CHAIRE JARISLOWSKY
ÉCOLE POLYTECHNIQUE MONTRÉAL
CIRANO

RISQUES TECHNOLOGIQUES

BULLETIN DE LIAISON

Été 2001
Volume 5, N° 1

Nouvelles technologies, nouveaux risques?

Les entreprises semblent sous-estimer les risques qui apparaissent avec l'Internet

par ***Nathalie de Marcellis****, CIRANO et GRID – ENS Cachan*

Le développement des nouvelles technologies de l'information et de la communication a eu un impact important sur les activités des entreprises et leurs performances. L'utilisation de plus en plus fréquente des outils informatiques, la mise en place de réseaux de plus en plus étendus et l'apparition de *l'Internet* contribuent à assurer des opportunités d'augmentation de la connectivité et de la flexibilité des entreprises. De plus, de nouvelles stratégies commerciales sont rendues possibles. Les entreprises disposent désormais d'un outil convivial et simple d'utilisation pour se faire connaître (*site web*) et vendre leurs produits (*site web avec espace marchand*). Toutefois, les entreprises ne doivent pas négliger leur vulnérabilité croissante face à l'apparition des risques qui accompagnent l'évolution des technologies : « les menaces sont à la hauteur des enjeux » (Lamère, 1997). La malveillance informatique est de plus en plus considérée comme « le risque technologique numéro un des entreprises » (CEA, 1997).

Le démarrage de ce projet a été rendu possible grâce à AGRA Monenco Inc., à la Chaire Jarislowsky et à la subvention du CRSNG accordée au Réseau de calcul et de modélisation mathématique (RCM_2).

PARTENAIRES

CIRANO - Centre interuniversitaire de recherche en analyse des organisations.

Centre de sécurité civile de la communauté urbaine de Montréal.

RESPONSABLES DU PROJET

Bernard SINCLAIR-DESGAGNÉ Ph.D.

Nathalie de MARCELLIS Ph.D.

CHERCHEURS PRINCIPAUX

Marcel BOYER Ph.D. professeur à l'École Polytechnique de Montréal et au Département de sciences économiques de l'Université de Montréal, titulaire de la Chaire Jarislowsky, président-directeur général du CIRANO.

Bernard SINCLAIR-DESGAGNÉ Ph.D. professeur au Département de mathématiques et de génie industriel de l'École Polytechnique de Montréal, directeur de recherche au CIRANO, chercheur invité à l'École Polytechnique de Paris.

Nathalie de MARCELLIS Ph.D. chercheure post-doctorale au CIRANO, chercheure associée au GRID–ENS (Cachan).

Les nouveaux risques qui apparaissent

Les entreprises doivent identifier les événements indésirables liés à l'utilisation de l'Internet. Internet fait apparaître de nouveaux risques et a un effet aggravant sur les risques informatiques déjà connus, comme les virus. De nombreux exemples peuvent être donnés et les caractères « multiformes » et « multisources » des menaces encourues peuvent être soulignés.

Les événements indésirables

Via Internet, un utilisateur, appelé « internaute », peut :

- attaquer le réseau ou le paralyser par le système ou par les données. L'attaque type consiste en l'injection sur le réseau de l'entreprise d'un code malicieux appelé « Cheval de Troie ». Ce dernier permet d'ouvrir des failles de sécurité et de donner le contrôle du réseau à distance en passant outre les systèmes de surveillance. Nombre d'entre eux sont identifiés et peuvent parfois être éradiqués à l'aide d'un simple antivirus mis à jour. Certaines attaques peuvent déclencher un encombrement majeur des lignes avec des connexions qui se démultiplient et qui rendent les services du site non accessibles ou avec une « inondation » de messages email qui rend indisponible la messagerie.

- pirater un site Web et altérer le contenu des pages Web ou le détourner (l'adresse renvoie à un autre site). Ces menaces peuvent faire subir à l'entreprise un préjudice en terme d'image mais aussi engager sa responsabilité si les informations modifiées à son insu sont utilisées par des tiers.

