

# FEDISA

## COMMISSION RISQUES & ASSURANCES

**Réunion de lancement – Jeudi 6 mai 2010 – 17h**

**Jean-Laurent SANTONI**

L'objectif de cette Commission de travail est d'éclairer les aspects risques et assurance liés à la preuve électronique. Les risques stratégiques et financiers étant hors de notre champ de contribution, sont essentiellement appréhendés les risques opérationnels et aléatoires.

Trois typologies de risques doivent à notre sens être visées :

- Les risques du projet stricto sensu (projet : moyens, ressources humaines, démarche, planification, management... ; contractuel : relations avec des prestataires externes, contenu du contrat... ; fonctionnel : fonctionnalités du produit, ergonomie, interfaces, service rendu à l'utilisateur... ; technique : architecture, performances, technologies, matériels et logiciels de base, configuration des postes de travail... ; organisationnel : structures, procédures, acteurs).
- Les risques de conservation des données archivées (disponibilité : pouvoir accéder à l'information recherchée ; intégrité : faire en sorte que l'information obtenue soit correcte ; confidentialité : garantir que seules les personnes habilitées accèdent à l'information ; auditabilité : permettre de tracer de manière fiable l'émetteur et le destinataire de l'information).
- Les risques de non restauration des données ou de perte de valeur probante

On ne reviendra pas sur les risques du projet stricto sensu qui ne diffèrent pas de tout projet de dématérialisation et d'archivage électronique, risques pour lesquels les réponses assurantielles en matière de garantie de bonne fin de projets informatiques sont très faibles.

### **Risque de la preuve « électronique » ou de l'électronique probante ?**

A notre sens, répondre à la question de la gestion des risques et du transfert assurantiel revient à aborder d'une part la problématique liée à la force probante de l'information et d'autre part celle de l'informatisation de la preuve. En d'autres termes, il s'agit de savoir s'il s'agit d'un problème de dommage informatique à la preuve, ou d'une responsabilité liée à la perte de force probante de l'informatisation.

#### Domage informatique à la preuve.

Cette approche s'inscrit dans une dimension technique afin d'identifier les multiples faits générateurs potentiels de dommage et leurs incidences en termes de coût. Elle suppose la mise en œuvre de six grandes classes de mesures de sécurité, qui permettent à la fois la gestion du risque et l'appréciation par l'assureur du niveau de risque résiduel qu'il assume :

- Mesures structurelles : éviter certaines agressions en jouant sur la structure même du système d'information ;
- Mesures dissuasives : permettent, en jouant sur l'organisation et en utilisant des mesures techniques, d'éviter que l'agresseur ne mette à exécution sa menace.
- Mesures préventives : évitent qu'une agression n'atteigne le système d'information (barrage, contrôle d'accès, détection-interception...)
- Mesures de protection : empêchent les détériorations ou en limitent l'ampleur (détection-réaction, anti-propagation...)
- Mesures palliatives : permettent de limiter les conséquences d'une détérioration en la masquant et en proposant des solutions de repli.
- Mesures de récupération : permettent de récupérer une partie du préjudice subi par transfert des pertes sur un tiers (clauses contractuelles, actions en justice...)

#### Responsabilité liée à la perte de force probante de l'informatisation.

Cette approche s'inscrit dans une dimension davantage juridique et vise les faits générateurs susceptibles d'entraîner la mise en cause de la responsabilité de l'entité considérée (entreprise privée ou collectivité publique, fournisseur des produits ou de services), et la mise en jeu de la garantie de l'assureur. Pour ce faire, nous préconisons une analyse des critères déterminant le comportement des victimes (approche socio-comportementale). Il est important de connaître la ou les catégories socioprofessionnelles des cocontractants afin de savoir à qui s'adresse la prestation, la nature des informations traitées (plus les données seront dites sensibles, plus l'éventualité d'une réclamation sera grande), le degré de technicité nécessaire à l'utilisation. En outre, dans les contrats passés entre professionnels, l'introduction de clauses limitatives de responsabilité est de nature à minorer le risque de responsabilité. L'étude juridique est un élément déterminant de la protection des mises en cause.

