

**SURVOL**

# **Un panorama des mille et un risques associés au bogue de l'an 2000**

Par Jean-Charles Dubois

Pour le CIRANO —  
le Centre interuniversitaire de recherche  
en analyse des organisations

Février 1999

# Un panorama des mille et un risques associés au bogue de l'an 2000

Par Jean-Charles Dubois\*  
ariska@videotron.ca

Février 1999

---

\* Le présent document exprime uniquement l'opinion de l'auteur. Par conséquent, il n'engage aucunement le CIRANO – le Centre interuniversitaire de recherche en analyse des organisations – commanditaire de l'étude.

L'auteur remercie ceux qui ont fourni de l'information sur le statut de conformité de leur organisation. Il remercie également Bernard Sinclair-Desgagné pour ses conseils judicieux et pour la révision du document.

Jean-Charles Dubois est président de Ariska, une société conseil en gestion du risque, processus et informatique. Il détient un maîtrise en Systèmes d'Information de l'Université de Sherbrooke où il a complété un mémoire sur un système expert en analyse du risque en estimation. Il a quelques articles à son actif et il est auteur du livre intitulé *L'analyse du risque : une approche conceptuelle et systématique*, publié chez McGraw-Hill en 1996. Il publiera bientôt un guide de gestion du risque en informatique. Enfin, il est intervenu dans le cadre de projets An 2000 chez Avenor, Bombardier et la Banque Laurentienne.

## Résumé

Le bogue de l'an 2000 découle de l'utilisation d'un format de date abrégé pour représenter l'année dans les diverses composantes informatiques. Les conséquences directes du bogue sont d'une part de pouvoir perturber pendant une durée indéterminée le fonctionnement des organisations et, d'autre part, de potentiellement corrompre l'information ou de la rendre inaccessible aux utilisateurs.

L'évaluation objective des différents risques découlant de ce problème technique est un enjeu de taille car la situation comporte toujours beaucoup d'incertitude. En même temps, cet exercice s'avère particulièrement ardu étant donné les multiples contraintes et particularités du problème. Un pronostic sur les risques de l'an 2000 doit donc inévitablement reposer sur un minimum d'hypothèses et une évaluation subjective des pertes et de leurs probabilités.

## TABLE DES MATIÈRES

<b>INTRODUCTION</b>	4
<b>LA PROBLÉMATIQUE</b>	5
DÉFINITIONS	6
LES ENJEUX ÉCONOMIQUES : DES PRÉVISIONS ASTRONOMIQUES	7
LES ENJEUX LÉGAUX : QUI SERA LE BOUC ÉMISSAIRE ?	8
<b>EXAMEN DE LA SITUATION</b>	9
LE CARACTÈRE UNIQUE DU PROBLÈME	9
<i>L'universalité</i>	9
<i>L'interdépendance des systèmes</i>	10
<i>La pléthore d'information</i>	10
<i>La prévisibilité</i>	10
<i>Le problème du futur</i>	11
<i>Les anomalies drôlement bien cachées</i>	11
<i>La fragilité du système</i>	12
<i>Le phénomène amplifié</i>	12
LES FACTEURS PSYCHOLOGIQUES : BIAIS ET ATTITUDE	12
L'AMBIGUÏTÉ DU DISCOURS	14
PRÊT, PAS PRÊT ?	15
LES CAUSES DU RETARD	16
<i>La rareté et la volatilité des ressources</i>	16
<i>Trop peu, trop tard</i>	17
<i>Un stade de maturité plutôt primitif</i>	17
<i>Un piètre historique de performance et de qualité</i>	17
<i>L'héritage d'un certain libéralisme</i>	18
<i>La concentration du problème</i>	18
<i>La contrainte de compatibilité des bases de données</i>	18
LA SITUATION AU QUÉBEC ET AU CANADA	18
<b>SYNTHÈSE DES RISQUES</b>	20
TYPOLOGIE DES RISQUES	20
<i>Le risque technique</i>	21
<i>Le risque informationnel</i>	22
<i>Le risque opérationnel</i>	22
<i>Le risque économique</i>	23
<i>Le risque humain</i>	23
LES RISQUES PAR SECTEURS D'ACTIVITÉS	24
<i>Les secteurs des services publics et de la santé</i>	24
<i>Le secteur financier</i>	25
<i>Le secteur manufacturier</i>	26
<i>Les secteurs aéronautique, naval et militaire</i>	27
<i>La gestion d'entreprise</i>	27
LES MESURES DE RÉDUCTION DU RISQUE	28
<i>Le remplacement</i>	28
<i>La méthode de fenêtrage</i>	28
<i>La méthode d'expansion</i>	29
<i>L'implication de la haute direction</i>	29
<i>La vérification interne et externe de la conformité</i>	29
<i>L'incontournable mise à l'essai</i>	30
<i>Les plans d'urgence ou de contingence</i>	30
LES LIMITES DES SOLUTIONS	31
LES RISQUES MÉCONNUS ET SOUS-ESTIMÉS	32
<b>QUELQUES HYPOTHÈSES SUR LES RISQUES À VENIR</b>	32
<b>CONCLUSION</b>	35

# INTRODUCTION

Le bogue de l'an 2000 est un problème de conception informatique qui a rarement causé autant de questionnement sur les conséquences éventuelles pour l'ensemble des secteurs de l'économie à l'échelle mondiale. Qui aurait cru que deux zéros puissent changer la trame de l'activité informatique et engendrer une crise d'incertitude qui, vraisemblablement, ne sera résolue qu'après coup ? On a vu récemment la crise financière asiatique avoir des répercussions sur tous les marchés. Or, on pourrait faire un parallèle entre l'interdépendance des économies et celle de l'industrie informatique. Les activités d'échanges de biens et de services entre clients, fournisseurs et consommateurs sont à l'origine de nombreux traitements de l'information, du simple bon de commande jusqu'au transfert électronique de données en temps réel.

Plusieurs organisations à forte concentration d'activités informatiques sont dans une situation d'impasse, dans une période de frénésie où le compte à rebours s'effrite de jour en jour et accentue la pression sur tous les intervenants. Par contre, d'autres entreprises subissent moins de tension ; on pense à celles qui ont pris cette menace au sérieux et qui ont démarré les projets à temps, à celles comportant peu de traitements informatisés et à celles qui ont alloué les budgets nécessaires.

Mais même si certaines entreprises croient se soustraire aux conséquences directes de l'an 2000, elles peuvent être exposées à des risques d'affaires tout aussi pernicieux. D'une simple mauvaise interprétation d'une date jusqu'à la disparition de partenaires commerciaux, les organisations seront directement ou indirectement victimes d'éventuelles défaillances informatiques. D'autres secteurs où l'informatique joue un rôle d'arrière plan sont à risque, notamment ceux de la santé, de l'énergie, des télécommunications ainsi que le secteur manufacturier.

Pour être en mesure de mieux apprécier les mille et une facettes des risques reliés à l'an 2000, nous présentons d'abord la problématique et nous expliquons les particularités du problème, suivi d'une synthèse et d'une approche objective d'évaluation du risque.

# LA PROBLÉMATIQUE

Le problème de l'an 2000 résulte du fait que certaines composantes informatiques utilisaient jusqu'à tout récemment deux caractères au lieu de quatre pour représenter l'année dans une information de date. Par exemple, le 1<sup>er</sup> janvier 2000 serait représenté par 00/01/01 au lieu de 2000/01/01. Dans plusieurs cas, des mécanismes dotés d'une horloge électronique, comme les ordinateurs, interpréteront cette date comme 1900 au lieu de 2000. Certains mécanismes ne seront pas fonctionnels parce qu'ils interpréteront 00/01/01 comme étant « Aucune date n'est disponible ». S'ajoute au passage à l'an 2000 l'année bissextile que certains logiciels et systèmes d'exploitation ont omis de considérer. Un autre cas particulier est celui du 9/9/99 et le 99<sup>e</sup> jour de 1999 où certains logiciels pourraient comporter des limites artificielles de programmation, c'est-à-dire qu'une série consécutive de « 9 » peut parfois être utilisée pour représenter la fin logique d'un algorithme quelconque. Par conséquent, bon nombre de composantes informatiques pourraient provoquer des erreurs de calcul, de tri, d'affichage et parfois même des arrêts complets.

L'origine du problème remonte au début de l'ère informatique alors que le format abrégé des dates permettait de réaliser d'importantes économies sur les coûts d'utilisation de l'espace mémoire vive et de la mémoire sur support magnétique. Ce souci d'économie était empreint d'ignorance, ou du moins d'insouciance, quant aux conséquences futures. On présumait que les programmes et langages primitifs seraient remplacés bien avant le nouveau millénaire.

Tel ne fut pas le cas. Nombre d'organisations continuent à utiliser des systèmes informatiques mis au point il y a plus de 30 ans. De plus, malgré une baisse substantielle des coûts d'utilisation de la mémoire, les mauvaises habitudes se sont perpétuées sans se préoccuper outre mesure des répercussions. Ce n'est que vers la fin des années 80 que l'industrie informatique a sonné l'alarme et, malgré cela, plus d'une organisation a tardé à réagir pour maintes et maintes raisons. D'ailleurs, certains fabricants proposaient jusqu'à tout récemment du matériel non conforme à l'an 2000 tel que la génération des microprocesseurs 286, 386 et 486. Même Windows 95 et Internet Explorer 4.0, pour ne nommer que ceux-là, comportent des problèmes liés à l'an 2000<sup>1</sup>.

---

<sup>1</sup> Webster, B.F, « Year 2000: Frequently Asked questions », Washington D.C. Year 2000 Group, August 1998.