- usurper l'identité d'un partenaire d'échange, imiter des signatures électroniques, détourner des fichiers clients ou même détourner des fonds électroniques, etc.

Les entreprises ne doivent pas négliger leur vulnérabilité croissante face à l'apparition des risques qui accompagnent l'évolution des technologies : « les menaces sont à la hauteur des enjeux ».

Les spécificités du commerce électronique

Beaucoup d'entreprises ont fait leur entrée dans le commerce électronique[1]. Avec Internet, les entreprises peuvent faire du commerce au niveau mondial et ainsi trouver de nouveaux marchés. Toutefois, les entreprises ne doivent pas négliger les problèmes d'intendance des sites marchands mais aussi les risques spécifiques qui peuvent apparaître avec le cyber-commerce. Un contrat de vente sur Internet est assimilé à un contrat de vente à distance. Toutefois, les échanges étant dématérialisés, la preuve de la vente est plus complexe. Elle peut se faire par une signature électronique fiable et par la conservation durable du message. Un autre problème est lié au paiement qui se fait directement en ligne. Beaucoup de clients hésitent encore à divulguer leur numéro de carte de crédit. Ils pourraient être la cible de hackers et ceci même si le numéro est crypté[2]. De plus, certains internautes malveillants utilisent des faux numéros de cartes de crédit qu'ils ont créés. Tout cela, au détriment par exemple des fournisseurs de services, qui se trouvent dans l'impossibilité d'identifier les fraudeurs et donc d'engager une procédure contre eux. De plus, le commerce électronique étant par nature international, en cas de conflit des problèmes de législation vont se poser : est-ce la loi du pays d'émission ou de pays de réception qui va s'appliquer ?

La malveillance informatique : menaces internes / menaces externes

Les risques informatiques sont en général analysés selon trois grandes catégories de causes : accidents (physiques, pannes, etc.), erreurs (d'utilisation, de conception ou de réalisation) et malveillances (fraude, sabotage, attaques logiques, divulgation de données, etc.). C'est ce dernier point qui pose le plus de problèmes. En 1996, deux tiers des entreprises françaises ont été victimes de fraudes informatiques et toutes sont susceptibles d'être à nouveau concernées. Au Canada, les chiffres sont équivalents (KPMG, 2000). Récemment, la court Québécoise a condamné un jeune homme de 22 ans pour s'être introduit dans les ordinateurs du gouvernement. En Ontario, un homme a été condamné pour s'être introduit frauduleusement dans les bases de données

(Suite page 2)

(Suite de la page 1)

de la NASA. Ainsi, avec Internet, les risques liés à la fraude informatique sont démultipliés. Le piratage et la malveillance touchent n'importequel type d'entreprise. Toutefois, à chaque type d'activité correspond une exposition particulière et les risques sont spécifiques par secteur (il faut distinguer les institutions financières, les sociétés commerciales et les sociétés industrielles). De plus, un effectif plus important et l'existence de localisations diverses augmentent l'exposition.

Le Cabinet Ernst & Young a publié en 1998 une liste des principales provenances des menaces informatiques[3]. Les agresseurs externes sont souvent des hackers expérimentés (dans certains cas, ils sont « envoyés » par des concurrents). Toutefois, un grand nombre d'experts estiment le risque émanant des salariés plus important que celui provenant de l'extérieur car ceux-ci peuvent disposer d'une connaissance beaucoup plus pointue des systèmes sur lesquels ils sont présents. Enfin, les partenaires et les employés des fournisseurs représentent une menace grandissante, notamment en raison de la croissance des extranets. De plus, il peut s'agir d'un employé d'une société de service sous-traitée pour la maintenance des machines ou pour la mise en conformité des systèmes (pour le passage à l'an 2000 et en Europe, pour le passage à l'euro). Dans 80 % des cas, l'auteur ou le complice a ou a eu une relation contractuelle avec l'entreprise victime.

