



HAL
open science

La gestion du risque

Yvon Pesqueux

► **To cite this version:**

| Yvon Pesqueux. La gestion du risque. Master. France. 2020. halshs-02909236

HAL Id: halshs-02909236

<https://shs.hal.science/halshs-02909236>

Submitted on 30 Jul 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Yvon PESQUEUX

Hesam Université

Professeur du CNAM, titulaire de la Chaire « Développement des Systèmes d'Organisation »

292 rue Saint Martin

75 141 Paris Cédex 03

France

Téléphone ++ 33 (0)1 40 27 21 63

FAX ++ 33 (0)1 40 27 26 55

E-mail yvon.pesqueux@lecnam.net / yvon.pesqueux@gmail.com

Site web eesd.cnam.fr

La gestion du risque

Résumé

Ce texte est organisé de la manière suivante. Après une introduction qui pose la thématique de la gestion du risque, il aborde successivement : l'évaluation des risques ; le management du risque ; le lien entre les logiques de normalisation et avec la dualité « prescription – coercition » ; la gestion interne du risque, classer pour maîtriser ? ; le traitement du facteur humain ; l'emphase des catégories de l'audit.

Introduction

Il faut d'abord souligner que plus la quête de l'efficacité s'approfondit et plus le risque croît, cette quête étant par nature porteuse de risques. La gestion des risques relève d'un paradoxe qui consiste à ramener le « hors limite », imprévisible par nature, dans des limites. C'est ainsi que cette logique paradoxale conduit aux injonctions du même nom au regard d'une asymétrie dans le rapport au futur et de la conjonction / disjonction de la gestion des risques avec l'organisation existante. C'est sans doute ce qui permet de comprendre les logiques de « sur-réaction » qui fondent la gestion des risques et la « sur-référence » à des procédures, « sur-référence » qui apparaît en dualité, cette dimension « sur-procédurale » ayant surtout pour effet de mettre en place une logique incrémentale dans la tentative désespérée de ramener le « hors limite » dans des limites. Le « hors limite » est justement d'une autre substance organisationnelle que le « en limite », d'où le fait que la gestion des risques se trouve surtout être située dans l'univers de la conformité plus que dans celui du risque. C'est en cela qu'à la dualité « vision – confiance » du rôle de direction, la gestion du risque tend à lui substituer la dualité « conformité – réputation », le risque étant considéré comme naissant de la non-conformité pour atteindre la réputation. La gestion des risques met donc en avant les représentations du risque sur la base de la dualité « bienfaisant – malfaisant », le risque perdant ici toute dimension bienfaisante (à la différence de ce qu'il en est en entrepreneuriat) pour être considéré comme possédant une essence malfaisante.

La gestion des risques met en avant les représentations malfaisantes du risque. Le *design* y prévaut, c'est-à-dire une accumulation de méthodes, de protocoles (des outils et des démarches), de dispositifs, etc., *design* qui rapproche la gestion du risque de la gestion de la qualité. D'un point de vue managérial d'ailleurs, à un TQM (*total quality management*) correspondrait un TRM (*total risk management*), cette perspective ouvrant le champ à l'émergence d'un modèle organisationnel¹ du risque.

Une caractéristique marque implicitement ou explicitement les protocoles de la gestion des risques : la répétitivité supposée de leurs éléments. Les protocoles sont conçus à partir de phases qui seraient répétées dans tous les cas de figure, indépendamment des spécificités des cas².

L'axe permettant de fonder la perspective gestionnaire du risque est celui qui distingue les techniques d'évaluation du risque (*risk assessment*) des techniques de management du risque (*risk management*), ces deux volets pouvant fonctionner aussi bien ensemble qu'indépendamment. Mais ces deux aspects reposent sur le postulat de l'objectivation possible du (ou des) risque(s). Rappelons d'ailleurs combien le *risk assessment* est une tradition des deux secteurs économiques que sont l'assurance et la banque, deux secteurs qui se sont toujours traditionnellement chargés des risques. Le domaine du *risk assessment* est à la fois d'ordre quantitatif (c'est-à-dire essentiellement la traduction du risque en termes financiers) et d'ordre qualitatif (expression du risque en termes d'impact potentiel et de probabilité de survenance). Il s'agit de prendre un gage sur l'avenir (et non d'anticiper). Il va combiner deux analytiques, celle de l'occurrence et celle de l'impact. Ce sont les raisonnements probabilistes qui dominent en la matière. Rappelons aussi combien le *risk management* tend aussi vers la plus sectaire (ou plus ridicule ?) logique des *prepers*, c'est-à-dire ceux qui se préparent au risque comme on se prépare à la fin du monde ! Le *risk management* repose également sur le postulat de la séparabilité des risques (d'où la multiplication des risques à épitète...).

Les grands courants conventionnels du *risk assessment* sont les suivants :

- La théorie de l'utilité espérée qui part de deux motivations premières enracinées au plus profond de nos systèmes cognitifs : l'aversion pour le risque (donc éviter les situations dangereuses) et la recherche de réalisations (donc prise de risque). Ces deux motivations interfèrent avec les processus décisionnels faisant de la préférence non pas une constante mais une construction. Le décideur, considéré comme rationnel et conscient, maximise une fonction d'utilité sous contraintes classique de temps et de budget en s'appuyant sur de l'information. Confronté à différentes situations, il recherche la maximisation de l'utilité espérée compte tenu d'une probabilité associée au risque (son aléa).
- La théorie des perspectives a été fondée par D. Kahneman & A. Tversky³ en partant du constat de la non-linéarité des probabilités associées aux événements auxquels les individus se trouvent confrontés. A la différence de la théorie précédente, deux phases construisent le choix : la phase de structuration des informations qui est une phase préparatoire de « reformulation – simplification » et la seconde, phase d'évaluation, qui

¹ Y. Pesqueux, *Organisations : modèles et représentations*, PUF, Paris, 2002

² N. Beck & J. Brüderl & M. Woywode, « Momentum or Deceleration? Theoretical and Methodological Reflections on the Analysis of Organizational Change », *Academy of Management Journal*, June 2008, vol. 51, n° 3, pp. 413-435

³ D. Kahneman & A. Tversky, « Prospect Theory: An Analysis of Decision under Risk », *Econometrica*, 1979, n° 42, pp. 263-291

conduit à évaluer les options et choisir celle qui a le plus de valeur. En d'autres termes, des probabilités subjectives se substituent aux probabilités objectives de la théorie précédente.

Ces deux courants sont complétés par les théories de l'acceptabilité du risque avec :

- La théorie sociale ou psychométrique du risque qui s'intéresse aux déterminants des perceptions du risque compte tenu d'un postulat de rationalité empirique globale du risque effectuée par les individus. P. Slovic⁴ a ainsi proposé des *items* « qualité » du risque : son caractère volontaire (exposition au risque), connu (ou inconnu), la perception de ses conséquences immédiates ou différées, l'estimation des conséquences subies par les générations futures, son caractère juste (ou injuste), son ampleur catastrophique, la confiance (ou non) dans l'évaluation du risque proposée par la communauté scientifique, son rapport « coût – bénéfice ».
- Le principe de précaution (avec son analyse « coût – bénéfice »).

Rappelons aussi que, conformément aux catégories du management, le *risk management* va prendre deux dimensions (plus une liée aux contingences sectorielles). La dimension stratégique du *risk management* tend à être formalisée de plus en plus par référence à une gouvernance des risques, la dimension opérationnelle par rapport à des normes ou des méthodes et au regard de formalisation de thèmes de gestion (avec, par exemple, le PCA – plan de continuation d'activité) ainsi que par rapport aux logiques de *compliance* (se conformer à... et donner des explications). Cette autre distinction est ce qui permet de distinguer « gouvernance des risques » de « gestion des risques » ou encore le risque « pour » les organisations du risque « de » l'organisation. C'est aussi dans le cadre du *risk management* qu'opère la distinction entre « audit des risques » (identification des failles et des vulnérabilités) et « analyse des risques » (intégration de l'analyse de la conséquence de la faille). C'est cet ensemble « *risk assessment* – *risk management* » qui a donné lieu à la distinction entre les approches par la mesure de l'historique qui consiste à travailler sur l'historique des incidents (qui est en particulier imposée par Bâle II en matière bancaire, par exemple), les approches par la mesure des risques intrinsèques qui consiste à analyser les probabilités de survenance et les impacts de et sur les métiers dans le but de dresser une cartographie des risques perçus et les approches par la mesure des risques résiduels afin d'analyser les impacts « de » et « sur » les métiers et d'estimer les vulnérabilités correspondantes.