## Définitions

*Conformité* est un terme utilisé pour caractériser la compatibilité d'une composante à l'an 2000. Selon l'Association canadienne de normalisation, la conformité à l'an 2000 stipule que ni la performance ni la fonctionnalité ne sont affectées par le changement de date avant, pendant et après l'an 2000. La conformité implique également que pour toutes les interfaces et l'entreposage de données, le siècle dans toutes les dates soit spécifié explicitement ou implicitement à l'aide d'un algorithme non ambigu ou par des règles d'inférence.

Le concept de *risque* est universellement reconnu comme une perte multipliée par la probabilité de cette perte. Globalement, le risque de l'an 2000 pourrait être défini par les pertes résultant des non-conformités multipliées par les probabilités d'occurrence de l'ensemble des situations de non-conformité. On pourrait également ajouter les pertes indirectement reliées à la non-conformité, comme celles encourues avant l'an 2000 à cause de problèmes organisationnels, ou les pertes stratégiques causées par le retard technologique.

Malheureusement, l'évaluation du risque pose deux problèmes fondamentaux. Premièrement, il est difficile d'évaluer les probabilités de non-conformité étant donné l'absence d'historique. Deuxièmement, les pertes potentielles sont autant des pertes tangibles qu'intangibles. C'est pourquoi on devrait plutôt parler de l'incertitude de l'an 2000. Néanmoins, nous garderons le terme *risque* pour les fins de l'article.

On entend par *composante informatique* tout mécanisme servant à traiter, à emmagasiner ou à transférer de l'information par voie électronique. Bref, toute forme d'instrument dans lequel on retrouve une horloge électronique. Voici une liste non exhaustive des composantes pouvant être affectées par le bogue de l'an 2000.

Catégorie	Exemples
Logiciel	Langages de développement et bases de données
	Systèmes d'exploitation
	Progiciels commerciaux
	Programmes utilitaires
	Applications développées maison
Matériel	Ordinateurs centraux, mini, micro
	Microprocesseurs
Équipement spécialisé	Machines industrielles et robots
	Réseaux de télécommunication, systèmes téléphoniques

	Équipements médicaux tels que « scanners », hémodialyses, régulateurs cardiaques.
	Appareils de navigation navals et aériens
	Ascenseurs et élévateurs
	Systèmes de sécurité, alarmes, coffres-forts à minuterie
	Systèmes de ventilation, de climatisation et de chauffage
	Magnétoscopes
	Équipements de contrôle de procédés
	Véhicules munis de systèmes électroniques ou microprocesseurs
	Équipements de code à barre
	Caisses enregistreuses et télécopieurs
	Senseurs, valves et autres appareils de contrôle
	Équipements pour impression et emballage

### ***Les enjeux économiques : des estimations astronomiques***

Pour faire face au problème, plusieurs experts prévoient des investissements par les compagnies de l'ordre de 300 à 600 milliards de dollars à l'échelle mondiale. Capers Jones est l'un de ceux qui proposent les coûts les plus élevés ; 1 335 milliards de dollars à l'échelle mondiale pour les coûts de réparation et de remplacement. Les coûts après l'an 2000, ceux des dommages *ex post*, des poursuites judiciaires et des dépenses de recouvrement, s'élèveraient à 2 286 milliards \$. Les analystes s'entendent généralement sur les coûts de vérification et de correction par ligne de code, soit entre 1,1 \$ et 1,5 \$. La différence se situe dans l'estimation du nombre de lignes de code. Peu importe la validité de ces chiffres, nous pouvons constater l'ampleur du phénomène qui dépasse celle de désastres naturels tels que les tremblements de terre ou les ouragans comme Andrew dont les dommages furent de l'ordre de 12 milliards.

Chez nos voisins américains, un rapport de l'*Office of Management and Budget* du gouvernement des États-Unis évalue le budget de préparation à l'an 2000 sur la période de 1996 à 2000, pour 27 de ses divisions, en excluant celui de la défense, à 2 292 millions \$. Le système d'assurance-emploi nécessite à lui seul un budget de 200 millions \$, celui de la NASA 45 millions \$. Selon les prévisions du regroupement des banques canadiennes, l'industrie des services financiers allouera au projet environ 600 millions \$. Le budget moyen des institutions financières est de l'ordre de 100 millions \$.

À l'exception des entreprises de biens et de services informatiques, l'an 2000 représente une perte nette, voire un gouffre financier, pour bon nombre d'organisations et par ricochet pour



l'économie et la collectivité. Non seulement les budgets de capital et d'exploitation en informatique sont-ils exceptionnels depuis quelques années, mais le spectre des conséquences incertaines plane toujours à l'horizon.

### ***Les enjeux légaux : qui sera le bouc émissaire ?***

Puisque l'an 2000 est un événement prévisible et qu'il ne peut être classé à titre de force majeure ou d'acte de Dieu, les conséquences ne sont généralement pas assurables. Dans le contexte actuel, les assureurs cherchent de plus en plus, lors des renouvellements, à exclure les dommages causés par la transition à l'an 2000. La grande majorité des renouvellements d'assurance qui se font à l'heure actuelle prévoient une exclusion spécifique des risques liés à l'an 2000 et ce, dans tous les domaines de l'assurance. Pour ceux qui souhaiteraient obtenir une certaine forme de protection face à l'an 2000, certains assureurs offrent déjà des polices spéciales à cet effet. Les primes varient de 2 % et 8 % du montant de la couverture.

Ce sont les firmes et leurs administrateurs qui, en principe, assument la responsabilité des dommages. Les litiges en responsabilité pour les problèmes liés au bogue de l'an 2000 vont porter sur la qualité de l'information que détenaient les administrateurs au moment de la prise de décision. Ont-ils obtenu toute l'information pertinente ? Ont-ils étudié tous les choix possibles ? Ont-ils suivi l'évolution de la situation et pris les mesures nécessaires ? À qui ont-ils demandé conseil ? Un administrateur pourrait être tenu personnellement responsable si, par exemple, il participe activement à une affirmation de la compagnie à l'effet que ses opérations seront conformes à l'an 2000, tout en sachant cette affirmation fautive ou en ne faisant aucune vérification à ce sujet, et qu'un client de la compagnie subit des dommages après s'être fié à cette affirmation<sup>2</sup>. Les déclarations de conformité sur Internet pourraient donc être retenues comme éléments de preuve. On sait que la responsabilité professionnelle pour le bogue de l'an 2000 peut être invoquée par les intervenants suivants : 1) les clients pour les pertes subies parce que la firme ne peut remplir ses obligations ; 2) les firmes qui ont acheté des logiciels ou des services de développement de logiciels ; 3) les entités externes pour les pertes financières causées par la perte ou la corruption des données.

---

<sup>2</sup> Pouliot Mercure, « La responsabilité personnelle des administrateurs et des dirigeants dans le cadre du bogue de l'an 2000 », Sheraton Montréal, 10/11/1998.

La responsabilité des gestionnaires à l'égard du problème de l'an 2000 se réfère souvent à la notion de diligence raisonnable. Dans le Black's Law Dictionary, la diligence raisonnable est définie comme le degré de prudence, d'activité, et d'attention auquel on peut à bon droit s'attendre de la part d'une personne raisonnable et prudente et dont fait habituellement preuve cette personne raisonnable et prudente face à une situation donnée ; elle ne fait l'objet d'aucune norme absolue, mais dépend des faits propres à chaque cas.

Une des premières représailles gouvernementales relatives au problème de l'an 2000 a été faite par la *Securities and Exchange Commission* des États-Unis<sup>3</sup>. Elle a imposé des sanctions à 37 firmes de courtage pour avoir omis de produire à temps un statut complet de conformité à l'an 2000. Ces peines symboliques, mais stratégiquement importantes, variaient de 2000 à 3000 dollars. Ce n'est qu'un exemple des problèmes légaux liés au passage à l'an 2000, problèmes qui, selon toute vraisemblance, s'accroîtront.

## **EXAMEN DE LA SITUATION**

### ***Le caractère unique du problème***

Qu'est-ce qui explique le phénomène de l'an 2000 ? Pourquoi y a-t-il autant d'énergie consacrée à résoudre un problème en apparence technique et banal ? En fait, l'an 2000 n'est pas tant un problème technique qu'un problème de gestion et de logistique à multiples contraintes. Voyons quelques-unes de ces caractéristiques qui font de l'an 2000 une première dans l'industrie informatique et qui expliquent en partie les difficultés rencontrées dans les organisations.

#### *L'universalité*

Nul ne peut échapper au problème de l'an 2000. La population pourrait être témoin de certaines irrégularités notamment lorsqu'elle transige avec les entreprises, lorsqu'elle paie ses impôts et lorsqu'elle obtient des services de santé. Du secteur primaire au secteur tertiaire, des services financiers aux services gouvernementaux, toutes les activités utilisant directement ou indirectement les technologies de l'information s'exposent à des problèmes de conformité.

---

<sup>3</sup> Mercury Center, « Regulators crack down on brokerages over Y2K », October 21, 1998.

### *L'interdépendance des systèmes*

S'il ne s'agissait que de résoudre leurs propres problèmes de conformité, un pourcentage raisonnable d'entreprises serait en bonne position pour effectuer un passage sans anicroches. Mais quand ce n'est pas le système d'information utilisé par l'entreprise qui est menacé, ce sont ceux des fournisseurs, des clients et des partenaires commerciaux qui forment tous les maillons de la chaîne de production et de service. C'est pourquoi le risque des uns devient le risque des autres. La valeur ajoutée à chaque étape de transformation et d'échange repose sur un minimum de traitements de l'information. Si l'un d'eux connaît des problèmes de qualité, de productivité, de logistique ou de comptabilité, c'est tout le réseau qui pourra en subir les conséquences.