Les conséquences

L'utilisation des réseaux et des nouvelles technologies aggrave le risque sur les informations en matière de *disponibilité*, *d'intégrité* (l'information ne peut être modifiée en principe que par les utilisateurs habilités), de *confidentialité* et *d'imputabilité* (propriété qui permet d'imputer de façon certaine une opération à un utilisateur à un moment donné). Les conséquences sont donc liées directement à la perte de données (coût de reconstitution), à la perte d'exploitation engendrée (en cas d'indisponibilité du réseau), à la fraude (remboursement de sommes d'argent détournées) ou à la reconstitution de l'image (après diffamation). Une enquête récente du FBI et de l'Institut de Sécurité informatique a montré que les pertes dues à la malveillance informatique avaient dépassé les 360 millions de dollars entre 1997 et 1999. Le « e-crime » suit donc la croissance du « e-business ».

Un grand nombre d'experts estiment le risque émanant des salariés plus important que celui provenant de l'extérieur.

Une vulnérabilité sous-estimée

Les résultats d'une enquête récente du cabinet KPMG (KPMG, 2001) sont alarmants. Les nombreuses lacunes en matière de sécurité informatique montrent que les entreprises n'ont pas encore mesuré la vulnérabilité liée à l'utilisation de l'Internet. Par exemple, 29 % des entreprises qui ont une connexion Internet n'ont pas de système de sécurité adapté. De plus, depuis la mise en place d'une connexion Internet, très peu d'entreprises ont modifié leur logique de contrôle d'accès. Les entreprises interrogées ont du mal à comprendre les risques de « l'économie électronique ». Même si les entreprises admettent l'existence de risques, 40 % des risk-managers interrogés avouent n'avoir qu'une connaissance médiocre en ce domaine. De plus, les risques de malveillance (fraude, vol de propriété intellectuelle, etc.) restent un sujet tabou. Les entreprises victimes ne souhaitent pas dévoiler les défaillances de leurs systèmes informatiques, pour des raisons d'image ou par rétention de l'information des services concernés (qui veulent éviter d'attirer l'attention des actionnaires).

L'incertitude rattachée à l'utilisation des réseaux informatiques et la complexité des systèmes en réseaux vont obliger l'entreprise à adopter une démarche globale de gestion des risques.

Les solutions

De nombreux exemples montrent que les entreprises n'ont pas mis en place de politique de gestion adaptée aux spécificités de ces risques et ceci même dans les secteurs où l'informatique est l'outil de production (cas de la banque ou de l'assurance). L'entreprise doit prendre en compte ces différents problèmes pour se préparer aux éventuels risques associés à l'utilisation de l'Internet et à ce nouveau type de commerce. Ainsi, l'incertitude rattachée à l'utilisation des réseaux informatiques et la complexité des systèmes en réseaux vont obliger l'entreprise à adopter une démarche globale de gestion des risques qui prenne en compte l'évolution continuelle des systèmes, l'apparition de nouveaux risques et l'aggravation des risques existants, la spécificité de la structure en réseau et l'environnement législatif et social. Les entreprises doivent identifier les types d'agresseurs réels et potentiels et quelles sont leurs pratiques. L'entreprise doit être vigilante à l'égard de son personnel, de ses collaborateurs, de ses partenaires et des prestataires extérieurs qui interviennent ponctuellement. Cette connaissance participe en effet au critère de définition de la politique de sécurité, notamment pour adapter les systèmes de protection aux différents types d'attaques. Au « e-crime », il faut une politique de « e-secure ». De plus, les entreprises peuvent chercher à transférer leurs risques. Toutefois, les solutions d'assurance ont tardé à apparaître. Une étude des perspectives assurantielles pour les risques liés aux NTIC (de Marcellis & Gratacap, [1998]) a montré que les assureurs sont très attentifs à l'essor des NTIC mais en l'absence de cadre juridique stable, ils avaient hésité à proposer des solutions globales. L'absence d'une demande d'assurance importante a aussi freiné l'essor des nouveaux contrats. Aujourd'hui, la plupart des grandes compagnies d'assurance (Lloyd's, AIG, Chubb, Zurich, AXA, etc.) proposent des produits spécifiques en cas d'interruption électronique des affaires pour cause de « cyber-vandalisme ».