L'institutionnalisation va opérer au travers d'un jeu social concernant un secteur (par exemple Bâle 2 pour le secteur financier, Solvency pour l'assurance, REACH pour le secteur de la chimie), une catégorie politique (COSO 2 pour les sociétés cotées sur la place financière de New-York), un maillage associatif *lobbyiste* (FERMA par exemple – *Federation of European Risk Management Association* dont le membre français est l'AMRAE – Association pour le Management des Risques et des Assurances de l'Entreprise) ou encore l'IMdR (Institut pour la Maîtrise des Risques), les deux associations ayant d'ailleurs des membres en commun. Il existe donc, tout comme pour la qualité⁵, un maillage de la société civile en associations autour de la question du risque.

Le *risk management* ne peut non plus être envisagé indépendamment des notions associées de

⁴ P. Slovic, « Perception of Risk », *Science*, n° 236, 1987, pp. 280-285

⁵ Y. Pesqueux, *Qualité et management – une analyse critique*, Economica, Paris, 2008

sécurité, de fiabilité et de sûreté ou encore de celle de vulnérabilité et de peur : gérer les risques, c'est aussi gérer les peurs ! Il se réfère à la figure du *risk manager*, personnage dont la justification professionnelle est justement qu'il gère les risques au regard de compétences en matière financière, juridique, technique, commerciale, etc. A ce titre, il identifie les risques, propose des mesures de maîtrise de ces risques (prévention, etc.), élabore et met en œuvre la politique et le plan d'assurance des risques, participe à l'animation du personnel au sujet des risques et communique sur les risques avec la direction. Il dispose à ce titre de réseaux de veille et d'alerte (qu'il conçoit et met en œuvre s'ils n'existent pas), possède la tutelle de la gestion des incidents et des crises, conçoit les méthodes et outils de gestion à destination des opérationnels et optimise le coût global du risque par une politique de gestion des risques et une politique de maîtrise des risques. Il peut être considéré comme un concepteur et / ou comme un acteur de la gestion des risques. Cette seconde acception est la définition qu'en donne le FERMA (www.ferma.eu) qui en fait un coordinateur, un éducateur et un communicateur dans la mesure où le repérage des risques n'est pas de sa seule responsabilité, responsabilité limitée alors à sa capacité de repérage. Mais, comme pour beaucoup de logiques de gestion (il en va ainsi du contrôle de gestion et du contrôleur de gestion dans la mesure où le contrôle dépasse largement ce que fait le contrôleur), la gestion des risques dépasse largement ce que fait le *risk manager*.

La perspective gestionnaire du risque se réfère à des raisonnements de classements associés au risque dont les principaux sont les suivants : « inductif – déductif », « qualitatif – quantitatif », « général – spécifique ».

C'est ici qu'opère souvent la confusion entre risque et menaces (menace considérée dans le même sens que dans les matrices SWOT).

Forces

Menaces

Opportunités

risque

Faiblesses

C'est à ce titre aussi que l'on peut parler de stratégies « type » de gestion des risques avec :

- La stratégie d'« élimination - diversification » des risques soit par renoncement à certaines activités, soit par diversification des activités ;
- La stratégie de transfert des risques à des entités extérieures (comme avec l'assurance) ;
- La stratégie des fonds propres qui consiste à détenir des ressources destinées à ce financement, que ce soit de façon volontaire ou réglementaire comme dans les activités financières.

Et que la gestion du risque s'articule au contrôle interne dont la trilogie fondatrice est construite sur trois critères : pertinence, complétude et efficacité.

Il y aurait pourtant une forme de contradiction entre la perspective de la maîtrise des risques et le risque inhérent à l'acte même d'entreprendre. Rappelons que les rapports protégés ne peuvent jamais qu'être stériles tout comme ce fut le cas pour le délire (?) qui a prévalu à la construction des abris anti atomiques. Rappelons aussi la perspective foucauldienne qui voit la discipline comme une technologie, ce qui permet d'ouvrir le champ de la représentation des techniques de gestion du risque comme une technologie disciplinaire outillée. Rappelons enfin que la gestion du risque repose sur des outils redevables de la logique plus large du thème des outils de gestion.

Mais une autre dualité possible est celle que F. Jubert⁶ mentionne, d'après E. Freidson⁷, avec deux modèles de la gestion des risques : le modèle du professionnalisme (où compétences individuelles et expertise priment) et le modèle bureaucratique (où c'est la formalisation des règles qui prime). Mais, dans les deux cas, il est bien question d'un agent organisationnel qui est considéré à la fois comme bienveillant (donc pouvant être considéré comme antidote du risque) et comme malveillant (d'où l'ensemble des procédures dans lesquelles il faudra l'enserrer car il est à la source du risque).

Les réponses organisationnelles reposent principalement sur le présupposé de l'agent risqué d'où :

- La réduction par automatisation de l'intervention humaine partout où cela est possible ;
- Le repérage et l'élimination des sources principale d'erreurs humaines ;
- La limitation de l'initiative des opérateurs par la mise en œuvre de procédures et de règles sensées tout couvrir.

Mais outre l'ensemble indéterminé que constitue la gestion du risque, tous ces aspects « font système », la fiabilité de fonctionnement accrue qui en découle entraînant corrélativement une baisse de la vigilance, effet parfois qualifié de paradoxe d'Icare⁸. La conduite des processus se présente en effet assez peu comme une suite d'activités bien ordonnées. Il existe nombre d'activités peu programmables et des situations imprévues ou ambiguës, d'où l'importance de la reconnaissance du rôle des Hommes⁹.

Pour mettre en perspective la thématique de la gestion du risque, il est possible de se référer à un tableau à double entrée venant croiser « *business risk* – risque organisationnel » et « gestion industrielle des risques – gestion financière des risques – gestion des risques liés au système d'information », même si ces distinctions sont très archétypiques et méritent d'être discutées à la frontière. C'est le dernier type de risque, le risque lié au système d'information qui a donné lieu aux développements les plus récents avec l'accent mis sur les conséquences liées aux pertes de données sensibles et aux contraintes juridiques et réglementaires de la continuation d'activité.

	Logique de l'instrumentation	
	<i>Business risk</i>	Risque organisationnel
Gestion industrielle des risques	problématiques de la sécurité et de la sûreté dont le risque alimentaire,	problématiques de la fiabilité et de la sûreté de fonctionnement

⁶ F. Jubert, « Le professionnalisme aux limites d'un dispositif de gestion des risques » in V. Boussard (Ed.), *Au nom de la norme – Les dispositifs de gestion entre normes organisationnelles et normes professionnelles*, L'Harmattan, collection « Sociologie de la gestion », Paris, 2006, p. 41-62

⁷ E. Freidson, *Professionalism: The Third Logic on the Practice on Knowledge*, The University of Chicago Press, 2001

⁸ D. Miller, *Le paradoxe d'Icare – Comment les entreprises se tuent à réussir ?*, PUL Laval, Québec, 1993

⁹ B. Journé, *Les organisations complexes à risques : gérer la sûreté par les ressources, étude de situations de conduite de centrales nucléaires*, Thèse Ecole Polytechnique, janvier 1999

		chimique, nucléaire constituent une forme spécifique	
Logique des normes	Gestion financière des risques	problématiques du risque « client »	problématiques du contrôle interne compte tenu des trois « piliers » de Bâle 2 : risque de marché, risque de crédit et risque opérationnel
	Gestion des risques liés au système d'information	problématiques du risque liées au système d'information compte tenu de dommages à éviter (dommages aux matériels, aux informations)	problématique de la continuation d'activité

Il existe en fait une proximité entre ces perspectives car il y est plus question de quête de sécurité que de gestion du risque. Les protocoles proposés vont donc reposer sur la séquence « diagnostic (repérage) – solution », en cohérence avec la vieille logique du *problem solving* dans l'utopie tout aussi ancienne du « management scientifique ».