#### **Assurance de la preuve « électronique » ou de l'électronique probante ?**

L'optimisation de la protection d'assurance dépend de la situation de l'assuré : soit l'assuré porte le risque de la preuve « électronique » et auquel cas il ne pourra garantir que les dommages atteignant cette preuve, assumant seul le risque de perte du caractère probant ; soit l'assuré est l'entité professionnelle qui assume à la fois le risque de la preuve « électronique » confiée par un tiers et le risque d'électronique probante, et cela pourrait se traduire par la mise en place d'une double couverture, la première étant une indemnisation de type « dommage pour compte » et la seconde, plus traditionnelle, mettant en jeu des contrats de responsabilité civile professionnelle, exploitation et le cas échéant produit.

#### Les Dommages pour compte

Cette couverture vise l'indemnisation forfaitaire des pertes financières subies par toute personne (personne physique ou morale) en cas d'indisponibilité du service ou document archivé, voire à l'atteinte à l'intégrité ou la confidentialité de ce document sécurisé avant même que la responsabilité civile professionnelle ne soit mise en cause.

L'indemnisation à verser se veut immédiate dès lors que le préjudice subi est quantifié; ce premier niveau indemnitaire permet d'apporter une solution financière rapide aux sinistres isolés en évitant une mise en cause directe de la technologie utilisée ou des procédures d'archivage ou de gestion de la preuve.

Cette protection financière peut également bénéficier à l'assuré qui porte le risque de la preuve « électronique » puisqu'il s'agit d'une assurance de dommages et non pas d'une assurance de responsabilité supposant d'être un tiers pour être indemnisé.

Sous réserve d'une analyse plus précise des besoins de garantie, on peut imaginer que l'assurance de dommages permettrait le remboursement des pertes financières directes, quantifiables et justifiées, subies par la personne utilisatrice du service en cas d'atteinte à la conservation ou à la validité probante résultant d'une erreur accidentelle ou résultant d'une fraude ou d'un acte de malveillance. Par fraude ou acte de malveillance, on entend les actes de détournement et/ou d'appropriation illégitime d'une information ou d'un bien corporel ou incorporel suite à usurpation d'identité de la personne, utilisation ou détournement de l'archive et compromission de l'archive. Egalement pourrait être pris en compte le remplacement des archives perdues, détériorées accidentellement ou détruites accidentellement. Au titre du service, chaque personne ayant la qualité d'Assuré bénéficierait d'une garantie par volume d'archivage ou volume d'utilisation du service, avec une limite maximum qui s'appliquerait pour l'ensemble des pertes financières garanties survenant au cours d'une même période d'assurance. En outre, le montant de la garantie par période d'assurance et le niveau de la garantie pourraient dépendre de la catégorie ou de la nature du service rendu (archivage, archivage à valeur probante, attestation de gestion de preuve).

#### La responsabilité civile professionnelle

Dans l'hypothèse où une circonstance exceptionnelle, un accident, une erreur ou un acte malveillant plus généralisé impacteraient de façon massive la technologie ou les procédures de l'entité (entreprise privée ou collectivité publique, fournisseur des produits ou de services), le processus d'indemnisation pourrait prévoir, au delà d'un seuil défini contractuellement, le basculement des réclamations du contrat dommage dans la couverture responsabilité civile, ceci afin d'augmenter la capacité indemnitaire. Il en résulterait la prise en charge par l'Assureur des conséquences pécuniaires de la Responsabilité Civile que l'entité peut encourir, quel que soit le fondement sur lequel la responsabilité est recherchée, du fait des dommages corporels, matériels et immatériels consécutifs ou non, susceptibles d'être causés à un tiers du fait des activités notamment suite à la défaillance du procédé technologique, d'un défaut d'application totale ou partielle des procédures résultant d'une erreur, omission, faute, négligence humaine.

Dans tous les cas, la difficulté principale que nous relevons tient dans le moment de la constatation du sinistre et de la question de l'imputabilité du contrat d'assurance. En d'autres termes, il s'agit ici de prendre en considération la temporalité, situation que les assureurs connaissent bien en assurance de construction décennale pour laquelle la garantie de dommages-ouvrage est acquise pendant une période de dix années au cours de laquelle le vice de construction peut se révéler. Des problématiques similaires existent en matière de

responsabilité produits, intégrant notamment les dispositions de la Directive Européenne sur les produits défectueux et son correctif lié au risque de développement. La question sera donc de savoir quel sera l'assureur (ou solidairement ou non les assureurs successifs) qui sera appelé en garantie le jour de la révélation du préjudice matérialisé soit par un dommage informatique à la preuve, soit par la perte de la force probante de l'informatisation. A défaut d'avoir la réponse, nul n'ignore plus la question.