Bibliographie

Comité Européen des Assurances, 1997, *« Internet… menaces, sécurité et assurance»",* hors-série n°6, Décembre.

De Marcellis N. & A. Gratacap, 1999, « Technologies de l'information et de la communication et gestion des risques : bilan et perspectives assurantielles pour l'entreprise » , *Revue Communications et Stratégies,* n°33.

Lamère, J.M, 1997 , *« Les risques des nouvelles technologies de l'information »*, in Encyclopédie de l'assurance, publiée sous la direction de F. Ewald et J.H Lorenzi, Economica.

Reboul P. & D. Xardel, 1997, *Le commerce électronique : techniques et enjeux*, Eyrolles.

Rapport KPMG, 2001, « 2001 Global e.fr@ud. survey "».

Rapport KPMG, 2000, « E-Commerce and Cyber Crime in Canada : new strategies for managing the risks of exploitation ».

[1] En 2000, le commerce électronique représentait 5,3 % du PIB aux Etats-Unis.

[2] Cette méthode est aussi appliquée pour récupérer les codes d'accès et les mots de passe. Les protections de l'entreprise (Fire-wall) peuvent ainsi être franchies sans problème.

[3] Enquête sur la montée du crime informatique – Les Echos – 10 février 1998.

Événements passés

- Bernard Sinclair-Desgagné a prononcé une conférence le 15 janvier 2001 au ministère français de l'environnement sur « L'entreprise privée et l'environnement ». Cette conférence fait partie des séminaires Claude Henry, financés par la fondation de l'Ecole Polytechnique de Paris, qui ont pour but de présenter aux décideurs les avancées récentes en économie de l'environnement.
- Nathalie de Marcellis a fait un séminaire au CIRANO le vendredi 9 février 2001 : « Une analyse expérimentale des décisions de l'assureur : des risques informatiques classiques aux risques qui apparaissent avec l'Internet ». Un cahier de recherche CIRANO sera bientôt disponible.
- Nathalie de Marcellis a présenté un article intitulé « An Analysis of the French Insurance Scheme against Natural Catastrophes » écrit en collaboration avec E. Michel-Kerjan (Ecole Polytechnique de Paris & GREQAM) et T. Warin (CREFE – UQAM & CIRANO) au 41ème Congrès annuel de la Société Canadienne de Science Economique qui s'est déroulé à Québec les 16 et 17 mai 2001.

Assurance des Catastrophes Naturelles :

les spécificités du système français

par ***Nathalie de Marcellis****, CIRANO et GRID – ENS Cachan*
et ***Erwann Michel-Kerjan****, École Polytechnique de Paris, GREQAM et CIRANO*

L'année 1999 fut la seconde année la plus coûteuse de toute l'histoire de l'assurance mondiale[1]. Les tempêtes *Lothar* et *Martin* qui dévastèrent l'Europe de l'Ouest en décembre 1999 causèrent, en France, le décès de 92 personnes et des dégâts assurés d'un montant supérieur à 7 milliards d'euros. Cette catastrophe a démontré la vulnérabilité de la France aux événements climatiques à grande échelle et projeté sur le devant de la scène publique la question de l'indemnisation des victimes, et donc celle de l'assurance de tels événements.