Par ailleurs, il est possible de mettre en avant l'existence de deux voies duales dans cette logique du *problem solving* : une voie conséquentialiste (on mesure le risque sur la base de ses conséquences) et une voie causaliste (à partir des conséquences, on essaye de remonter vers les inducteurs de risque). Cette logique du *problem solving* tend à réduire le risque à trois dimensions : financière, juridique (d'où la quête de responsabilités) et de réputation. La gestion des risques prend trois modalités : procédurale, organisationnelle, gouvernance et pilotage, les deux premières modalités s'inscrivant dans un projet de complétude (une gestion « complète » des risques) et les deux dernières dans un projet d'incomplétude

Ces protocoles vont se construire sur l'univers d'institutionnalisation *ad hoc* en cohérence avec les catégories du « moment libéral¹⁰ » c'est-à-dire l'auto-décret, sur la base de l'argument d'expertise, des normes de fonctionnement dans la séquence de la privatisation : des normes privées rendues publiques en se dispensant de la preuve de leur représentativité. Ainsi en va-t-il du risque opérationnel selon Bâle II qui distingue les risques financiers (risque de crédit, de marché et autres risques, inhérents à l'activité bancaire) des risques non financiers dont les risques opérationnels liés à des événements internes et / ou externes et des risques stratégiques. Le comité ajoute à la panoplie « classique » des stratégies d'élimination des risques (par la diversification comme dans la théorie du portefeuille, par le transfert comme avec l'assurance, par les fonds propres) la prise en compte de la dimension comportementale et de la dimension

¹⁰ Y. Pesqueux, *Gouvernance et privatisation*, PUF, collection « la politique éclatée », Paris 2007

organisationnelle au regard de la dualité « fréquence – sévérité » emprunté au domaine de la fiabilité industrielle, avec des dispositifs de diagnostics et de contrôles essentiellement procéduraux. On pourrait parler à ce titre d'un strict tropisme disciplinaire de la gouvernance mâtiné de logiques issues de l'audit.

Sur un plan plus général, la littérature professionnelle sur la gestion du risque repose sur deux aspects : un plaidoyer pour le managérialisme et un culte voué à la simplicité donnant lieu à une véritable boulimie de méthodes et de recommandations dans une perspective réduisant brutalement la dimension technologique de cette gestion à un ensemble d'outils. S'agit-il alors d'appel aux sens (aux cinq sens) pour tenir lieu d'appel au sens (but). C'est pourquoi elle sera remplie de références à des normes (considérées comme des techniques d'évaluation du risque) et à des *check list* (techniques de management du risque) venant constituer des protocoles sans théorie dans la volonté de pousser ces protocoles à leurs limites au travers des grilles du PPSS (Prévention, Protection, Sécurité, Sauvegarde). Elle conduit alors à se référer aux modalités de gestion de la qualité en introduisant une forme de circularité entre gestion du risque et gestion de la qualité. Comme on l'a souligné plus haut, gérer la qualité, c'est gérer le risque et *vice versa*. Au *Total Quality Management* correspond en miroir un *Total Risk Management*. Elle met en avant une approche informationnelle et communicationnelle du risque en multipliant les collectes et remontées d'information. Or il est important de noter combien une approche informationnelle du risque est conditionnée par une représentation *a priori* qui est de l'ordre politique de l'idéologie. L'approche communicationnelle conduit à se référer à une rhétorique qui tend à faire de la gestion du risque « la gestion du risque de tout », pour reprendre l'expression de M. Power¹¹. De plus, en termes de genèse de logiques organisationnelles, à la « projectification » à outrance de la gestion par projet, correspondrait la « risquification » à outrance, à la fois en liaison avec la référence au projet mais aussi de façon plus large et indépendante, par référence aux risques à épithète.

Rappelons de plus que le contexte juridique de la gestion des risques a profondément évolué ces dernières années du fait de la combinaison de deux logiques de droit : la référence à la *soft law* par rapport à des « principes », en particulier le principe de précaution et les perspectives de *deep pocket* en matière d'indemnisation qui vont faire payer les agents qui le peuvent (les entreprises en général) non parce qu'elles sont coupables mais parce qu'elles peuvent payer, la justice tendant à devenir, en ce domaine, un jeu de mistigri ! Mais en fondant ainsi la responsabilité sur des principes éthiques, cela montre d'autant plus cruellement l'absence de perspective sociale en la matière.

Les normes vont se caractériser par :

- Des prescriptions proposées par un groupe légitime dans le contexte du volontarisme managérial, qu'il s'agisse d'entreprises d'un secteur donné (au regard de l'épithète qui sera accolée au risque) ou d'un groupe professionnel ;
- La mise en avant d'une utilité qui permet de définir une responsabilité de conformité (évaluation du risque) et une responsabilité de prescription (management du risque) d'où la substitution d'une omniscience de la règle normative à l'omniscience des Pouvoirs Publics sur la base de cet argument d'utilité ... qui permet de continuer à faire de bonnes affaires ! Les médias vont ainsi critiquer l'omniscience des Pouvoirs Publics en mettant en avant

¹¹ M. Power, *La société de l'audit : l'obsession du contrôle*, Editions La Découverte, Paris, 2004

l'émotivisme du risque, les pouvoirs des juges, la plus légitime et en même temps souveraineté résiduelle en démocratie libérale, le tout à partir de faits divers.

Une norme de référence est offerte par l'ISO avec son document *ISO/IEC Guide 73 Risk management – Vocabulary – Guidelines for use in standards* qui définit le risque comme « la combinaison de la probabilité d'un événement et des conséquences de celui-ci », que l'aléa soit positif ou qu'il soit négatif. Il définit l'appréciation du risque comme un « processus général d'analyse et d'évaluation ».

Une autre norme de référence est celle du *Coso Report (Committee of Sponsoring Organizations of the Treadway Commission)*¹². Il définit le contrôle interne comme le processus mis en œuvre pour fournir une assurance raisonnable quant à l'atteinte des trois objectifs que sont la réalisation et l'optimisation des opérations, la fiabilité de l'information financière et la conformité aux lois et règlements. Au début des années 2000, PriceWaterhouse, déjà co-auteur du *Coso Report* a développé, à la demande du comité, un référentiel méthodologique de la gestion des risques dénommé *Coso II*¹³. Ce référentiel est marqué par des aspects tels que la prise en compte systématique des risques dans l'étude des options et des scénarios stratégiques sur la base de concepts tels que l'appétence aux risques (niveau de risque accepté choisi par les dirigeants et validé par le conseil d'administration), la tolérance aux risques (écarts acceptés par rapport aux objectifs compte tenu d'une batterie d'indicateurs), une démarche d'anticipation par identification des événements susceptibles d'affecter la réalisation des objectifs (positivement sous la forme d'opportunités et négativement sous la forme de risques) et la prise en compte et la maîtrise des risques dans la définition des objectifs afin de faciliter l'intégration de la gestion des risques dans le fonctionnement courant.

