire à la marge sur coût variable », qui se note CHMCV** et se calcule de la façon suivante :

$$*CHMCV = \frac{\text{Marge sur coût variable de l'année}}{\text{Nombre d'heures d'activité de l'année}}$$

Méthodes d'évaluation des coûts invisibles de l'espionnage industriel	
Etapes d'évaluation des coûts historiques (coûts dilués dans les éléments de coût)	**Etapes d'évaluation des coûts d'opportunité**
Mode d'évaluation SOF ou QQFI : **Etape 1 : le module social** • répertorier les actions de prévention, de protection et de réparation concernant l'espionnage industriel ; • rechercher spécifiquement les causes des différentes actions ; • ordonner les causes en catégories ; • faire un Pareto des causes en fonction du nombre d'occurrences par catégorie. **Etape 2 : le module organisationnel** • mettre en liste les actions de prévention, de protection et de réparation qui ont été mises en œuvre ; • chiffrer les impacts des actions mises en œuvre. **Etape 3 : le module financier** • valoriser les coûts de chacune des actions.	**Coûts de non-potentiel stratégique et autres coûts d'opportunité liés au temps perdu à la résolution des problèmes d'espionnage industriel :** **Etape 1 :** déterminer le temps perdu par les employés à la résolution des problèmes d'espionnage industriel (à l'aide d'un brainstorming ou autres outils de gestion) ; **Etape 2 :** calculer le CHMCV* ; **Etape 3 :** évaluer les coûts de non-potentiel stratégique (en multipliant le temps perdu par CHMCV*). **Coûts de non-production et autres coûts d'opportunité liés aux occasions perdues :** **Etape 1 :** identifier les variables de production (ou de profit) impactées par l'espionnage industriel à l'aide d'un Pareto, d'un brainstorming ou autres outils de gestion ; **Etape 2 :** quantifier (historiquement ou de manière prévisionnelle à l'aide des systèmes d'information de l'organisation) ces variables avant la survenance de l'espionnage industriel ; **Etape 3 :** évaluer ces variables après la survenance de l'espionnage industriel ; **Etape 4 :** en déduire les coûts d'opportunité (**variables avant espionnage industriel – variables après espionnage industriel**).

II. Les outils du levier de contrôle interactif pour appréhender les figures libres de l'espionnage industriel

En effet, il s'agit d'impliquer l'ensemble du personnel d'une organisation, au travers d'une concertation constante formellement ou informellement (débat, dialogue, réunion, brainstorming, discussion, etc.), dans la recherche d'informations pour non seulement détecter les failles qui subsistent dans les stratégies mises en place, mais aussi prévenir les variables d'incertitudes stratégiques, en se démarquant de la concurrence et en assurant sa pérennité.

Outils / Méthodes	**Etudes de référence**
Débat et dialogue	Simons (2000) qui est l'instigateur dudit levier de contrôle affirme que le débat et le dialogue sont les marques de fabrique des systèmes de contrôle interactifs.
Dialogues, formations et de la communication	Berland et Sponem (2007) montrent, au travers d'une étude sur la transformation du budget d'une entreprise chimique en système interactif, l'implication plus forte des managers dans le processus de contrôle, via des dialogues entre les dirigeants, des formations et de la communication.
Réflexion collective	Naro et Travaillé (2010) donnent l'exemple de la formalisation d'une stratégie à la réalisation d'un balanced scoredcard dans deux entreprises industrielles et commerciales à travers la réflexion collective des différents acteurs (dont les fonctions et les niveaux de qualification étaient différents).
Discussions	Fasshauer (2012) évoque dans l'utilisation du forecast au sein d'une division européenne d'un groupe américain les discussions hebdomadaires entre les responsables locaux, les équipes de direction du groupe et de la division, et leurs supérieurs hiérarchiques. Ces révisions hebdomadaires sont effectuées dans le but d'améliorer les prévisions mensuelles.

LISTE DES TABLEAUX

TABLE DES FIGURES

TABLE DES MATIERES

Elaboration d'un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion

Plusieurs problèmes accablent les organisations, mais l'espionnage industriel occupe de plus en plus une place grandissante. Ses conséquences sont catastrophiques, allant des pertes de sommes colossales à la faillite de certaines entreprises. Ce travail de recherche, s'inscrivant dans le champ disciplinaire des Sciences de Gestion, particulièrement du contrôle de gestion, a pour finalité d'appréhender le processus de contrôle de l'espionnage industriel dans les organisations, en élaborant un système de contrôle de l'espionnage industriel par la fonction contrôle de gestion. Après une revue de littérature et une première vague d'entretiens semi-directifs, qui ont montré les limites des protections juridiques et les vides de gestion des protections techniques contre l'espionnage industriel, nous avons construit un modèle théorique du processus de contrôle de l'espionnage industriel par la fonction contrôle de gestion, qui met en interaction les figures imposées / libres, les leviers de contrôle diagnostic / interactif et leurs outils, et les six dimensions d'analyse réajustées. Ensuite, nous avons élaboré un système de contrôle de l'espionnage industriel, en déterminant ses outils et en spécifiant son instrumentation dans les organisations. Une deuxième vague d'entretiens semi-directifs a été effectuée pour justifier la pertinence dudit système auprès des spécialistes professionnels et universitaires du contrôle de gestion.

Mots-clés : Espionnage industriel - Contrôle de gestion - Système de contrôle - Elaboration - Processus de contrôle.

Elaboration of a system of control of the industrial espionage by the management control function

Several problems overwhelm organizations, but industrial espionage is becoming more and more important. Its consequences are catastrophic, ranging from the loss of colossal sums to the bankruptcy of certain companies. This research work, which is part of the disciplinary field of Management Sciences, particularly management control, aims to understand the process of controlling industrial espionage in organizations by developing a control system of industrial espionage by the management control function. After a literature review and a first wave of semi-directive interviews, which showed the limits of legal protections and management gaps of technical protections against industrial espionage, we constructed a theoretical model of the control process of industrial espionage by the management control function, which puts into interaction the imposed / free figures, the diagnostic / interactive control levers and their tools, and the six readjusted analysis dimensions. Then we developed a system of control of the industrial espionage by determining its tools and specifying its instrumentation in organizations. A second wave of semi-directive interviews was conducted to justify the relevance of this system with professional and academic management control specialists.

Keywords : Industrial espionage - Management control – System of control - Elaboration - Control process.

Discipline : SCIENCES DE GESTION

Spécialité : CONTRÔLE DE GESTION

Université de Reims Champagne-Ardenne

REGARDS - EA 6292

Bâtiment 13

57 Rue Pierre Taittinger 51100 Reims