Depuis 1982[2], il existe en France un système unique d'assurance des Catastrophes Naturelles fondé sur une entente entre le gouvernement, les compagnies d'assurance privées et un réassureur public, la *Caisse Centrale de Réassurance*. L'indemnisation est du ressort des compagnies d'assurance (la garantie Cat. Nat. est une extension de garanties dommages existantes) mais c'est l'Etat qui fixe les conditions d'assurance et qui met en place les mesures de prévention. Dans ce domaine aussi, il conviendrait de parler d'exception française tant est spécifique le système en vigueur. En termes d'indemnisation, son fonctionnement a rarement été mis en défaut. Si bien qu'un nombre croissant d'institutions (notamment la Banque Mondiale) et de gouvernements étrangers, aux Etats-Unis[3], en Asie ou encore en Europe[4], envisagent de le reproduire ou de s'en inspirer. Sont présentées ici certaines caractéristiques du système[5] dont les plus récents changements entrés en vigueur au 1er janvier 2001.

Une double couverture

Il existe en France deux « types » de couverture suivant l'événement naturel considéré. Les dégâts dus aux effets du vent, de la grêle, du gel, du poids de la neige, considérés comme *assurables*, sont couverts par *la garantie tempête*, incluse, depuis 1990, dans tout contrat d'assurance habitation, et sont alors pris en charge exclusivement par les compagnies d'assurance sans intervention de l'Etat. Les dégâts dus aux événements naturels considérés comme *non assurables* (par exemple, mouvements de terrain, séismes, avalanches, sécheresse, inondations,…) sont exclus de cette garantie mais peuvent être pris en charge au titre de la *garantie catastrophes naturelles* (Cat. Nat.). Néanmoins, il revient au législateur (Ministère de l'Intérieur) de décréter les zones touchées en « état de catastrophes naturelles », condition nécessaire pour l'indemnisation des victimes[6]. Dans ce cas, le système mixte spécifique aux événements qualifiés de « catastrophes naturelles » est activé.

Fonctionnement du système

Reposant sur un principe de solidarité nationale, une surprime catastrophe naturelle est prélevée sur tous les contrats d'assurance dommages aux biens (contrats « socle »). Celle-ci est définie par un taux de surcharge (fixé par la direction de Trésor au Ministère des Finances) identique sur tout le territoire et appliqué à la prime d'assurance payée par l'assuré (personne physique ou morale) : plus élevée est la prime du contrat socle, plus la surprime catastrophe naturelle payée par l'assuré à son assureur le sera également[7]. Initialement fixé à 5,5 % pour les biens autres que les véhicules terrestre à moteur, ce taux s'élève aujourd'hui de 12 % des primes ou cotisations afférentes au contrat de base (800 millions d'euros de primes cat. nat. en 1999).

Pour favoriser l'adhésion des assureurs à ce système, l'Etat a mis en place un système de réassurance par le biais de la *Caisse Centrale de Réassurance* (avec un traité de réassurance original combinant quote-part et excédent de pertes annuelles) dont il est l'unique actionnaire. L'Etat se pose également en garant de la CCR. Cela signifie qu'il assure une garantie illimitée des indemnisations, et c'est bien là une particularité du système. Les assureurs se réassurent en grande majorité auprès de la CCR, même si tout assureur est libre de se garantir auprès d'un autre réassureur de son choix, voire même ne pas se réassurer du tout. A la naissance du système, le taux de cession à la CCR, en garantie cat. nat., a été relativement élevé (supérieur à 80 %). Puis, il a chuté au fil des ans, synonyme à la fois d'une meilleure connaissance du domaine par les assureurs et d'une sinistralité plus faible, pour atteindre une moyenne de 43 % en 1988. En 1982, la CCR proposait des traités de réassurance où le taux de cession pouvait varier entre 40 % et 90 %. Dans les années 90, suite à une forte sinistralité due aux nombreuses inondations (dommages assurés pour 92/96 : 1,5 milliards d'euros) et sécheresses (1,4 milliards d'euros pour 1996/98) déclarées catastrophes naturelles, le taux maximal offert a été ramené à 60 % le 1 janvier 1997. D'ailleurs, depuis le 1er janvier 2000, la CCR n'offre plus aux assureurs qu'un taux unique de cession en quote-part de 50 % et le commissionnement en réassurance à été annulé.