Une autre norme de référence est celle de la FERMA qui, comme tout organisme de ce type, offre un cadre de référence en matière de terminologie, de processus de déploiement de la gestion des risques (un protocole donc), d'organisation de la gestion des risques et d'objectif de cette gestion. Comme pour toutes les logiques de ce type, ce cadre est issu d'un consensus ayant pris pour base les travaux d'associations britanniques du domaine (IRM – *Institute of Risk Management*, AIRMIC – *Association of Insurance and Risk managers* et le *National Forum for Risk Management in the Public Sector* – ALARM). Pour la FERMA, « la gestion des risques devrait être un processus continu d'amélioration qui commence avec la définition de la stratégie et se poursuit avec l'exécution de celle-ci. Elle devrait traiter systématiquement de tous les risques qui entourent les activités de l'organisation, que celles-ci soient passées, présentes et surtout futures ». La FERMA propose de distinguer entre les risques d'origine externe (risques financiers tels que taux d'intérêt, de change, crédit, risques stratégiques tels que la compétition, les changements des clients, les changements dans l'activité, les risques opérationnels tels que les réglementations, la culture et la composition de l'équipe dirigeante et les périls tels que les contrats, les événements naturels, les fournisseurs, l'environnement) et les risques d'origine interne (liquidité et *cash flow*, recherche & développement et capital intellectuel, fusions & acquisitions, intégration, système de contrôle des comptes et système d'information, recrutement, chaîne d'approvisionnement, employés, mobiliers, biens et services). Le processus de gestion des

¹² Coso Report, *Internal Control Integrated Framework*, traduction, *La pratique du contrôle interne*, Editions d'Organisation, Paris, 1994

¹³ PriceWaterhouse, *Enterprise Risk Management*

risques repose sur un protocole d'audit formel dans le but de modifier les risques repérés. En accord avec les objectifs stratégiques de l'organisation, il s'agit d'apprécier les risques (analyse du risque avec leur identification, leur description et leur estimation), d'en effectuer un compte rendu (menaces et opportunités), de les traiter, d'effectuer un compte-rendu sur le risque résiduel (avec un processus de communication interne et externe) et de mettre en place un suivi. Les cinq dimensions du risque concernent le niveau stratégique, le niveau opérationnel, le niveau financier, la gestion des connaissances et la conformité aux règles et aux normes du domaine. La description vise la portée du risque, sa nature (cf. les dimensions), le repérage des « parties prenantes » et de leurs attentes, leur quantification (importance et probabilité), la tolérance et l'appétence pour le risque (qui vise les moyens de la gestion des risques), leur traitement (au regard des moyens existants et à mettre en œuvre), la définition des actions d'amélioration et le développement d'une stratégie et d'une politique des risques. Le référentiel parle de « profil de risque » et de structure et administration du risque en rappelant le rôle de *sponsor* de la direction, celui des unités opérationnelles, celui d'un service de gestion des risques, celui de l'audit interne d'où l'idée de mettre en place des procédures de surveillance des risques.

Une autre référence est celle de l'*Institut pour la Maîtrise des Risques* (IMdR) qui a pris la suite en 2002 de l'*Institut de Sécurité de Fonctionnement* (ISdF) avant de fusionner en 2006 avec l'*Institut Européen des Cindyniques* (IEC). L'ISdF a été créé en 1989 à l'initiative du Ministère de l'Industrie et regroupant principalement l'*ex Mouvement Français pour la Qualité* (disparu en 2003 à la suite des coupes budgétaires de l'époque), l'*Association Française des Ingénieurs et Responsables de Maintenance* (AFIM) et l'*Association Française pour l'Analyse de la Valeur* (AFAV). Son objectif était de faire de la sûreté de fonctionnement un élément central de réflexion et d'action à partir de quatre paramètres : la fiabilité, la maintenabilité, la disponibilité et la sécurité. L'IEC a pris la suite du colloque de l'UNESCO de 1987 pour se consacrer à la question du risque à la suite des catastrophes de Tchernobyl, de Bhopal et de Challenger. Il s'est focalisé sur la notion de situation de danger au regard de cinq espaces cindyniques : l'espace statistique (mémoire de l'histoire), l'espace épistémique des représentations, l'espace des finalités, l'espace déontologique des normes, règles, etc. et l'espace axiologique des valeurs. L'IMdR a en outre reçu l'appui de 14 groupes industriels et organise l'animation de groupes de travail et des rencontres de même qu'il rassemble une documentation et réalise des études commandées. Il met l'accent sur l'importance d'une démarche préventive en matière de gestion des risques.

Mais le processus de légitimation de la norme est également important suivant qu'il est construit sur des modalités ouvertes (démocratie délibérative et / ou argument de la participation) ou bien sur des modalités fermées (club d'experts et argument de l'expertise).

La gestion du risque distingue enfin deux logiques temporelles, celle de la réponse dans l'urgence, qui recoupe et apporte de l'emphase aux autres perspectives de l'urgence, si courantes dans les logiques de gestion aujourd'hui et celle de la réponse dans le temps, *a priori* et *a posteriori*. Dans les deux cas, les objets sont communs : les procédures et le cadre décisionnel. Il en va aussi de la thématique des agents de la gestion du risque au regard du mélange qui s'établit entre les professionnels et les volontaires, les agents du dedans et ceux du dehors de l'organisation, les deux catégories tendant à se croiser. Elle conduit à la confusion entre deux personnages : le consultant et le sauveteur.

L'évaluation des risques

L'évaluation des risques repose sur l'application de techniques utilisées par ailleurs dans le but de quantifier les effets et des recueils d'accidents afin de mieux analyser les causes à partir d'échelles de gravité, des retours d'expérience et des banques de données. Les cindyniques considèrent ainsi qu'« un danger peut être représenté selon deux paramètres qui sont la gravité et la probabilité. C'est en agissant sur ces deux axes que l'on pourra diminuer le nombre et l'ampleur des catastrophes qui ne sont que réalisation du danger »¹⁴. Comme l'indique D. Pécaud, « cette estimation se fonde sur un rapport que chacun serait en mesure d'établir entre l'existence de dangers connus, inhérents à une situation donnée, et un but que l'on se propose d'atteindre »¹⁵.

P. Rubise cite ainsi les quelques lois définies en matière de modélisation du risque :

- La loi de la réticularité cindynique (le danger qui menace un individu est fonction de son environnement) ;
- La loi de l'antidanger (la gravité d'un danger est accrue par la sous-estimation de sa probabilité) ;
- La loi d'invalidité cindynogène (l'excursion d'un système hors de son domaine de validité est créatrice de dangers) ;
- La loi de l'éthique cindynique (la qualité des relations dans un réseau est un facteur de réduction du danger) ;
- La loi de l'accoutumance au danger (avec le temps, la conscience des dangers de faible probabilité diminue).

L'acceptabilité d'un risque est le « niveau de criticité résultant d'une décision explicite et justifiée, fondée sur la gravité acceptée des conséquences »¹⁶, son impact, la « conséquence ou effet produit par la réalisation du risque. Il est évalué en termes de coûts, de délais et / ou de performances techniques »¹⁷, la gravité l'« effet produit par la réalisation du risque, c'est-à-dire les impacts dommageables que le risque peut avoir sur le respect des objectifs du projet »¹⁸.

L'estimation du risque est le « processus utilisé pour affecter des valeurs à la probabilité, à la détectabilité et aux conséquences d'un risque »¹⁹.

La sévérité d'un risque est le rapport entre la probabilité d'occurrence (fréquence d'apparition par rapport au nombre de cas) et l'impact (coût des dommages et de remise en état) sur la bonne marche du processus. La probabilité d'occurrence correspond aux chances raisonnables (à la vraisemblance mathématique) que le risque a de se réaliser lors du déroulement du processus et de se matérialiser en difficultés réelles. Le risque acceptable est fonction de l'impact probable et

¹⁴ P. Rubise, article « risque technologique », *Encyclopedia Universalis*

¹⁵ D. Pécaud, *Risques et précaution – L'interminable rationalisation du social*, Editions La dispute, Paris, 2005, p. 97

¹⁶ H. Courtot, *La gestion des risques dans les projets*, Economica, Paris, 1998, p. 40

¹⁷ H. Courtot, *op. cit.*, p. 40

¹⁸ H. Courtot, *op. cit.*, p. 40

¹⁹ H. Courtot, *op. cit.*, p. 40

de sa gravité. La criticité constitue la valorisation du risque. Elle s'exprime par une valeur résultant de la combinaison des caractéristiques quantifiées du risque, à savoir sa gravité, sa probabilité d'occurrence et / ou sa détectabilité.

Cette perspective repose sur l'analyse « coûts – avantages » (ou « coût – inconvénients » pourrait-on dire aussi), au nom du conséquentialisme qui prévaut dans le « moment libéral ».

Le management du risque

Avec le management du risque, il s'agit, pour les agents organisationnels, de développer les « bonnes pratiques » qui visent, avant tout, la réduction de toute transgression par une pédagogie construite sur une exacerbation de la sensibilité au risque. Les certifications et les normes sont aussi la preuve de l'implication d'une organisation formalisée dans le processus de gestion des risques. D. Pécaud²⁰ distingue la prévention, la précaution et la préservation de soi et des autres, trois attitudes qui renvoient à des pratiques différentes. Les politiques de prévention ont pour but d'assurer la tranquillité sur la base d'une attitude volontariste qui suppose l'existence de dangers possibles à figurer comme étant « objectifs » au regard de connaissances dont ils sont déduits. Les deux autres attitudes ne sont pas seulement fondées sur des certitudes mais sur des représentations considérées comme « normales », institutionnalisées, en quelque sorte. En particulier la dernière, la préservation de soi et des autres dépend de l'attention que chacun prête aux autres.