### *La pléthore d'information*

L'ampleur et l'universalité du problème ont contribué à faire de l'événement un sujet de discussion et d'analyse hors du commun auprès de la communauté informatique. Dans la plupart des médias écrits et électroniques, comme le réseau Internet, on retrouve des groupes de discussions, des services d'aide, des rapports d'analyse et des comités de vigie. Les organismes gouvernementaux et les sociétés affichent par exemple le statut d'avancement de leurs projets, et les fournisseurs de logiciels et d'équipements informatiques affichent leur statut de conformité.

Cette pléthore d'information accroît l'efficacité des communications puisque tous et chacun peuvent, en principe, connaître le statut de leurs partenaires d'affaires. Mais cela n'est pas sans causer des difficultés. Il devient parfois difficile de porter un jugement sur l'état réel de la situation. Les entreprises pourraient notamment tromper leurs partenaires et clients en présentant une image favorable de façon à maintenir leur confiance.

### *La prévisibilité*

Chose particulière, la date butoir pour la plupart des composantes informatiques est connue, soit le 1<sup>er</sup> janvier 2000. Les problèmes peuvent parfois survenir avant et même après cette date. On pense notamment aux applications qui effectuent des traitements impliquant des dates futures ou passées. Par exemple, les systèmes de gestion d'obligations à échéance de 30 ans avaient dû être corrigés pour l'année 1970, les hypothèques de 20 ans ont dû être corrigées pour l'année 1980 et ainsi de suite. D'autres

systèmes auront, après l'an 2000, de la difficulté à faire des comparaisons avec les années antérieures.

### *Le problème du futur*

Jusqu'à tout récemment, le traitement des dates n'était pas une source majeure de préoccupations. Les algorithmes, les fonctions et les formats de date permettaient d'effectuer des opérations avec beaucoup de latitude. Les applications étaient mises au point sans nécessairement se préoccuper de la date d'utilisation ; la date du jour était généralement utilisée pour mettre à l'essai les diverses composantes.

L'an 2000 pose un nouveau problème, celui de corriger un problème qui n'est pas encore survenu. En effet, hormis les environnements micro-informatiques, il est dangereux de simuler l'an 2000 sur un même ordinateur central en même temps que la date courante. Pour remédier à ce problème, les grandes entreprises doivent s'approprier des ordinateurs centraux à des coûts énormes : environ 20 000 \$ par jour. De plus, les essais sur l'an 2000 impliquent l'utilisation d'outils spécialisés et la génération d'un historique représentatif des données. Tout ceci s'ajoute à la complexité du problème et cela exige beaucoup d'imagination de la part des professionnels de l'informatique car il s'agit d'une première expérience pour la majorité d'entre eux.

### *Des anomalies drôlement bien cachées*

Les applications informatiques peuvent toujours être corrigées lorsqu'elles comportent des anomalies ou lorsqu'elles ne répondent pas à des critères de qualité définis. Les organisations se sont d'ailleurs dotées d'outils, d'environnement d'essais et de méthodes relativement bien adaptés à ce contexte. L'an 2000 a ceci de particulier : il existe un très grand nombre de dates dans les fichiers et elles sont utilisées dans une multitude de programmes. Elles n'ont pas nécessairement d'endroit ni d'identification précise, et parfois on retrouve des variables dérivées des dates. Puisqu'une organisation type comporte des centaines, voire des milliers, de composantes informatiques, la difficulté se situe au niveau de la recherche et de l'analyse d'impact. Il existe des outils sophistiqués pour identifier et corriger les problèmes de dates, mais leur efficacité varie entre 70 % à 80 %. Tout n'est donc pas parfait.

### *La fragilité des systèmes*

Telle une chaîne, les systèmes d'information sont aussi fiables que la plus faible de leur composante. Il suffit de peu pour qu'une erreur, si minime soit-elle, soit à l'origine de pertes substantielles et parfois même vitales. Par exemple, Bennett<sup>4</sup> rapporte que la bourse belge ferma ses portes pendant deux jours en 1997 lorsque son nouveau système commença à traiter les transactions boursières de 1997 en date de 1996. Le même auteur rapporte qu'en 1996, un petit programme informatique a tenté de stocker un nombre de 64 bits dans une composante limitée à 16 bits. Il en résulta une perte de 7 milliards de francs à l'Agence Spatiale Européenne lorsque la fusée Ariane 5 explosa moins d'une minute après le décollage. Ces deux exemples parmi tant d'autres démontrent la fragilité des systèmes informatiques et leur impact économique et humain.

### *Le phénomène amplifié*

La médiatisation du phénomène de l'an 2000 jumelée à une image de catastrophe contribue à amplifier le problème et ses conséquences. On pourrait également ajouter que le phénomène n'est pas à l'abri du sensationnalisme. En effet, il est relativement facile d'étaler les conséquences potentielles reliées à une défaillance informatique. L'an 2000 suit le même pattern que le phénomène de Malbrout : plus on s'attarde à identifier et à analyser les risques, plus on en découvre et plus ils sont mis en évidence. Conséquemment, les risques sont mis en relief parfois exagérément ; on prend même conscience des risques qui existent déjà dans d'autres contextes informatiques.

### ***Les facteurs psychologiques : biais et attitude***

On constate deux attitudes vis-à-vis du problème de l'an 2000 : les optimistes et les pessimistes. Cela explique sans doute que nombre d'entreprises n'ont pratiquement rien fait alors que d'autres ont consacré des budgets très importants pour éviter toutes les défaillances possibles. Une des raisons du laxisme tient au fait que les individus ont tendance à ignorer les événements ayant une très faible probabilité ou qui sont éloignés dans le temps, peu importe la gravité des conséquences<sup>5</sup>. Heureusement, la sensibilisation porte fruit. Les spécialistes du risque ont

---

<sup>4</sup> Bennet, R.F., « Oversight Hearing on Financial Institutions and the Year 2000 problem », 10 juillet 1997.

<sup>5</sup> Kunreuther, H., « Limited Knowledge and Insurance Protection », *Public Policy*, 1976, vol. 24, p. 227-261.

observé que le public est très sensible aux risques lorsque les gouvernements, les sociétés privées et d'autres institutions l'en informent<sup>6</sup>.

L'engagement à résoudre le problème de l'an 2000 varie d'une organisation à l'autre, d'une culture à l'autre et d'un individu à l'autre. Certains sous-estiment les risques associés à l'an 2000 et ne prennent pas les mesures nécessaires, soit par ignorance, soit pour éviter d'engager des dépenses. Ce dernier type d'individu reconnaît peu de bénéfices associés à la vérification de la conformité, est prêt à subir d'éventuelles pertes ou est sujet à des contraintes budgétaires, c'est pourquoi il investira le minimum. Cette attitude pourrait également s'expliquer du fait qu'il y a un biais systématique dans l'évaluation des facteurs d'influence, les individus percevant plus facilement le risque des choses qui leur sont mieux connues<sup>7</sup>.

Une autre attitude est celle de l'aversion pour le risque. Cette attitude se traduit par la prise de mesures de réduction du risque dont les coûts surpassent l'espérance mathématique des pertes. On constate souvent ce phénomène dans les décisions d'assurances. Cela se traduit donc notamment par un redoublement d'effort pour éviter que les systèmes informatiques ne perturbent les opérations et surtout pour ne pas ternir l'image corporative. Ces comportements proviennent également du fait que les individus ne veulent pas être associés à une erreur par omission. Des mesures exceptionnelles sont parfois prises pour rassurer les gestionnaires en vérifiant plusieurs fois et dans des conditions très rigoureuses la conformité à l'an 2000. Par exemple, la responsabilité des administrateurs influence le niveau de certitude exigé sur le statut de conformité ; certains préfèrent effectuer un nombre exagéré de tests plutôt que d'être responsables des défaillances informatiques. S'il y a défaillance, ils pourront toujours se défendre en alléguant avoir consacré tous les efforts possibles.

Le consommateur pourrait craindre le changement de siècle (même si techniquement le 21<sup>e</sup> siècle n'arrive que le 1<sup>er</sup> janvier 2001). Cela pourrait se traduire par des retraits massifs des comptes financiers ou par une vente de titres boursiers. D'ailleurs, selon un article du *USA Today*<sup>8</sup>, la Banque Fédérale Américaine veut être prête au cas où les consommateurs se précipiteraient pour effectuer des retraits. Pour soutenir les 460 milliards de dollars en circulation, elle ajoutera 50 milliards au 150 milliards déjà en réserve pour l'an 1999. Selon

---

<sup>6</sup> Morgan, G., « L'évaluation et la gestion des risques », *Pour la science*, no 191, septembre 1993, p. 28.

<sup>7</sup> Dubois, J.-C., *L'analyse du risque : une approche conceptuelle et systémique*, Chenelière/McGraw-Hill, 1996, p. 43.

<sup>8</sup> Mayer, M., « A stash of cash for Y2K », *USA Today Tech Report*, 20 août 98.

l'auteur, personne ne sait combien suffirait à l'échelle nationale parce qu'on ne sait pas si le passage à l'an 2000 sera un problème mineur ou une grave crise. Il ajoute ceci : « Je connais beaucoup d'individus travaillant sur l'an 2000 qui passeront cette période avec beaucoup d'argent comptant sous le matelas. »

### ***L'ambiguïté du discours***

Quiconque cherche à évaluer l'ampleur des conséquences globales fera face à des prédictions ambiguës. Voyons quelques arguments invoqués des deux côtés.