La réussite du système repose sur quatre atouts majeurs :

- L'obligation d'assurance : le système s'appuie donc sur l'assiette de prélèvement maximale : l'ensemble des foyers et des entreprises du pays;
- L'existence d'un taux unique, au nom de la solidarité nationale face aux catastrophes naturelles ;
- Le partenariat avec l'industrie de l'assurance : il présente deux avantages, i) il est facile à un assureur d'ajouter une ligne de risque à son portefeuille sans grand changement de gestion; ii) il existe en France un réseau très dense d'agents d'assurance qui permet des procédures d'expertise des dommages et une indemnisation plus rapides que dans le cas d'un fonds public d'indemnisation (la loi fixe le délai maximal des indemnisations à trois mois).
- La possibilité de se réassurer auprès de la Caisse Centrale de Réassurance : elle présente un avantage comparatif certain en disposant d'une garantie illimitée de l'Etat.

Les tempêtes de 1999 furent un test grandeur nature pour toutes les composantes de ce système[8]. En effet, il convient de rappeler que « seulement » 305 millions d'euros (garantie cat. nat.) des 7,3 milliards d'euros de dommages assurés furent pris en charge par ce système. Néanmoins, pour la première fois de son histoire, la CCR, dont les réserves d'égalisation ne s'élevaient qu'à 150 millions d'euros, a du faire appel à la garantie de l'Etat. Les assurés ont été indemnisés assez rapidement au regard de l'ampleur de l'événement. De ce point de vue, le système a prouvé son efficacité.

Un nombre croissant d'institutions (notamment la Banque Mondiale) et de gouvernements étrangers, aux Etats-Unis, en Asie ou encore en Europe, envisagent de reproduire le système français ou de s'en inspirer.

Limites actuelles

Néanmoins, la recrudescence actuelle d'événements dans des zones d'habitation et/ou industrielles posent certaines questions de fonds au système en place. Nous en évoquons quatre :

- Si la France admet plus volontiers que d'autres pays l'idée même d'égalité face aux catastrophes et donc de solidarité nationale, le taux de surprime étant identique pour tous les risques, il n'incite guère à des comportements de prévention (phénomène de hasard moral).
- La réalisation des *Plans de Prévention des Risques* reste timide. L'entrée en vigueur depuis le 1er janvier dernier, pour les localités dépourvues de tels plans, de montants de franchise croissant avec le nombre d'événements identiques et déjà indemnisés par le passé, pourrait inciter à rendre publique davantage d'information sur les risques et donc à plus de prévention.
- Un système de scoring tel que le *Community Rate System* mis en place aux Etats-Unis pourrait être considéré avec bénéfice. Comment mesurer, en l'absence actuelle de connaissance des primes actuarielles sur l'ensemble du territoire, le véritable degré d'efficacité économique d'un tel système?
- Enfin, celui-ci n'est aucunement préparé à faire face à d'éventuels *Big Ones* tels qu'une inondation majeure de la Seine ou de la Loire (on estime à 6 milliards d'euros les dégâts directs qui résulteraient d'une inondation identique à celle survenue en 1856) ou un tremblement de terre à Nice (dommages assurés estimés à près de 20 milliards d'euros; garantie cat. nat. exclusivement).

Depuis 1992, de nouveaux produits ont été créés sur les marchés financiers (CBOT et CATEX). Ils permettent aux assureurs, réassureurs, mais aussi aux gouvernements, de diversifier les risques et d'absorber des montants de dommages, catastrophiques pour eux, dans un marché dont les flux dépassent 19 000 milliards de dollars. Le recours à ces instruments

(Suite page 4)

(Suite de la page 3)

requiert néanmoins une analyse actuarielle poussée des risques qui, n'existe pas encore en France. D'ailleurs, une connaissance qui précise les niveaux de risques, pourrait-elle soutenir très longtemps, autrement que par le pouvoir du législateur, le principe de solidarité qui fait l'essence même de ce système ?