La prévention du risque a alors donné lieu au développement de recherches et d'enseignements ainsi qu'au développement de la thématique de la gestion de l'accident (c'est le domaine de la protection avec des plans de secours où les différents acteurs – policiers, pompiers, secouristes, médecins, administratifs, etc. – sont positionnés à l'avance afin d'accroître leur efficacité et d'éviter certaines redondances ou lacunes). La précaution est également apparue et participe à la construction d'un droit international.

Le management des risques est le processus itératif appliqué tout au long d'un programme et qui regroupe les activités d'identification, d'estimation et de maîtrise des risques²¹.

Il repose sur une phase d'analyse (rationalité procédurale) à partir de classe de risques (« *ensemble cohérent de risques quant à leur nature et aux responsabilités associées à leur management* »²²) par phase, cause, origine, fonctionnalités et par risques organisationnel et humains. Ceci permet de distinguer les risques mineurs des risques majeurs, critiques et catastrophiques. La rationalité procédurale tient ici en quelque sorte lieu de pensée magique, l'application de ces catégories étant une sorte d'assurance tous risques.

La phase de maîtrise est vue comme l'« *ensemble des actions définies et conduites dans le but de*

²⁰ D. Pécaud, *Risques et précaution – L'interminable rationalisation du social*, Editions La dispute, Paris, 2005, p. 101

²¹ H. Courtot, *op. cit.*, p. 38

²² H. Courtot, *op. cit.*, p. 35

réduire et de maintenir la gravité des risques à un seuil au moins tolérable »²³. Elle vise soit à lever le risque, soit à transférer le risque, soit à atténuer le risque, soit à accepter les risques résiduels (les risques subsistant après le traitement des risques « importants ») et, parmi les logiques proposées, la mise en œuvre un suivi des risques (activité dont le but est de maintenir ou d'améliorer la visibilité sur le risque et de s'assurer de l'application des actions de maîtrise) est considérée comme majeure.

Le management du risque met également l'accent sur la notion de « culture du risque » venant en fait masquer une injonction d'obéissance à des procédures.

Le management du risque a conduit à l'apparition d'une nouvelle fonction dans l'organisation, celle de *risk management* ainsi qu'à de nombreuses méthodes. Il conduit également à la glorification des politiques visant à la sûreté.

Le lien entre les logiques de normalisation et avec la dualité « prescription – coercition »

M. Laccassagne & B. Mugnier²⁴ définissent la prescription et la coercition comme « *les conditions dans lesquelles doit s'effectuer l'activité économique des firmes, la coercition répond aux exigences de police de cette activité, et est la juste conséquence de la prescription* ». Le présupposé de l'articulation « prescription – coercition » repose sur la compétence reconnue à l'autorité publique en matière de risque. C'est la discussion de cette logique qui a conduit aujourd'hui, dans une perspective néo-libérale, à la remise en cause de ce présupposé du fait d'une articulation supposée à accorder aux intérêts mutuels des *stakeholders*. La justification en est qu'il faudrait aujourd'hui prendre en compte les interdépendances croissantes qui jouent au sein des organisations pour mieux cerner la mesure de ce risque. Il en va ainsi avec le développement des *Safety Cases* au Royaume-Uni, développement signalé par les auteurs et lié à l'émergence de la *risk-based regulation* dans l'industrie d'extraction du pétrole *offshore*. A ce titre, les *Safety Cases* sont à la sécurité dans ce secteur ni plus ni moins ce que les *Business Cases* sont à la responsabilité sociale de l'entreprise ou à la quête plus générale des *best practices* dans le contexte de la régulation du « moment libéral ».

Les *Safety Cases* sont des documents qui doivent faire un « usage approprié » d'analyses de risques quantitatives pour démontrer que :

- Le système de management est adéquat pour assurer la conformité avec des exigences statutaires en termes de sécurité et de protection des personnes ;
- Des dispositions adéquates ont été prises pour que la plate-forme puisse être auditée ;
- L'ensemble des dangers pouvant potentiellement engendrer un accident majeur a été identifié.

A ce titre, on n'est d'ailleurs pas si loin que cela non plus de la thématique actuelle du *Total Quality Management*. Les mesures doivent être prises dans la perspective de réduire ces risques au niveau le plus faible qu'il est possible d'atteindre en pratique (*As Low As Reasonably Practicable*, ALARP). En termes de management, la régulation issue des *Safety Cases* introduit trois aspects : un déplacement de la charge de la preuve du régulateur vers le régulé, le fait que

²³ H. Courtot, *op. cit.*, p. 38

²⁴ M. Lassagne & B. Mugnier, « La nouvelle réglementation des risques comme enjeu du management », *Actes des XVI^e journée des IAE*, Paris, 2002

les éléments que l'opérateur avance à l'appui de sa demande d'approbation doivent être vérifiables par le biais des audits et enfin la mention d'un critère d'acceptabilité du risque. C'est la mise en place d'un lien explicite entre les différents aspects de la sécurité conjuguée à une responsabilisation qui a fait le succès des *Safety Cases* dans le droit-fil de l'idéologie utilitariste qui domine aujourd'hui. C'est sans doute aussi la perspective de pouvoir faire soi-même sa police interne... à l'écart des regards indiscrets ... On retrouve donc ici l'aspect auto-référenciel qui est une des caractéristiques constantes des perspectives néo-libérales et à l'autonomisation de la réflexion « sécurité » par rapport à l'intérêt général.

Le Livre Blanc *Stratégie pour la future politique dans le domaine des substances chimiques* en date du 27 février 2001 (Commission des Communautés Européennes) s'inscrit dans la même perspective, néo-libéralisme oblige, par le développement d'un système de classification unique et d'une base de données centrale pour la mise en place d'un régime de responsabilité tourné vers l'industrie et l'affirmation d'une volonté d'harmonisation des conditions dans lesquelles doivent se dérouler les essais. Le Livre Blanc illustre bien le passage de la réglementation exclusivement prescriptive à une réglementation (ou une volonté de réglementation) qui intègre, dans un cadre nécessairement négocié, à la fois les contraintes financières et économiques – dans un sens lui-même à négocier – des entreprises et les exigences de sécurité des personnes et de préservation de l'environnement dans la perspective néo-libérale de la primauté des intérêts catégoriels (donc *in fine* de ceux des plus forts, des plus rusés).

Avec ce type expansionniste de gestion des risques, on sort donc de la dichotomie « gestion publique des risques », fondée sur une logique de la recherche de l'intérêt général par imposition d'une conformité à une gestion privée des risques, appuyée sur l'optimisation des techniques de production du seul point de vue de l'intérêt individuel de l'entreprise.

C'est ainsi que la norme ISO 73 « Gestion du risque – vocabulaire – principes directeurs pour l'utilisation dans les normes » tente de promouvoir une approche cohérente de la description des activités relatives à la gestion des risques et à l'utilisation de la terminologie de la gestion du risque.

Toujours dans la même perspective néo-libérale, la contractualisation (pour bénéficier de l'incomplétude des contrats) apparaît donc comme fondement de la nouvelle réglementation du fait du développement simultané de deux décloisonnements : l'un, horizontal, entre de multiples agents de la production à la fois autonomes et interdépendants, l'autre, vertical, entre l'autorité de réglementation et les organisations, qui introduit une relation plus centrée sur l'appréciation des risques et les moyens mis en œuvre pour les réduire que sur les moyens eux-mêmes pris *in abstracto*. Ce double décloisonnement ouvre ainsi la voie à une nouvelle forme de contractualisation entre entreprise et régulateur dans le sens de la primauté des intérêts de l'entreprise. La référence est donc la notion de « partie prenante » comme masque du « Bien Commun » et instrument de déclassement de l'omniscience des Pouvoirs Publics. Ce seraient en effet les « parties prenantes » qui seraient détentrices de cette omniscience au nom de leur proximité avec le « terrain ».