Le premier discours est celui de l'alarmiste qui cherche à alerter la communauté face aux dangers potentiels en dénonçant le manque d'engagement des organisations ou en étalant le spectre des conséquences. L'économiste en chef de la société Deutsche Morgan Grenfell, Edward Yardeni<sup>9</sup>, affirme qu'il y a six chances sur dix de voir l'économie mondiale essayer en 2000 une récession majeure comparable au premier choc pétrolier. Il croit que la récession de l'an 2000 sera déflationniste et qu'une chute de 1000 milliards de dollars du PIB américain et de la capitalisation boursière de Wall Street est possible. Ceux qui anticipent une baisse du marché boursier suggèrent de transférer le capital dans d'autres types d'investissement. Il existe d'ailleurs des fonds de placements comprenant uniquement des sociétés certifiées « Conformes à l'an 2000 ».

Le deuxième discours est celui de ceux qui croient au succès de l'opération, ceux qui banalisent le problème et pour lesquels il existe des solutions. Selon Gartner Group, les progrès qu'accomplissent les institutions bancaires américaines leur ont permis de réduire les risques de défaillance des systèmes critiques à environ 50 % en 1997, comparativement à 90 % pour l'an 1996. Plusieurs organisations affirment être prêtes pour l'an 2000, incluant les institutions financières et la plupart des organisations visitées sur Internet. Selon un rapport préparé par le Groupe de travail de l'an 2000, plus de 90 % des entreprises canadiennes sont conscientes du problème, ce qui constitue au moins une assurance que des moyens seront pris pour résoudre le problème.

---

<sup>9</sup> AFP, Washington.

### *Le discours, encore l'affaire des initiés*

Contrairement aux médias électroniques, les chaînes de télévision et les journaux populaires ont été relativement muets jusqu'à la fin de 1998. Il y avait certes des éléments de curiosité chez la population, mais dans l'ensemble elle ne semblait pas trop se préoccuper des enjeux. C'est pourquoi les non-initiés n'avaient qu'une vague idée de la nature et de la portée du problème. Néanmoins, comme on peut le constater depuis le début de l'an 1999, il y a une augmentation constante du nombre d'émissions de télévision et de radio, de même que de publications destinées au grand public. Si ces premières communications n'ont pas encore généré d'effet de panique notable, nous devons reconnaître qu'il y a encore quelques mois devant nous et que ce scénario est toujours plausible. Par exemple, il ne semble pas y avoir eu de correction à la baisse du marché boursier due à la crainte du bogue de l'an 2000. Peut-être est-il trop tôt pour conclure, mais le contraire, soit une forte hausse avant l'an 2000, est plutôt difficile à envisager. Le marché boursier est reconnu comme étant sensible aux rumeurs et anticipe plutôt subjectivement les tendances économiques.

### ***Prêt, pas prêt ?***

Selon une étude récente<sup>10</sup>, éviter les catastrophes qui risquent de survenir au tournant du millénaire constitue la priorité de six des sept sociétés américaines du classement Fortune 500. Des études menées par le Groupe de travail de l'an 2000 démontrent une nette amélioration au Canada par rapport à l'année dernière quant à la prise de conscience du problème et des moyens utilisés pour le résoudre. Cependant, ces mêmes études reconnaissent que la situation est toujours inacceptable.

Une prévision du Gartner Group<sup>11</sup> en 1997 stipule qu'à la fin de 1999, moins de 70 % des systèmes informatiques critiques et orientés vers les clients seront conformes à l'an 2000. Le *Software Productivity Research*<sup>12</sup> corrobore également cette prédiction et croit que plusieurs applications informatiques aux prises avec des problèmes de date ne seront pas réparées d'ici l'an 2000. Aussi, ce n'est qu'en mars 1999 que 90 % des systèmes critiques de la NASA<sup>13</sup> seront conformes, la proportion étant de 40 % à la fin de 1998.

---

<sup>10</sup> Cap Gemini, Year 2000 Update in DCI IT News, August 19, 1998.

<sup>11</sup> GartnerGroup, Year 2000: Does Package Replacement Spell Relief ?, February 19, 1997.

<sup>12</sup> Contingency Planning for Te Year 2000 Software Problem, Capers Jones.

<sup>13</sup> Status of NASA's Year 2000 Progress, April 1998.



L'Europe est concentrée sur la conversion à l'Euro et a peu de temps à consacrer à l'an 2000. La Russie fait de la sensibilisation mais manque de ressources financières. L'Asie, et plus particulièrement le Japon qui est touché par la récession, sont davantage préoccupés par le maintien des emplois que par la résolution des problèmes de l'an 2000. L'Afrique, l'Amérique du Sud et les autres pays en voie de développement sont loin derrière. D'après l'évaluation faite par l'Agence canadienne de développement international (ACDI), 2 de ses 391 projets bilatéraux ont été classés à haut risque (risque de perte de vie) et 39 à risque moyen.

Selon le rapport du Groupe de travail de l'an 2000<sup>14</sup>, 70 % des entreprises canadiennes prennent des mesures comparativement à 45 % en octobre 1997. Dans l'ensemble, le pourcentage des entreprises qui prennent des mesures officielles a doublé passant de 9 à 18 %. Fait particulier, la moitié des grandes entreprises ne prévoient pas être prêtes avant le cours de l'année 1999 ou ne savent pas quand elles le seront.

Somme toute, on constate qu'un bon nombre d'organisations ne seront pas prêtes à temps. En même temps, on souligne un progrès constant. La question fondamentale est maintenant d'évaluer l'importance relative des problèmes de non-conformité. Il faut également voir la progression d'ici la date fatidique car il est toujours possible d'agir avant l'an 2000.

### ***Les causes du retard***

On peut se demander pourquoi les organisations ne sont toujours pas prêtes, pourquoi elles consacrent tant d'efforts et pourquoi nous en sommes rendus à résoudre les problèmes à la dernière minute. Plusieurs facteurs expliquent pourquoi il y a toujours de l'incertitude.

#### *La rareté et la volatilité des ressources*

L'accroissement de la demande de professionnels en informatique n'est pas compensé par l'offre. Résultat : les salaires sont en forte hausse, les coûts des projets surpassent les prévisions, les experts ne sont pas disponibles. Un phénomène très dommageable est celui du départ de ressources clés. Les organisations sont alors parfois prises au dépourvu, ne connaissant pas toutes les particularités des systèmes.

---

<sup>14</sup> « Groupe de travail de l'an 2000 : au-delà des progrès, des craintes sérieuses », *Les affaires*, octobre 1998, p. 30.

### *Trop peu, trop tard*

Malgré les avertissements répétés de la communauté informatique, les dirigeants d'entreprise ont longtemps sous-estimé l'ampleur que prendrait le problème. Leurs préoccupations, davantage axées sur le déploiement de solutions d'affaires, ne tenaient pas compte de l'effet de report et d'accumulation. Les premières demandes budgétaires pour l'an 2000 ont longtemps manqué de crédibilité parce qu'il était difficile de justifier des investissements d'une telle envergure. Nombre de projets n'ont donc été mis en place que lorsque les entreprises ont été acculées au pied du mur. À la surprise générale, ces budgets sont encore plus importants maintenant, étant donné la rareté des ressources.

### *Un stade de maturité plutôt primitif*

On constate un manque de leadership et un manque d'organisation au sein des divisions d'informatiques. Près de 70 % des organisations sont au niveau 1 selon l'échelle croissante (de 1 à 5) de maturité du processus logiciel (CMM) établie par le Software Engineering Institute. Les organisations n'étaient tout simplement pas prêtes à relever un défi de cette envergure et de ce niveau de complexité.

D'abord les inventaires de composantes n'étaient pratiquement pas à jour. Dès que complétés, on ne savait toujours pas qui était responsable de chacune des composantes et il fallait déterminer si elles étaient conformes ou non, sans savoir ce que conforme signifiait. De plus, plusieurs ont eu de la difficulté à distinguer les différents types de composantes et à déterminer les stratégies qui devaient être employées pour les rendre conformes. Toutes ces questions ont causé de longs débats sur les priorités, les bénéfices, les impacts et les contraintes associés à chacune d'elles.

### *Un piètre historique de performance et de qualité*

Les projets informatiques font mauvaise figure en termes de productivité, de développement et de qualité du logiciel. Une étude réalisée par KPMG constatait que trois projets informatiques sur quatre dépassaient leur échéancier de 30 % ou plus. Or, l'empressement de dernière minute laisse planer de sérieux doutes quant au respect des échéances des projets de l'an 2000. Les géants, tels IBM et Microsoft, allouent d'énormes budgets à la réalisation des essais. Malgré tout, les logiciels comportent des anomalies. Par exemple, la dernière version SP4 de Windows NT remplaçant la version 4.0 comporte 600 corrections

d'anomalies. La version 4.5 de Netscape comporte au-delà de 4000 améliorations (et corrections d'anomalies) par rapport aux versions précédentes.

#### *L'héritage d'un certain libéralisme*

Bien qu'il existe des normes internationales sur les dates et sur d'autres usages en informatique, bien peu d'entreprises les respectent. On dénote également l'absence de réglementation sur la pratique informatique, en ingénierie notamment. Résultat : l'industrie informatique est victime de son propre libéralisme et de son laxisme dans l'implantation de mécanismes rigoureux et reconnus. La non-conformité à l'an 2000 est sans doute l'héritage de cette absence de normes.