[1] Swiss Reinsurance Company (2000), Sigma No. 2.
[2] *Journal Officiel,* Loi n°82-600 du 13 juillet 1982 relative à l'indemnisation des victimes de catastrophes naturelles.
[3] Cf. les travaux de David Moss à Harvard.
[4] La Commission européenne ayant souhaité la mise en place d'un système européen d'assurance des catastrophes naturelles s'inspirant très largement du schéma français.
[5] Pour une analyse plus détaillée, voir Michel-Kerjan (2001), « Insurance against Natural Catastrophes: Is the French Scheme the Good One? », mimeo, Laboratoire d'économétrie de l'Ecole Polytechnique, Paris.
[6] Voir notamment De Marcellis et Michel-Kerjan (2000), « Tempête ou catastrophe naturelle : Implications sur les systèmes d'indemnisation », Revue *Préventique-Sécurité*, Numéro de Février, pp.42-45.
[7] Munier, B.(1997), « Réflexion sur la prévention des risques naturels et l'indemnisation des dommages », in La prévention des risques naturels, Rapport d'évaluation du Comité interministériel de l'évaluation des politiques publiques, La Documentation Française.
[8] cf. le rapport de la mission interministérielle dirigée par Gilles Sanson sur « l'évaluation des dispositifs de secours et d'intervention mis en œuvre à l'occasion des tempêtes des 26 et 28 décembre 1999 », remis au Premier ministre français en janvier 2001.

Commentaire sur le livre « Entre savoir et décision, l'expertise scientifique » de Philippe Roqueplo (Groupe Sciences et questions, Institut National de la Recherche Agronomique (INRA) – France, 9 avril 1996)

par **Bernard Sinclair-Desgagné**,
École Polytechnique et CIRANO

Dans un monde régi par le pari de l'innovation et par un accroissement vertigineux mais morcelé des connaissances, les responsables politiques et les dirigeants d'entreprise ont sans cesse recours aux avis de spécialistes – médecins, ingénieurs, économistes, informaticiens, psychologues, etc., que ce soit pour bien poser les problèmes ou encore (plus traditionnellement) pour articuler des solutions. Les récentes crises liées au sang contaminé ou à la vache folle ont toutefois révélé les lacunes de certaines pratiques du recours à l'expertise.[1] La question de l'organisation de l'expertise est donc désormais à l'ordre du jour de nombreuses instances politiques et privées dans la plupart des pays industrialisés.

Dans ces circonstances, une personne avertie ne saurait éviter de lire la conférence de Philippe Roqueplo intitulée « Entre savoir et décision, l'expertise scientifique ». Dans un premier temps, l'auteur avance une claire mais fine distinction entre le chercheur faisant œuvre scientifique et celui jouant le rôle d'expert. Contrairement au premier, ce dernier a en effet conscience de participer à un processus de décision; le contexte et les enjeux de ce processus risquent donc d'avoir un impact sur le format, voire la teneur, des connaissances qui seront finalement rendues. Une seconde partie présentent les raisons pour lesquelles on fera de plus en plus appel à l'expertise, le politique devant devenir un interlocuteur privilégié des scientifiques. La troisième partie discute le principal problème que doit affronter le chercheur faisant office d'expert : celui-ci doit la plupart du temps transgresser les limites de son domaine proprement dit, soit par manque de temps, soit par exigence de pluridisciplinarité. Une quatrième partie traite des modes de communication de l'expertise; le pour et le contre de l'expertise confidentielle y sont examinés. Enfin, la conclusion constitue un plaidoyer en faveur de l'institutionalisation des procédures de recours à l'expertise, voire de préparation des chercheurs en ce sens.

Depuis la date où cette conférence à été prononcée, la littérature portant sur l'organisation de l'expertise a véritablement explosé. Les propos de Philippe Roqueplo constituent néanmoins toujours l'une des présentations les plus lucides sur le sujet. Leur conclusion, cependant, laissera peut-être le lecteur sur sa faim, car plusieurs nouveaux points de vue sur l'encadrement institutionnel de l'expertise se font jour depuis quelques mois.[2] Des percées sont actuellement palpables, qui devraient avoir un impact significatif sur le développement de la « nouvelle économie basée sur le savoir ».