C'est ce qui vient ouvrir de nouvelles opportunités stratégiques et opérationnelles en introduisant dans les représentations managériales l'idée que *good business*, prévention des risques et profitabilité à long terme, loin d'être antinomiques, se renforceraient mutuellement. Ce

renouvellement des modalités de la mise en oeuvre effective d'une gestion des risques ouvre un nouvel espace à la compétition entre les organisations sur la base de la prise en compte de la maîtrise des risques dans leurs processus et la communication sur celle-ci.

Alors même qu'une suspicion de négligence pèse sur une organisation après un accident, celle-ci devient infondée si l'on peut apporter la preuve de la conformité à une norme d'acceptabilité du risque reconnue comme adéquate par les autorités de régulation et, indirectement, par la puissance publique, dans la mesure où cette norme est issue de conditions économiques acceptées et que les moyens mis en oeuvre pour l'atteindre ont été dûment approuvés (même si leur niveau peut *a posteriori* être considéré comme insuffisant). Le questionnement se déplace de la conformité à des prescriptions externes abstraites vers la validité de la norme.

Mais il faut également souligner qu'une notion telle que le « risque acceptable » est souvent évacuée au profit du principe de précaution et que l'on en revient alors au présupposé implicite de l'autorité publique. Sans doute est-ce aussi une des raisons du succès de ce principe pourtant relativement flou et contestable.

La gestion interne du risque

Il s'agit ici du royaume des grilles regroupant des méthodes très protocolaires destinées à proposer une vision du rôle du manager dans la démarche de gestion des risques redevable du vieux projet du management scientifique. Les ingénieurs ont ainsi conçu une pléthore de méthodes chargées d'anticiper les défaillances (on en compte plusieurs centaines !). Elles reposent sur une chronologie d'étapes attribuant des rôles aux différents agents et conduisent à la nécessité de construire une mémoire des risques.

Différents types de méthodes sont alors proposées :

- Les méthodes descendantes causes -> effets qui relèvent de la logique de déclinaison avec, par exemple, APR (Analyse Préliminaire des Risques – US Air Force, décennie 1960) qui repose sur des enquêtes de terrain et des schémas de procédés. Cette méthode a pour objet de mettre en évidence les principaux risques susceptibles d'être rencontrés lors de la conception de systèmes nouveaux. AMDEC (Analyse des Modes de Défaillance des Composants, de leurs Effets sur le Système et de leur Criticité, apparue durant la décennie 60 dans l'industrie aéronautique) propose une analyse par composants de plus en plus détaillés. Elle repose sur un raisonnement inductif (« causes – conséquences ») mais présente l'inconvénient de sa lourdeur et de son coût de mise en oeuvre. Elle est aujourd'hui très répandue et elle est systématiquement utilisée dans toutes les industries « à risque » (nucléaire, spatial, chimie). C'est une démarche probabiliste qui a pour objectif d'analyser de manière systématique et préventive les défaillances d'un système technique ou d'un équipement dont les conséquences peuvent affecter sa fiabilité et sa maintenabilité. HAZOP (*Hazard and Operability Study*, apparue dans décennie 1970 dans l'industrie chimique) opère par analyse des écarts par rapport à une norme.
- Les méthodes stochastiques comme la méthode de l'arbre de défaillance (Bell, décennie 1960) ou MAC (Méthode des Arbres de Causes) qui propose une représentation graphique déductive, le diagramme « causes – conséquences ». Par exemple, la méthode de combinaison

des pannes résumées (MCPR, industrie aéronautique) est mise en œuvre afin de prendre en compte l'effet systémique des pannes (avec la notion de PRI, PRE et PRG, pannes résumées internes, externes, globales), l'évaluation probabiliste est effectuée pour tenir compte du jeu qui s'établit entre incertitude et irréversibilité, ROMPIT (*Risk and Opportunity Management Process Improvement Team*, Honeywell 1995) est plus dévolue au management de projet.

- Les méthodes ascendantes (sous forme de représentations principalement) partent des effets pour aller vers les causes et relèvent d'une logique incrémentale sur la base de formalisations dont les principales relèvent des supports suivants (au point que les logiciels *ad hoc* existent aujourd'hui sur ces bases-là) : chaînes de Markov, méthode de Monte Carlo, réseaux de Petri.

La gestion des risques repose sur le thème de la décision rationnelle revisitée avec la mise en avant :

- De la notion de jugement (les bases informationnelles, le contexte, la mémoire, la créativité, l'expérience) ;
- Du retour d'expérience et le raisonnement par cas (récupération donc structuration, mémorisation et hiérarchie des cas – particuliers et atypiques, re-mémorisation, réutilisation, révision et apprentissage) ;
- De l'aide à la décision et l'apprentissage par phases : curiosité, confiance, coopération, aide individuelle, collective ;
- De la capitalisation de l'expérience ;
- De la simulation ;
- De l'importance accordée à la communication ;
- De la gestion collective des dangers et l'architecture coopérative d'information et de communication.

Classer pour maîtriser ?

Il est d'abord important de souligner que la classe dans laquelle se retrouvera le risque est aussi ce qui indiquera la solution. Classer est donc à la source des protocoles *ad hoc* de gestion des risques.

Dans la perspective du classement, différentes typologies sont ainsi proposées :

- La typologie des risques de V. Giard²⁵ qui distingue entre : les risques internes, les risques externes, les risques liés à la prévision d'utilisation des ressources, les risques de détection tardive, les risques de diagnostic erroné, les risques de réponse inappropriée. Les risques internes sont liés à l'imprécision des objectifs et des tâches, au manque de cohérence du cahier des charges, aux risques techniques et d'industrialisation et au manque de maîtrise des processus de développement et de suivi de projets. Les risques externes sont liés à l'obsolescence commerciale (attentes du marché, concurrence), aux risques réglementaires sur les spécifications (mauvaises informations sur la réglementation). Les risques liés à la prévision d'utilisation des ressources sont liés aux risques relatifs à la définition des ressources requises (respect de normes de sécurité et d'environnement, réglementation des personnels) et aux risques relatifs à la disponibilité des ressources requises (méconnaissance

²⁵ V. Giard, *Gestion de production et statistiques appliquées*, Economica, Paris 1995

de la performance de certaines ressources, sous-estimation de l'apprentissage de ressources nouvelles, mauvaise prise en compte des problèmes organisationnels). Les risques de détection tardive sont liés à la défaillance des systèmes d'information (internes et externes) et au traitement de l'information (disponibilité de l'information et des moyens de traitement). Les risques de diagnostic erroné sont liés à la mauvaise identification de la cause et à la représentation mentale du réel. Les risques de réponse inappropriée sont liés à la recherche d'un bouc émissaire tiers, au souci de temporiser et à l'excès de procédures (création de nouvelles règles conduisant à l'asphyxie du système).

- L'analyse par cause distingue les risques pays (risques politiques, administratifs, risques financiers, fiscaux, de change, événements naturels), le risque client (risques de concurrence et insolvabilité, risques d'appels excessifs en garantie, risques d'interruption de contrats), les risques produits (risques d'inexpérience d'étude et de conception, risques de méconnaissance des besoins réels des clients), les risques contractuels (risques de précipitation ou d'erreurs, risques de litiges, risques sur l'estimation des conditions de paiement, risques sur le juridique), les risques fournisseurs (défaillance, solvabilité), les risques internes de réalisation (risques sur études, fournitures et travaux, modification des cas de force majeure, risque du personnel, risque de la réception, non-conformité, performance, transport, emballage, pilotage), le risque d'atteinte de l'image de marque, les risques de dommages (matériels ou corporels, indirects ou immatériels).
- L'analyse par origine d'H. Courtot sépare les aléas (liés à la définition, à une définition insuffisante, à des antécédents inquiétants, à des technologies risquées, à des besoins très importants de recherche & développement, à des intervenants peu fiables), les risques externes potentiels, incontrôlables et non évaluables (intervention administrative, phénomènes naturels, malveillance, sabotage, vandalisme, effets indirects, sociaux, politiques, écologiques), les risques externes évaluables, non contrôlables (marché, concurrence et fourniture, coût de possession de l'ouvrage, change, inflation), les risques internes non techniques évaluables plus ou moins contrôlables (difficultés managériales, maîtrise des délais insuffisante, maîtrise insuffisante des coûts, rupture de trésorerie), les risques techniques généralement contrôlables (modification dans la technologie, maîtrise insuffisante des processus, dimension et ou complexité du projet), les risques juridiques contrôlables (licences, permis, brevets, les problèmes contractuels, la rupture de contrat, le contentieux).