#### *La concentration du problème*

L'an 2000 mobilisera de plus en plus d'efforts et d'investissements dans une même période de temps. Conséquemment, les services de soutien bureautique seront littéralement débordés d'appels au moment crucial, les fournisseurs devront pallier à une forte demande d'information sur la conformité ou pour la réparation des problèmes. Un autre effet pervers résulte des nombreux changements qui, apportés simultanément, déstabilisent les organisations en sollicitant les ressources de tout bord, que ce soit pour confirmer l'utilisation des composantes, déterminer les propriétaires, choisir les solutions, les mettre en œuvre ou vérifier leur conformité.

#### *La contrainte de compatibilité des bases de données*

Lors de migration et de conversion d'application ou de bases de données, il est souvent nécessaire d'assurer la compatibilité dite ascendante. Ainsi, le format de date à 2 positions pour l'année a longtemps dû être pris en compte pour faciliter le processus. Parce que les changements de format coûtent beaucoup plus cher et que peu d'organisations bénéficiaient de ce type particulier d'expertise, plusieurs projets de conversion à 4 positions pour l'année ont été reportés maintes et maintes fois.

### ***La situation au Québec et au Canada***

Selon certains experts, les pays en meilleure position seraient ceux du Commonwealth, les Pays-Bas, la Suède et l'Australie. Les institutions financières canadiennes sont en bonne position comparativement à celles des États-Unis. On compte 17 banques à chartes

canadiennes comparativement à plus de 800 aux États-Unis. Le nombre plus restreint de banques et d'échanges inter-institutionnels expliquerait le risque moins élevé au Canada.

Plusieurs intervenants se sont coordonnés pour sensibiliser les organisations devant la menace du bogue de l'an 2000. Une des 18 recommandations du Groupe de travail de l'an 2000 se lisait d'ailleurs comme suit : « Effectif le premier avril 1998, toutes les banques canadiennes et autres institutions prêteuses devraient arrêter de prêter des fonds à toutes les entreprises, petites, moyennes ou grandes, qui ne présentent pas un plan formel pour résoudre le problème de l'an 2000<sup>15</sup>. » Les gouvernements ont pris les initiatives nécessaires pour communiquer leur statut d'avancement. Le gouvernement fédéral met à la disposition des entreprises des mesures fiscales pour réduire les coûts de l'an 2000, notamment en permettant une dépense accélérée d'amortissement.

Les autorités assurant la sécurité ne prennent toutefois pas de chance. Tout récemment<sup>16</sup>, les Forces armées canadiennes ont reçu l'ordre de consacrer les prochains 14 mois à préparer ce qui pourrait être le plus vaste déploiement en temps de paix – des dizaines de milliers de troupes réparties à travers le pays et des frégates amarrées aux principaux ports – au cas où le problème de l'an 2000 serait à l'origine de troubles civils. Les 16 000 policiers de la GRC ne pourront pas prendre de vacances entre le 27 décembre 1999 et le 15 mars 2000, au moins jusqu'à ce que le problème de l'an 2000 soit circonscrit. Il en est de même pour les 5 000 policiers de Toronto et de Calgary. La division de prévention des incendies de Montréal comportera également des restrictions à ce sujet.

On rapportait récemment que lorsque le vérificateur de la Ville de Montréal a publié son dernier rapport annuel, le chapitre portant sur l'an 2000 et les TI au sein de l'organisation municipale avait soulevé de nombreuses inquiétudes<sup>17</sup>. Le vérificateur soulignait les risques majeurs que le passage de l'an 2000 présente pour la sécurité civile, les systèmes financiers et la production des eaux. Il soulevait la possibilité que la situation dégénère en graves crises si certaines choses n'étaient pas corrigées rapidement.

Selon le Directeur du projet « An 2000 » à Hydro-Québec, la grande majorité des composantes numériques ont atteint le statut de conformité à l'an 2000. Les risques opérationnels sont en

---

<sup>15</sup> *The Gazette*, Wednesday, February 4, 1998.

<sup>16</sup> « Army fears civil chaos from millenium bug », *The Globe and Mail*, 27 octobre 1998.

conséquence quasi inexistant. Malgré tout, Hydro-Québec procède à la certification des composantes et prépare un plan d'urgence pour l'année 1999. Un des risques d'affaires à envisager, s'il en est un, se situe au niveau des échanges et de la dépendance envers certains fournisseurs et partenaires de la société. Enfin, le transport et la distribution d'électricité comportent peu de composantes électroniques. De toute façon, des mécanismes de contrôle et d'aiguillage permettent d'identifier et de contourner les problèmes si jamais ils survenaient.

À la Régie des rentes du Québec, on affirme que toutes les composantes informatiques sont prêtes depuis le 31 décembre 1998, sauf pour une partie du registre des cotisants. De plus, le système d'administration de la Loi sur les régimes complémentaires de retraite sera remplacé à l'automne 1999.

## SYNTHÈSE DES RISQUES

### *Typologie des risques*

Plusieurs types de risques sont impliqués par le bogue de l'an 2000. Il y a principalement les risques spécifiques à l'informatique, mais il y a aussi les risques financiers et humains. Il existe également une échelle qualitative de niveau de risque qui peut être utilisée, comme celle ci-dessous<sup>18</sup>.

Niveau	Signification
1	Une défaillance qui peut entraîner des pertes de vie humaine ou des blessures.
2	Une défaillance qui peut entraîner un coût potentiellement fatal pour l'organisation.
3	Une défaillance qui peut entraîner des pertes substantielles mais non fatidiques pour l'organisation.
4	Une défaillance qui peut entraîner des pertes triviales ou un simple inconvénient pour l'organisation.

---

<sup>17</sup> Direction informatique, « Dompter l'an 2000 à la Ville de Montréal », septembre 1998, vol. 11, no 9.

<sup>18</sup> Don Estes, 1997, p. 5.

### Le risque technique

Le risque technique se rapporte au type de défaillance que peuvent présenter les différentes composantes informatiques.

Type de défaillance	Description
Entreposage	Mauvais entreposage ou archivage des données. Des documents pourraient être détruits ou recyclés par erreur parce qu'entre autres, une sauvegarde du 01/01/2000 pourra être considérée comme antérieure à celle du 31/12/1999.
Ordonnement	Mauvais tri par date ; les informations de l'an 2000 (00) apparaissent à l'écran ou sur un rapport avant celles de 1999 (99).
Logique	Certaines applications pourraient s'interrompre abruptement parce que >99 ou 00 n'auront pas été programmés. Par exemple, des traitements pourraient être interrompus brutalement à cause de méthodes de <i>hash-coding</i> qui divisent par l'année pour définir des pointeurs d'accès rapides aux informations. À l'an 2000, il pourrait donc y avoir division par 0.
Calcul	Les calculs impliquant des différences de dates peuvent être erronés. L'âge d'un individu est calculé à partir de la date du jour moins sa date de naissance : 2000 (00) – 1964 (64) donne – 64 ans au lieu de 36 ans.
Jours de semaine	Si le système d'exploitation retourne en 1900, le 2 janvier 1900 était un mardi alors que le 2 janvier 2000 sera un dimanche.
Limite artificielle	Les chiffres 9, 99 ou 999 sont parfois considérés comme une limite dans les programmes informatiques. Le 9/9/99 et le 99 <sup>e</sup> jour de 1999 pourraient causer des problèmes.
Année bissextile	Certains systèmes d'exploitation et des programmes maison n'ont pas prévu que l'an 2000 est une année bissextile. Plusieurs informaticiens n'ont pas tenu compte de la règle que les années bissextiles surviennent tous les 4 ans, sauf tous les 100 ans. Tous les 400 ans, l'année redevient bissextile (comme ce sera le cas en l'an 2000) sauf tous les 3600 ans.

### *Le risque informationnel*

Le risque informationnel se rapporte aux conséquences des défaillances techniques sur la qualité de l'information.

Type de perte	Description
Perte nette d'information	Destruction partielle ou complète de l'information ou incapacité partielle ou totale de son utilisation.
Perte d'intégrité	Corruption des données à la suite de mauvais calculs.
Perte de certitude	Caractère incertain de l'information. Des efforts sont nécessaires pour en vérifier la certitude.
Perte de validité	Invalidité de résultats à la suite de calculs erronés.
Perte de structure	Systèmes comportant plus d'un format de date causant des difficultés d'organisation, de recherche et de stockage.
Perte d'accessibilité	Incapacité d'accéder à des informations selon les anciens formats non conformes à l'an 2000.
Perte de compréhensibilité	Ambiguïté de l'information et difficulté d'interprétation. par exemple, 05/02/01. S'agit-il du 5 février 1901, du 5 février 2001, du 2 mai 1901, du 2 mai 2001, du 1 <sup>er</sup> février 1905, du 2 janvier 1905, du 1 <sup>er</sup> février 2005 ou du 2 janvier 2005 ?

### *Le risque opérationnel*

Le risque opérationnel se rapporte aux conséquences des défaillances, ou même des corrections apportées, sur l'efficacité des opérations.

Type de perte	Description
Perte nette de traitement	La perte nette de traitement d'information résultant de l'incapacité de s'exécuter en totalité ou en partie.
Perte de capacité	La réorganisation de certains logiciels pour être conformes à l'an 2000 peut réduire la capacité de traitement et ralentir les différents processus d'affaires.
Perte de traçabilité	Difficulté à pouvoir retracer des anomalies dues aux changements apportés aux programmes.
Perte de structure	Détérioration de la structure logique des composantes informatiques due à l'empressement de dernière minute.
Perte de maintenabilité	Incapacité des composantes à évoluer selon les besoins à cause d'une mauvaise réorganisation des programmes.
Perte de fiabilité	Erreurs intermittentes dues à la perte de fiabilité des réseaux.
Perte de simplicité	Complexité et effort d'analyse accrus, dus à la correction des composantes.