[1] A ce sujet, voir l'article d'Olivier Godard, « Vache folle et organisation de l'expertise scientifique », paru dans le numéro de décembre 2000 (vol. 4, no. 4) du bulletin *Risques Technologiques*.
[2] Voir, par exemple, les travaux de Philippe Marcoul, stagiaire post-doctoral à CIRANO de novembre 1999 à août 2000, de même que l'article récent de Bernard Sinclair-Desgagné et Estelle Gozlan, « A Theory of Environmental Risk Disclosure » (Cahier CIRANO no. 2001s-17).

Le CIRANO obtient une importante subvention pour étudier la gestion intégrée des risques, qui comporte un volet sur la gestion des risques technologiques majeurs.

Le ministère de la Recherche, de la Science et de la Technologie a annoncé le 29 janvier 2001 la subvention de deux projets pilotés par le CIRANO dans le cadre des programmes Valorisation – Recherche – Québec (VRQ). Plus spécifiquement, le projet dirigé Michel Patry s'intitule « Développement d'outils de mesure, d'intégration et de gestion des risques ». Il a pour objectif de **fournir aux gestionnaires un outil intégré d'aide à la gestion et de support aux décisions en matière de risque.** Les organisations, qu'elles soient privées ou publiques, fonctionnent dans des environnements turbulents. De plus en plus, elles prennent conscience qu'elles sont sujettes à diverses menaces et qu'elles ne sont plus sûres d'atteindre leurs objectifs que ce soit en terme de rendements ou autres. Reconnaissant cet état de fait, on parle de plus en plus fréquemment de l'analyse des risques auxquels sont soumises les organisations. La gestion des risques exige l'adoption de mesures financières, technologiques et organisationnelles en vue de faire face aux conséquences des différents états de la nature, pour coordonner les actions de gestion de risques afin de dégager une stratégie cohérente. Cette gestion est d'autant plus délicate, que les grandes organisations sont des entités complexes, dont les structures sont à la fois ramifiées et reliées entre elles. De là l'importance d'un outil de gestion des risques comme celui qui est proposé. Cet outil permettra de repérer et de mesurer les différents risques auxquels l'organisation est confrontée, d'identifier les arbitrages qui sous-tendent ces risques, d'évaluer les politiques alternatives de gestion de ces risques et enfin, concevoir et coordonner les stratégies de gestion du risque appropriées. Les risques dont il est question sont de plusieurs ordres : risques d'affaires, risques financiers, risques technologiques (pannes, baisse de performance), risques environnementaux (pollution, changements climatiques), risques contractuels, risques pour la santé de la population. L'outil possédera une architecture flexible et intégrera plusieurs instruments méthodologiques et logiciels à l'intérieur d'une procédure destinée à encadrer la démarche du décideur.

Événements à venir

Séminaire

- Anne Perrot (CREST&LEI – France) donnera un séminaire intitulé **« Politique de concurrence dans la net-économie »** le 13 juin de 9h à 12h au CIRANO.

Conférence

- Le *Laboratoire d'économétrie de l'École Polytechnique* de Paris et le *CIRANO* organisent une conférence interdisciplinaire conjointe sur **« L'organisation du recours à l'expertise scientifique en situation d'incertitude »** les 10 et 11 janvier 2002, à Paris. La conférence s'organisera autour de papiers invités et d'une sélection des papiers proposés. Pour obtenir des renseignements additionnels : *http://www.cirano.qc.ca/risques*

Risques technologiques

CIRANO, 2020, rue University, 25e étage,
Montréal, Québec, H3A 2A5
tél. : (514) 985-4000 # 3120
téléc. : (514) 985-4039
courriel : demarcen@cirano.qc.ca
www.cirano.qc.ca/risques