Cette manière d'aborder la gestion des risques est pourtant très loin d'avoir pris en compte ce qu'il est convenu d'appeler « la crise de la prescription ». Elle ignore en effet toutes les difficultés de l'élaboration et de la gestion de la règle au regard d'un risque dont la cause et / ou les effets sont considérés comme étant même identifiables, perspective reposant sur un véritable « impensé » du collectif (de son mode de construction à ses modalités de fonctionnement). Et c'est pourtant bien de cela dont il est question dans les enjeux de la gestion du risque. Le modèle implicite univoque est ce que l'on peut qualifier de modèle de substitution de la machine à l'homme, modèle que nous avons déjà qualifié plus haut de vieux projet du « management scientifique » alors qu'il est fondamentalement question de complémentarité donc de coopération de l'homme et de la machine et des hommes entre eux dans les contours d'un collectif technoscientifique. Dans ce vieux projet du management scientifique, il est question de flexibilité par les machines et par les hommes, de vocation à répondre à des conditions de fonctionnement dégradé, mais où sont donc passées les questions de l'autonomie, de la responsabilité, de la confiance, etc. ?

Pour sa part, avec la thématique de l'erreur, J. Reason²⁶ met l'accent sur les modalités de détection de l'erreur (autocontrôle, indication d'erreur par l'environnement, détection d'erreur par des tiers, analyse des taux d'erreurs, typologie des processus cognitifs qui entravent la détection d'erreur comme les biais de pertinence, les explications partielles, l'ajustement apparent du modèle mental, la difficulté à détecter les formes les plus fréquentes d'erreur). Il souligne le potentiel de transformation des erreurs latentes en catastrophes avec des systèmes de plus en plus automatisés venant poser la question du contrôle humain, des omissions liées à l'entretien des installations, des erreurs d'opérateur, des violations (routinières ou exceptionnelles) des règles. Il invite alors à l'évaluation et à la réduction du risque d'erreur humaine compte tenu de méthodes de réduction des erreurs.

Le traitement du facteur humain

Moins centrée sur les instruments que sur les personnes, toute une littérature s'est développée sur la gestion des risques liés à l'articulation des personnes et des systèmes techniques. Il s'agit moins (même si cette perspective ne peut être considérée comme absente dans ces travaux) de faire reconnaître la responsabilité des personnes que de marquer l'irréductible risque de l'articulation des personnes et des systèmes techniques. On assiste d'ailleurs depuis peu au passage de la notion de simulation à celle d'entraînement.

Par exemple, R. Amalberti dans *La conduite des systèmes à risques*²⁷ part d'un postulat qui tend à constituer un véritable dogme dans les travaux de ce type : celui de la rationalité limitée des agents. La gestion des risques pourrait en quelque sorte être assimilée à un projet d'action organisée à partir d'agents dont on doit considérer l'*a priori* ontologique de leur rationalité limitée. L'autre postulat est celui du déterminisme technologique qui fait de l'homme le facteur principal venant engendrer le danger dans le fonctionnement des systèmes techniques. Il va ainsi mettre en avant le concept d'acceptabilité du risque (interprété dans une perspective utilitariste sur la base d'un calcul de type conséquentialiste, le coût de la réduction du risque venant obérer la perspective d'efficacité qui est aujourd'hui un des caractères marquant des systèmes techniques).

L'agir humain s'inscrit donc dans une évidence des systèmes sociotechniques possédant les caractéristiques suivantes :

- Les processus sont dynamiques (d'où leur évolutivité qui les rendent délicats à contrôler) ;
- Ils restent sous le contrôle hiérarchique d'agents humains chargés de " conduire " le système ;
- Ils induisent deux risques : le risque d'accidents techniques, " externes " en quelque sorte à la présence d'agents humains car liés à leur substance technique même et le risque d'accidents liés à l'articulation avec des agents humains ;
- Leur existence est « macro-systémique » car ils s'inscrivent toujours en relations avec d'autres systèmes.

L'auteur formule également le constat de l'éloignement croissant de l'opérateur du résultat du

²⁶ J. Reason, *Human Error*, Cambridge University Press, 1990, 9781139062367, DOI: <https://doi.org/10.1017/CBO9781139062367>

²⁷ R. Amalberti, *La conduite des systèmes à risques*, PUF, collection « Le travail humain », Paris, 2001

processus (par la mise en œuvre d'une assistance technologique accrue) et l'injonction (demandée et obtenue) d'efficacité. Il constate donc le paradoxe du développement de systèmes plus fiables et plus efficaces, mais de risques résiduels qui, lorsqu'ils conduisent à l'accident, sont devenus plus intolérables du fait du « lot » humain concerné et aussi du fait, dirions-nous, d'une idéologie sécuritaire devenue de plus en plus légitime et actée, en particulier, par des jugements de justice. En d'autres termes, les enjeux de la gestion technique des processus ont évolué dans deux directions : la réduction de la fréquence des pannes mais aussi de l'erreur humaine par recours croissant à l'automatisation et le développement du retour d'expérience pour mieux estimer le risque de défaillance et prendre des mesures pour que les défaillances observées ne se reproduisent plus.

Pour R. Amalberti, cette perspective conduit à trois enjeux : pour les fiabilistes, il s'agit de détecter les erreurs et de mesurer le risque de leurs conséquences, pour les concepteurs, il s'agit de protéger le système contre le risque d'erreur humaine en le rendant plus tolérant à celles-ci et en multipliant les redondances d'affichage de l'erreur et, dans le domaine de l'aide, il s'agit de prendre en compte l'importance croissante accordée à l'aide au pilotage. C'est la gestion de ces enjeux qui conduit au déclassement des perspectives de la gestion par exception (gérer le risque lors de son occurrence en faisant son possible pour qu'il ne se reproduise pas ensuite) pour celle d'une gestion « positive » et continue du risque.

Il est donc important de proposer une typologie des facteurs de risque et l'auteur en propose la suivante :

- Les facteurs temporels avec la dynamique du processus qui permet de distinguer entre processus (ou phases de processus) longs et processus lents, la dynamique du processus ayant des conséquences en termes de prédictibilité de l'issue et en termes de réversibilité, la pression temporelle qui pèse sur l'opérateur, les systèmes de référence temporelle du processus (la question des synchronismes) ;
- Le risque avec : le risque externe car extérieur au sujet, le risque interne lié au sujet qui se décompose entre le risque de savoir-faire (celui d'un savoir-faire insuffisant) et le risque de ne pas savoir gérer ses ressources au moment opportun ;
- La coopération entre acteurs avec : les facteurs induits par la structure hiérarchique, les facteurs induits par les structures fonctionnelle et temporelle ;
- Les problèmes d'interface ;
- La question de l'expertise avec : la question de la représentation de la situation, des objectifs et de ses propres savoir-faire ; la limitation des ressources cognitives qui vient poser la question de la focalisation de l'attention du fait de la fragilité des processus « attentionnels », de la fatigue liée à la charge de travail ; la question du partage des représentations entre les agents impliqués par la même difficulté.

Cette typologie conduit à pouvoir proposer des modes de structuration de stratégies de gestion des risques dont les ingrédients sont les suivants :

- La gestion des compétences ;
- La planification et l'anticipation à la fois comme outil de représentation et comme outil de résolution de problème ;
- Le repérage des compromis cognitifs dont les ingrédients sont les suivants : degré de parallélisme ou non des activités (en série alors), degré d'autonomie de la compréhension par rapport à l'action ;

- La protection contre ses propres erreurs qui pose le problème de leur détection et celui de la protection contre celles-ci ;
- La question de la confiance (dans le système, en soi) et de la prise de risque calculée pour éviter d'autres risques.