Perte de normalisation	Perte de standards de qualité due à un manque de rigueur.
Perte d'uniformité	Perte d'uniformité des composantes utilisant plus d'une méthode de conversion.
Perte de compatibilité	Incapacité d'interagir avec d'autres composantes si les formats ne sont pas synchronisés.

### *Le risque économique*

Le risque économique se rapporte aux conséquences économiques et financières résultant directement des défaillances ou des corrections apportées. Ces conséquences découlent de la détérioration de la qualité de l'information et de la perte d'efficacité opérationnelle.

Type de perte	Description
Perte d'actif	L'information étant considérée comme un actif, si des informations sont perdues ou corrompues, les pertes pourraient être évaluées selon le coût de remplacement ou la valeur marchande. Dans certains cas, l'information peut avoir une valeur stratégique importante.
Perte de biens et services	La production et la distribution des biens et services pour l'ensemble des consommateurs et utilisateurs peuvent être ralenties ou interrompues pour une période de temps plus ou moins longue.
Perte de rentabilité	La rentabilité d'une entreprise peut être affectée de diverses façons. Une société dont le système informatique s'avère incapable d'opérer peut perdre approximativement de 3 à 4 % de ses revenus annuels pour chaque jour d'opération perdu. La perte de clients, la perte due à des créances non recouvrées de clients en difficulté, la perte due à des réclamations en vertu de garanties ou autres obligations, etc.

### *Le risque humain*

Comme pour le risque économique, le risque humain découle de la détérioration de la qualité de l'information et de la perte d'efficacité opérationnelle. Les conséquences peuvent être établies selon les défaillances des composantes informatiques sur les individus et la société, que ce soit directement ou indirectement. On peut parler de conséquences sur la santé et la sécurité, l'environnement, et surtout des aspects psychologiques. Voici un aperçu des risques humains potentiels.



Type de perte	Description
Perte de santé et de vie	Si des appareils médicaux sont nécessaires pour la survie ou le maintien de fonctions essentielles ou si des appareils sont défectueux lors d'une intervention, les risques peuvent aller d'un simple malaise jusqu'à la perte de vie. Si le contrôle de qualité de l'industrie alimentaire est défectueux, un empoisonnement pourrait arriver.
Perte liée à l'insécurité	Si des pannes touchent les infrastructures importantes, comme les réseaux d'électricité, d'aqueduc, de circulation et de communication, on peut s'attendre à ce qu'il y ait de l'angoisse.
Perte due à la tension psychologique et au stress	Les personnes responsables de systèmes informatiques et de la mise en place des solutions sont sujettes à un inconfort psychologique. Les conséquences vont de l'absentéisme aux maladies professionnelles.

### ***Les risques par secteurs d'activités***

Les risques varient selon l'importance relative et les probabilités d'occurrence d'une non-conformité. D'un secteur d'activité à un autre, on retrouve également des risques informationnels, opérationnels, économiques ou humains. Quelques-unes des conséquences potentielles ont été répertoriées.

#### *Les secteurs des services publics et de la santé*

Système	Conséquences
Énergie	Les équipements de génération d'électricité pourraient causer des fluctuations de voltage et même changer la fréquence.
Eau	Le contrôle de qualité des eaux et le contrôle de la pression pourraient être perturbés.
Soins de santé	Des appareils respiratoires, des stabilisateurs cardiaques, des appareils de filtration sanguine ou d'injection de médicaments pourraient, s'ils connaissent des défaillances, mettre en péril la santé des bénéficiaires. Par exemple, le 3 mai 1998, le <i>London Times</i> a révélé que dans un hôpital nord-londonien, une opération avait dû être reportée parce que le système informatique avait annoncé une rupture de stock des compresses. En fait, il y en avait en nombre suffisant mais leur date limite d'utilisation était fixée à 2001.

Services d'incendie	Des systèmes défaillants de gestion des effectifs et de logistique pourraient forcer à utiliser des méthodes manuelles et ainsi ralentir l'efficacité des interventions.
Sécurité publique	Certains modèles de feux de circulation ne sont pas conformes à l'an 2000. Des cas exceptionnels sont rapportés par le Gartner Group : la prison d'État de Virginie a découvert que son système de porte était non conforme à l'an 2000.
Transferts sociaux	Problème de calcul, d'allocation des prestations de programmes sociaux (d'assurance-emploi, de fonds de pensions) et de prélèvements (impôts, cotisations diverses)

### *Le secteur financier*

Système	Conséquences
Transferts électroniques de fonds	Format de date non compatible lors de la transmission d'information financière d'une institution à une autre. Tous les services interbancaires n'auront pas le format explicite des dates.
Transactions boursières	Problème de synchronisation et de compatibilité avec les différents courtiers et autres bourses à l'échelle mondiale. Que se passera-t-il par exemple lors du passage à la bourse de Londres fonctionnant 24 heures sur 24 ? Y aura-t-il un gel des transactions pendant un temps indéterminé ? On annonçait récemment que le passage de l'indice Dow Jones au-delà des 9 999 points pourrait causer de graves problèmes informatiques à Wall Street, les ordinateurs correspondants n'ayant pas été programmés pour gérer un indice à 5 chiffres.
Cartes de crédit	Certains suggèrent de vérifier les soldes avant le passage à l'an 2000. Des commerçants pourraient utiliser des appareils non conformes tels que des caisses enregistreuses. Certains logiciels traitant avec VISA ne seront disponibles qu'en avril 1999 comme pour l'application BankCard à la Banque Laurentienne du Canada.
Prêts personnels et hypothécaires	Transactions de correction en défaut lorsqu'elle réfère aux mois et années antérieurs. Des états de compte pourraient trier les transactions dans le mauvais ordre si 1999 et 2000 coexistent.
Rentes viagères et autres	Calcul des rentes, problème de projections des revenus ou allocations des prestations.
Guichet automatique et autres transactions bancaires	Des imprimantes de guichet pourraient imprimer des états de comptes avec des dates non conformes et induire en erreur. Les livrets devront être changés pour élargir la colonne de date. Les chèques imprimés 19-- ne seront plus utilisables.

Le secteur manufacturier

Système	Conséquences
Maintenance d'équipements	Les périodes d'entretien préventif pourraient être mal planifiées.
Contrôle de procédés	Les usines comportant des contrôles de procédés ont généralement des milliers de composantes numériques. Ils fonctionnent en continu et si l'une des composantes présente une anomalie, des pertes considérables pourraient survenir. Par exemple, dans le contexte d'une usine de pâte et papier comme Avenor, les pertes sont d'environ 25, 000 \$ l'heure pour les 4 premières heures et de plus d'un demi-million si la panne va au-delà d'une journée. Il peut y avoir des centaines de systèmes de contrôle intégrés (SCI) dans une installation de produits chimiques ou sur un site manufacturier. On a par exemple calculé qu'il y aurait de 8 000 à 10 000 SCI dans une plate-forme moderne de forage pétrolier en mer.
Contrôle de qualité	Différents paramètres de qualité pourraient être mal mesurés, comme la tension, la vitesse, la résistance, la densité, etc. Le problème peut parfois être observé à la toute fin et entraîner des pertes importantes.
Production à la chaîne	Les usines de montage <i>just-in-time</i> , dans l'industrie de l'automobile par exemple, comportent des milliers de composants qui sont acheminés quotidiennement par des centaines de fournisseurs aux différentes usines d'assemblage. Si l'un d'eux connaît un retard ou si un composant ne répond pas aux normes de qualité, l'efficacité de la production en sera inévitablement amoindrie.
Sécurité et surveillance	Les systèmes de surveillance caméra, à infrarouge ou autre, pourraient mal fonctionner et compromettre la sécurité. Le système de freinage d'un des manèges de Disney World en Floride a été découvert non conforme.
Ventilation	Arrêt de ventilation ; mauvaise détection de l'humidité, des bactéries ou de la pression ; dysfonctionnement des valves.
Valves, senseurs et autres composantes électroniques	Un des pires dangers qui guettent les entreprises est la présence de puces intégrées dans des machines ou des contrôleurs industriels <sup>19</sup> .

<sup>19</sup> « Bogue de l'an 2000: les PME québécoises se préparent », *Les Affaires*, octobre 1998.

Les secteurs aéronautique, naval et militaire

Système	Conséquences
Aviation	Dans le cas des compagnies aériennes, parmi les problèmes possibles, citons la perturbation des horaires des vols et des programmes d'entretien. La compagnie aérienne hollandaise KLM a indiqué qu'elle n'allait pas exploiter certaines routes au début de l'an 2000 s'il y a des doutes quant à la sécurité aérienne. Selon le IATA (International Air Transport Association), il subsistait un doute à l'endroit des fournisseurs de gestion du trafic aérien. La <i>Federal Aviation Administration</i> des États-Unis se dit prête à interrompre les trajets vers des pays où les systèmes informatiques ne seraient pas sûrs.
Navigation	Des systèmes de navigation et autres mécanismes de contrôle sur les bateaux pourraient ne pas être conformes. La Lloyds n'assurerait pas les bateaux qui n'auraient pas démontré leur statut de conformité. Aussi, les récepteurs GPS (Global Positioning System) utilisent un compteur de semaine sur 10 bits qui passera à 0 dans la nuit du 21/08/1999 au 22/08/1999 <sup>20</sup> .
Sous-marins, porte-avions, chars d'assaut et autres engins militaires	Une défaillance d'une composante électronique peut menacer la sécurité des militaires et de la population civile. On peut présumer que les forces armées modernes éviteront d'effectuer des manœuvres durant le passage à l'an 2000. Par contre, les États moins fortunés comme la Russie, la Chine et certains pays d'Europe centrale, peuvent avoir des mécanismes de contre-attaque automatique. Y aura-t-il un missile lancé par inadvertance ?

La gestion d'entreprise

Système	Conséquences
Gestion des achats	Rupture de stock ou surcharge.
Gestion des ventes	Retour de produits non conformes tels que des magnétoscopes.
Contrôle d'inventaire et des biens périssables	Mauvaises dates d'expiration des inventaires. Pertes de denrées périssables dues à des erreurs d'échéance.
Horaire de livraison	Les utilisateurs de systèmes de chauffage au mazout pourraient être en pénurie si les fournisseurs effectuent mal la distribution à cause d'erreurs dans le calcul de la

<sup>20</sup> *Datamation*, juin 1997, p. 31.

	consommation.
Service à la clientèle	Les services à la clientèle pourraient voir un accroissement significatif des appels des consommateurs.
Comptabilité	Possibilité d'erreurs lors des traitements de fin de mois, de trimestre et d'années. Par exemple, la facturation des interurbains faits dans la nuit du 31 décembre pourrait comporter des erreurs, car elle est basée sur l'heure de fin moins celle du début de l'appel. Incapacité de produire une liste des comptes-clients. Incapacité pour les clients de payer leur compte.
Gestion des ressources humaines	Pression induite sur les ressources informatiques pour accroître la productivité. Taux de rotation élevé des ressources. Accroissement de la tension au travail. Conflits de rémunération. Le mouvement Desjardins, par exemple, a instauré une prime de 20 % du salaire pour inciter ses informaticiens à demeurer à leur poste. Cela ne fut pas sans causer des frustrations chez les autres employés.

### ***Les mesures de réduction du risque***

Les principales solutions envisagées pour résoudre le problème de non-conformité des composantes à l'an 2000 sont le remplacement par de nouvelles versions ou par de nouvelles composantes, la mise au rancart, la conversion par méthode de fenêtrage et la conversion par méthode d'expansion. Cependant, il faut reconnaître que chacune d'elle comporte des risques.

#### *Le remplacement*

Un certain nombre d'entreprises ont investi des milliers, voire des millions de dollars pour remplacer les composantes non conformes à l'an 2000. Cela n'est pas sans risques puisqu'il est possible que ce type de projet n'arrive pas à temps en raison de la durée moyenne de son d'implantation (12 à 24 mois). En effet, des organisations peuvent avoir sous-estimé les efforts reliés à la conversion, à la formation et à la mise au point de tels systèmes. De plus, plusieurs greffent des modules maison à des logiciels commerciaux et peuvent entrer des paramètres de dates non conformes.

#### *La méthode de fenêtrage*

Avec la méthode de fenêtrage ce ne sont pas les bases de données qui sont changées, mais plutôt les programmes de telle sorte que le siècle est interprété selon une année pivot. Par exemple, les années supérieures ou égales à 80 sont considérées comme faisant partie

de 1900 (01/01/95 est interprété 01/01/1995) alors que les années inférieures à 80 sont considérées comme faisant partie de 2000 (01/01/75 est interprété 01/01/2075). Cette méthode, qui implique la modification d'un ou plusieurs programmes, comporte des dangers lorsqu'elle coexiste avec d'autres méthodes comme l'expansion ; les essais sont d'autant plus difficiles à préparer et à réaliser. De plus, puisque généralement de 6 % à 10 % des anomalies proviennent de la correction d'anomalies, toute modification aux programmes existants est une source potentielle d'erreur.

#### *La méthode d'expansion*

La correction par méthode d'expansion des champs consiste à allonger le format de date dans les fichiers et les programmes pour avoir l'année explicite à 4 positions. Le problème réside dans la quantité énorme de composantes à convertir, incluant parfois les archives, les liens avec d'autres systèmes, etc. Des étapes de vérifications manuelles doivent tout de même être utilisées pour procéder selon cette méthode. Qui plus est, cette stratégie n'apporte généralement pas de bénéfices à l'organisation, si ce n'est de se prémunir contre les risques du passage de l'an 2000. Le risque est également grand d'être dépassé par la concurrence qui a choisi la solution du remplacement.

#### *L'implication de la haute direction*

Les dirigeants d'entreprises ont progressivement compris les enjeux de l'an 2000 ; leur appui s'est traduit par une allocation importante de budget pour les activités informatiques et les équipements. Des politiques ont également permis d'accorder la priorité à ces projets et de donner plus de pouvoir discrétionnaires aux équipes informatiques. Pour réduire les risques de dépendance à l'endroit des fournisseurs, Hydro-Québec a établi une politique selon laquelle tout fournisseur ou consultant désireux de conclure un marché avec Hydro-Québec devra démontrer que ses biens ou ses services respectent les nouvelles exigences de conformité au passage à l'an 2000.

#### *La vérification interne et externe de la conformité*

Plusieurs organisations ont mis en place des groupes de vérification interne visant à certifier les diverses composantes informatiques. Le rôle de ces groupes a permis notamment de répondre aux questions suivantes : est-ce que les inventaires sont complets ? est-ce que tous les liens inter-applications ont été identifiés ? est-ce que les tests ont été complétés avec succès ? est-ce que la conformité des produits commerciaux a été vérifiée auprès des

fournisseurs ? D'autres ont également cherché l'avis d'experts-conseils externes afin de mesurer objectivement l'état de la situation. Par exemple, l'ITAA (Information Technology Association of America) offre un programme de certification à l'an 2000 au coût approximatif de 8 000 \$.

#### *L'incontournable mise à l'essai*

Ce n'est pas parce qu'un champ de date comporte 4 positions pour l'année qu'une composante est conforme. Inversement, ce n'est pas parce qu'une date est à 2 positions qu'elle n'est pas conforme. Aussi, même lorsque les essais des fournisseurs démontrent que les logiciels de base sont conformes, plusieurs utilisateurs croient que la seule façon d'être certain est de les tester dans leur propre environnement personnalisé<sup>21</sup>. De plus, l'interaction des systèmes multiplie le nombre d'essais à effectuer. Selon le rapport de l'*Office of Management and Budget*, les systèmes d'information, parce qu'ils interagissent et qu'ils échangent des informations, doivent être testés les uns par rapport aux autres.

#### *Les plans d'urgence ou de contingence*

Dans une enquête récente menée auprès de 128 compagnies américaines<sup>22</sup>, 72 % d'entre elles travaillaient à la planification de la contingence. En clair, il est temps que les grandes entreprises en retard anticipent les conséquences de défaillances possibles de leur fonctionnement sur leurs partenaires commerciaux et prennent les précautions nécessaires pour atténuer l'ampleur de ces perturbations. Dans les divers plans de contingence, que ce soit dans les sociétés ou les services publics, on propose les mesures suivantes :

- La police devrait accroître ses effectifs en prévision des interruptions de feux de circulation ou des pannes d'électricité qui risquent de s'accompagner d'actes de pillage et d'autres méfaits.
- La division de la prévention des incendies devrait accroître ses effectifs en prévision des fausses alertes et des incendies causés par un problème de détection.
- Les familles devraient s'assurer du plein de mazout, d'un approvisionnement suffisant en nourriture, de réserves en espèces.
- Lorsque les projets de remplacement ne pourront être complétés à temps, la méthode de conversion peut être utilisée. Si la méthode de conversion est trop longue, la méthode de fenêtrage peut être utilisée.

---

<sup>21</sup> Gartner Group, « Year 2000 : Do your Software Licenses Have a Silver Lining ? », 27 février 1997.

<sup>22</sup> DCI IT New, « Year 2000 Update », 19 août 1998.

- ❑ Lorsqu'un projet ne peut arriver à temps, quelle que soit la méthode, des procédures manuelles peuvent être mises en place.
- ❑ Certaines usines de transformation fonctionneront au ralenti au passage de l'an 2000 pour être en mesure de mieux observer le déroulement.
- ❑ Une entente au préalable avec des partenaires commerciaux pourrait parer aux éventualités comme pour les services de prises de commande, de la paye ou de la comptabilité.

Un des pièges de la contingence est de réduire l'efficacité des projets en cours en accaparant les ressources déjà sollicitées. Dans d'autres cas, la contingence est carrément impossible à réaliser dans les délais prévus. Les organisations sont alors dans une impasse. De plus, on peut douter du succès des projets de contingence ; si une organisation démontre un grand retard, on peut douter de sa capacité à instaurer un plan de contingence adéquat.

### ***Les limites des solutions***

Le plus dangereux de tout, c'est lorsque aucune solution ne peut être employée. Par exemple :

- ❑ On ne peut modifier certaines applications en opération parce que leurs codes source ont été perdus ou détruits par inadvertance.
- ❑ On ne peut obtenir des versions conformes ou avoir accès au code source lorsque les fournisseurs ne sont plus en affaires.
- ❑ On ne peut installer de nouvelles versions de certains équipements très spécialisés parce que des fournisseurs n'ont plus de disponibilité.
- ❑ Les solutions ne peuvent être adoptées à temps par manque de ressources humaines ou de ressources techniques.
- ❑ Certains problèmes ne seront détectés que si les ordinateurs sont redémarrés, comme dans le cas de certains ordinateurs personnels.