Dans un autre texte, ce même auteur²⁸ fait le point sur l'approche ergonomique des erreurs et des risques en signalant ce qu'il qualifie de tabous de la sécurité ayant engendré la logique intégriste de l'« assurance qualité » pour arriver au « zéro défaut ». C'est ce qui conduit, à ses yeux, à une méprise quant à la sécurité technique qui s'est pourtant considérablement accrue du fait des évolutions techniques de ces dernières décennies, donnant l'illusion que les actions sur le facteur humain n'ont eu que peu d'effet (car améliorer un système déjà sûr est toujours plus difficile qu'améliorer un système moins sûr) compte tenu d'une croissance considérable de la taille des systèmes (multiplication des agents). Or, la plus grande sécurité a rendu les agents de la société plus intolérants à l'accident dont le coût de réparation (judiciaire entre autres) s'est considérablement accru.

Les approches ergonomiques et de qualité se sont souvent limitées à l'étude objective des situations de travail et elle se sont fait piéger en ignorant le constat effectué ci-dessus et dans la recherche exclusive du diagnostic et de l'évitement des défaillances humaines. Les analyses d'erreurs ont contribué à créer plus d'encadrement et de procédures. En même temps, l'écart entre le perçu et le prescrit s'est accru car la façon d'exécuter le travail n'a pas changé, mais est devenue, du fait de la multiplication des procédures, plus difficile à cause de la réduction du périmètre d'autonomie autorisé (paradoxe de l'injonction hétéronome à l'autonomie). Une partie de l'ergonomie s'est consacrée à la critique de ses propres actions de contingentement de l'erreur, semant la confusion dans le bien fondé de ses fondements. Comme l'indique R. Amalberti, « *le premier mécanisme de rupture est l'excellence du niveau atteint en sécurité dans la plupart des industries, qui en retour a dévalué les moyens, les approches et les dogmes classiques proposés par les approches facteurs humains* »²⁹. Par ailleurs, l'analyse du risque concerne plus aujourd'hui la question des conflits entre les sécurités que celle de la défaillance d'une sécurité.

Il propose ici de distinguer entre trois objectifs :

- Un objectif individuel de bien être personnel qui est confronté au risque de dégradation de l'intégrité ou de la liberté de l'individu et au risque lié au préjudice de carrière que peut entraîner une faute professionnelle (avec, par exemple, l'engagement d'une responsabilité juridique individuelle) ;
- Un objectif de production lié aux catégories techniques et commerciales confronté aux risques des objectifs de qualité, de maintenance, de productivité, etc. ;
- Un objectif de qualité managériale confronté aux risques de qualité de l'équipe de direction en général et dans ceux de ses politiques organisationnelles, de ressources humaines, financière et de ses choix stratégiques, etc.

Les catégories de la gestion du risque devraient donc alors plutôt viser le contrôle des situations

²⁸ R. Amalberti, « Approche ergonomique des erreurs et des risques », in C. Gilbert (Ed.), *Risques collectifs et situations de crise – Apports de la recherche en sciences humaines et sociales*, L'Harmattan, collection « Risques collectifs et situations de crise », Paris, 2003, p. 187-197

²⁹ R. Amalberti, *op. cit.*, p. 190

que le contrôle des erreurs ce qui conduit à mettre en avant un modèle de sécurité écologique reposant sur :

- Un résultat acceptable et non un jugement événementiel instantané et pointilliste, ce qui ouvre l'espace de récupération des aléas et des erreurs ;
- L'erreur à ne considérer que comme une variable accessoire du processus (et non une variable essentielle), la compréhension des situations et la valorisation de l'expérience venant jouer un rôle important dans les compromis de compréhension ;
- La maîtrise des situations qui devrait être aidée par des heuristiques de situations de travail « aux limites » et non pas « en conformité » : les problèmes sont repérés précocement et s'explicitent quand ils peuvent être résolus de façon triviale.

La thématique de la captation totale de l'attention est en effet plus source d'erreurs qu'il n'y paraît (erreurs dans la phase de relaxation, déséquilibres psychologiques durables, etc.). Une sécurité imparfaite régule le risque au contraire de la fiction d'un système apparemment trop sûr. C'est alors la logique du « suffisant » qui l'emporte.

D. Pécaud³⁰ est beaucoup plus critique quant à la convocation de la notion de « facteur humain », en particulier au regard du traitement qui lui est réservé :

- Que veulent désigner ceux qui utilisent la notion ? Est-ce le travail humain pour mieux le dominer ?
- A l'inverse, la notion pourrait recouvrir l'idée de résistance à la généralisation des protocoles.
- Elle pourrait être comprise comme l'« objectivation » du facteur humain dans les catégories normatives de l'individualisme méthodologique, y compris sous la version de l'opportunisme.

L'emphase des catégories de l'audit

Toute activité humaine est susceptible d'examen sans pour autant que tout examen soit pertinent. L'audit dont il est question ici est bien l'audit opérationnel, mais il ne faut pas oublier que l'audit débouche sur l'expression d'une opinion et vise à éviter et éliminer les risques et les fraudes. L'audit est aussi un projet d'obéissance à la conformité voire de la construction d'un conformisme ... Et parfois mince est la frontière entre conformité et conformisme, comme c'est déjà le cas avec les normes qui servent si souvent de référentiel aux démarches d'audit. On retrouve, dans la gestion des risques, des caractéristiques plus générales qui existent aussi dans l'audit : le secret professionnel, l'indépendance, l'engagement de la responsabilité. La typologie des opérations visées par l'audit qui distingue les opérations répétitives des opérations non répétitives induit un regard différent sur le risque suivant les deux cas. Par ailleurs, la représentation du risque en audit (distinction entre risque inhérent – risque de contrôle interne - risque de non-détection) retrouve en gestion des risques une forme assez proche. Tout comme les modalités de la gestion des risques, l'accent y est mis sur le système de documentation et d'information, le système de preuves (les traces laissées sur la piste d'audit), les moyens matériels de protection, le personnel, le système de supervision. La crise actuelle de légitimité venant concerner l'entreprise conduit au sentiment qu'elle ne saurait plus être garante des sécurités nécessaires à la vie quotidienne. La difficulté du cadre institutionnel à la garantir « fait système » avec la suspicion adressée à l'entreprise. La réponse est passée par l'exacerbation des

³⁰ D. Pécaud, *Risques et précaution – L'interminable rationalisation du social*, Editions La dispute, Paris, 2005, p. 52 et suivantes

catégories de l'audit qui n'a eu de cesse d'élargir ses compétences en s'adressant directement au thème du risque lui-même au regard de l'expérience de détection et de contrôle qui serait la sienne même si rien n'a changé quant au fond. C'est sans doute ce qui peut justifier que les professionnels de l'audit, en particulier ceux de l'audit opérationnel, puissent lorgner sur des aspects de la gestion des risques. En effet, rappelons que, d'après J.-C. Bécour & H. Bouquin, l'audit opérationnel « *s'intéresse à la manière dont l'entreprise ou certaines de ses entités définissent et respectent leurs objectifs et leurs politiques, obtiennent, préservent, allouent et consomment tous les moyens nécessaires pour ces fins* »³¹.

Avec la gestion du risque, on doit bien noter la quête effrénée de dispositifs de détection et de contrôle à défaut et à la place d'une législation. Cette quête effrénée se situe dans une conception du risque qui relève d'un postulat de leur objectivisation possible, objectivisation autorisant alors une définition instrumentale de la notion. En quelque sorte, le risque apparaît quand on lui attache une valeur. *A contrario*, une telle conception ignore une conception immanente du risque, immanence liée à la vie et à l'activité, immanence « normale » du risque en quelque sorte, immanence qui en ferait tout autre chose qu'un problème à résoudre. Et c'est là que l'on retrouve la question de la confiance généralisée dont il était question avec A. Giddens et la société entrepreneuriale par nature³².

³¹ J.-C. Bécour & H. Bouquin, *Audit opérationnel – Efficacité, efficacité ou sécurité*, Economica, 2^e édition, 1996

³² A. Giddens, *Les conséquences de la modernité*, Paris, L'Harmattan, 1994.