## ***Les risques méconnus et sous-estimés***

Pendant que les ressources se consacrent au problème de l'an 2000, on ne procède pas à l'amélioration ou à la correction des autres problèmes. Cette situation réduit, par ricochet, la qualité du service et retarde des projets d'amélioration. Il s'agit là d'un risque souvent sous-estimé.

Un second problème provient de la fausse impression de conformité. Il faut avoir un doute raisonnable quant aux affirmations des organisations relatives à leur état de conformité. Celles-ci peuvent volontairement ou involontairement induire en erreur les utilisateurs. Bien qu'un grand nombre d'organisations soient de bonne foi, nul n'est à l'abri d'une fausse déclaration. Par exemple, après avoir déclaré tous ses appareils conformes à l'an 2000, le fabricant d'ordinateurs Compaq<sup>23</sup> s'est ravisé lorsqu'on a découvert que des modèles ont échoué le test de l'horloge interne.

Enfin, certaines composantes non répertoriées dans les inventaires pourraient s'avérer non conformes, le changement de logiciel pour une version plus récente pourrait ne pas avoir été fait systématiquement, des composantes jugées non conformes pourraient être omises et demeurer en opération, les multiples liens inter-composantes pourraient être désynchronisés.

## **QUELQUES HYPOTHÈSES SUR LES RISQUES À VENIR**

Lequel des scénarios, optimiste ou pessimiste, doit-on privilégier ? Est-ce que les scénarios apocalyptiques sont crédibles ou sont-ils seulement une tactique pour accroître la sensibilisation et mobiliser les intervenants ? La difficulté à laquelle nous faisons face est celle de l'évaluation objective du risque. En effet, l'identification des risques plausibles est difficile. Néanmoins, sachant qu'en situation normale les entreprises sont exposées à un certain nombre de risques informatiques, on peut s'attendre à ce que l'an 2000 multiplie leur survenance. Des problèmes pourraient être interprétés par les utilisateurs et par la population comme étant reliés à l'an 2000 même si leur nature est tout autre.

---

<sup>23</sup> DCI ITNews, « Year 2000 Update », 19 août 1998.

Fait intéressant, on a constaté que dans le secteur industriel, 1 à 2 % des contrôles échantillonnés se sont avérés non-conformes et que ce pourcentage est de 4 % dans le secteur maritime sur un échantillon de 3,100 composantes. Selon l'Association des hôpitaux du Canada, le taux de défaillance du matériel et des instruments médicaux oscille entre 7 et 10 %. Ces données doivent certainement être prises en compte dans l'évaluation des probabilités de défaillance.

Une approche hypothétique pour l'évaluation du risque est indispensable puisque nous n'avons aucune expérience concrète de ce phénomène jusqu'à maintenant. Voici donc quelques-unes des hypothèses qui peuvent être prises en compte lors de l'évaluation des risques.

Hypothèses	Description
Âge	Plus le parc d'équipement informatique est âgé, plus le risque est grand. En effet, bon nombre d'équipements et de logiciels conçus avant les années 1990 peuvent ne pas être conformes.
Automatisation	Plus les entreprises comporteront de mécanismes sophistiqués tels que des automates et des robots, plus le risque sera grand.
Centralisation	Plus le traitement de l'information et la gestion des systèmes d'information sont centralisés, moins le risque est élevé. La centralisation limite généralement la personnalisation des composantes informatiques, permet d'exercer un meilleur contrôle sur les changements et facilite la vérification et l'établissement de normes de conformité.
Complexité	Plus les opérations et l'environnement technologique sont complexes, plus le risque est élevé. Les composantes plus complexes nécessitent généralement plus de temps d'analyse, elles impliquent également l'intervention d'une expertise qui, dans un contexte de pénurie, est d'autant plus difficile à mobiliser. La complexité peut également réduire le temps disponible pour effectuer des changements.
Concentration	Plus les projets de remplacement et de conversion sont concentrés sur une même période, plus c'est risqué. Cela s'explique par le niveau élevé de changements qui déstabilisent les organisations et qui diminuent les chances de succès des projets.
Diversité	Plus les composantes et l'environnement technologique sont divers, plus le risque est élevé. La diversité est signe d'hétérogénéité, de multiplication des modèles, des modes de configuration et fonctionnement. Par conséquent, le temps d'intervention total est accru, ce qui multiplie les difficultés de coordination.

Interrelation	Plus les systèmes informatiques auront des liens avec d'autres systèmes à l'interne ou à l'externe, plus le risque sera grand. L'interrelation accroît les difficultés de synchronisation et nécessite une plus grande coordination des changements et de la vérification de la conformité.
Maturité	Plus les organisations sont matures, moins le risque de défaillances dues à l'an 2000 est élevé. La maturité n'est pas nécessairement liée à l'âge mais plutôt à la rigueur et à l'efficacité du processus logiciel et de la gestion des systèmes d'information.
Qualité	Plus les composantes sont considérées de bonne qualité, moins le risque est élevé. La qualité peut notamment correspondre au respect des normes de programmation et de documentation, à la stabilité du logiciel, à l'absence de redondance, à une nomenclature organisée, etc. Les interventions sont toujours plus efficaces lorsque la qualité est présente, par conséquent, le risque de non-respect des échéances est amoindri.
Régulation	Plus les organisations seront réglementées par législations ou autres mécanismes de contrôles externes, moins les risques seront grands. On présume que le rôle du régulateur aura incité à prendre les moyens nécessaires pour résoudre le problème.
Spécialisation	Plus les composantes et l'environnement technologique sont spécialisés, plus le risque est élevé. La spécialisation implique généralement une production restreinte et une personnalisation de l'entreprise comme pour les applications développées à l'interne ou les logiciels commerciaux peu répandus. Les applications et le matériel informatiques spécialisés sont généralement plus fragiles parce qu'ils ne profitent pas de l'expérience accrue en production de masse.
Stabilité	Plus les opérations sont en situation d'instabilité, plus le risque est élevé. En effet, les environnements informatiques instables sont un symptôme d'une mauvaise organisation du processus logiciel. Dans ce cas, les modifications ou le remplacement des logiciels non conformes présentent un taux d'échec élevé ou sont sujets à certains retards.
Taille	Les grandes organisations sont souvent moins aptes à mobiliser l'ensemble de leurs unités. Par contre, elles disposent de moyens financiers accrus et peuvent recourir plus facilement à des solutions de rechange.
Vitesse	Plus les opérations ou la production s'effectuent à grande vitesse et à grand volume, comme pour les usines d'assemblage, plus le risque sera grand. En effet, la vitesse implique un temps de réaction efficace et si un problème est rencontré, plus d'un produit pourrait être affecté.

## CONCLUSION

Prédire les risques associés au passage de l'an 2000 est encore une affaire de spéculation pour la majorité des individus et des organisations concernées. L'évaluation des risques pour la collectivité va au-delà de leur simple somme, et il faut appliquer une série d'hypothèses menant à des scénarios, du plus au moins probable.

Entre le discours alarmiste et le discours rassurant, il est difficile de porter un jugement objectif sur l'état réel de la situation et sur ce qu'elle sera le 1<sup>er</sup> janvier 2000. D'une part, l'industrie se rapproche de jour en jour d'une plus grande conformité et, d'autre part, plusieurs faits nous démontrent le manque de moyens. N'y a-t-il pas un biais systématique et une exagération de part et d'autre des interlocuteurs ? Il y aura certes des problèmes, mais sans doute pas dans la mesure où certains le prédisent. Le défi est de tracer un portrait réaliste des scénarios tenant compte à la fois des aspects techniques, organisationnels et psychologiques. Considérant le comportement des individus en situations d'incertitude, la volonté certaine des organisations à résoudre le problème, la capacité d'appliquer des solutions et le phénomène de médiatisation, nous croyons que les risques majeurs sont surévalués et que, par contre, les risques mineurs sont sous-évalués. Notons, toutefois, la multiplicité des risques mineurs pourrait paralyser tout autant les organisations.

Dans la courte histoire des technologies de l'information, nul doute que cette crise marquera l'industrie. Saurons-nous apprendre de ce phénomène ? Serons-nous capable d'éviter que ça se produise de nouveau ? Selon plusieurs opinions, le problème de l'an 2000 n'est pas tellement technologique; il s'agit plutôt d'un problème de gestion. En fait, plusieurs organisations se sont butées à cette dure réalité et ont dû repenser la façon de gérer les systèmes d'information, que ce soit au niveau des inventaires, de la rigueur des essais et des normes de qualité. C'est une leçon dont tous se souviendront, à savoir que *l'absence de qualité et le non-respect des normes* ont un prix. La création d'une corporation professionnelle, capable d'instaurer un code d'éthique et une réglementation, permettrait peut-être d'éviter qu'une telle situation se reproduise.

Mais encore faut-il composer avec certaines tendances de fond. L'obsolescence en informatique, c.-à-d. la perte de valeur économique due au retard technologique, est très élevée. Les logiciels comportent de nouvelles versions à peu près toutes les années, les ordinateurs

doublent de puissance en moyenne tous les 18 mois. En même temps, plus d'un facteur incite à capitaliser sur les technologies de l'information pour renouveler les pratiques d'affaires. Cette course effrénée au changement, jumelée à une forte variabilité de l'environnement technologique, est peut-être le grand responsable de la situation actuelle.

Cette crise nous aura fait comprendre que les organisations ont une capacité limitée de changements et qu'une progression moins anarchique assurerait une meilleure stabilité et une meilleure qualité des systèmes d'information. Le bogue de l'an 2000 a peut-être ceci de positif : c'est une occasion idéale de revoir les principes de gestion et de questionner les priorités.