BENOÎT DE ROQUEFEUIL, AVOCAT À LA COUR, CABINET BENSOUSSAN

# Contrats informatiques : savoir mesurer la conformité des prestations

Nature du projet, produits et services fournis, nombre des intervenants... Les contrats informatiques sont souvent d'une telle complexité que la mesure de conformité constitue elle-même une réelle difficulté.

*Benoît de Roquefeuil*

En droit des obligations, l'obligation principale du débiteur d'une obligation de faire (contrat de services) ou de donner (contrats de vente, de prêt ou de location) est de délivrer une chose ou une prestation conforme à l'usage convenu entre les parties. S'agissant des contrats informatiques, leur objet est quasi systématiquement d'une grande complexité, soit en raison de la nature même du bien fourni ou du service exécuté, soit en raison de la pluralité des fournitures (logiciels + matériels + services). D'une telle complexité il résulte naturellement que la mesure de la conformité des prestations ou des fournitures se révèle également particulièrement difficile et même parfois aléatoire. En pratique, on peut constater une véritable inflation des clauses de réception dans les contrats.

En effet, les clauses de réception, improprement dénommées «recette», renvoient désormais très souvent à des cahiers de recette de plus en plus élaborés qui ne sont pas toujours finalisés au jour de la signature du contrat, ou insuffisamment personnalisés par rapport au contrat (usage de cahier de recette type). Ainsi, les rédacteurs de contrats ne disposent pas toujours (pas souvent) des moyens techniques suffisants pour valider les processus de vérification de conformité qui sont mis en œuvre au terme de l'exécution des contrats.

## Outils normatifs

La mesure de la conformité constitue donc une réelle difficulté qui, si elle ne peut être maîtrisée complètement par la maîtrise d'ouvrage, accroît sensiblement son risque d'exploitation. Un certain nombre d'outils normatifs se sont développés ces dernières années dans le but de permettre aux utilisateurs des technologies de l'information de mieux maîtriser de tels risques. Ainsi, la norme COBIT, "référentiel de gouvernance des systèmes d'information" définit un ensemble de bonnes pratiques pour mesurer l'efficacité des systèmes d'information au regard des objectifs de l'entreprise et des risques technologiques associés. L'intégration des outils de mesure COBIT dans le contrôle de pertinence des approvisionnements, le contrôle de conformité des fournitures (matérielles ou intellectuelles) et l'analyse des qualités de service présente un double avantage.En effet, en premier lieu, il permet d'optimiser et d'harmoniser les processus de mesure de la conformité pour toute évolution des systèmes d'information. En second lieu, l'adoption des systèmes d'évaluation COBIT autour des 34 processus d'évaluation liés aux technologies de l'information confère également une «lisibilité» à l'entreprise, en vue d'éventuels audits auxquels elle pourrait être soumise.

## Processus structurants

La difficulté, néanmoins, pour l'adoption des normes COBIT réside dans le fait qu'elle suppose l'adhésion en parallèle à un processus qualitatif contraignant et le recours à d'autres processus normatifs qui, fortement structurants pour l'entreprise, supposent une conduite du changement de grande envergure.

Par ailleurs, il est possible que, dans certaines organisations, l'utilisation des modèles de gouvernance COBIT pour le contrôle des systèmes d'informations induisent des exigences de normalisation à la charge de fournisseurs de l'entreprise. Ainsi, pour l'acquisition et/ou la mise en œuvre de logiciels ou de progiciels, il pourrait être exigé que ces produits aient été développés suivant des normes de type CMMI ou "unified process" qui correspondent à autant de modèles ou référentiels de processus de production logicielle.

De même, pour les services, les règles de gouvernance COBIT pourraient conduire à exiger des prestataires qu'ils respectent les processus de production de services informatiques définis par les « bonnes pratiques » ITIL (Information Technology Infrastructure Librairy), associées aux "processus de certification British standard BS15000 ET BD0005" du British Standard Institute. Enfin, la gouvernance COBIT peut encore induire l'exigence du respect de normes de gestion de projet, telles que notamment PMI ou PRINCE2.

## Recours à des "bonnes pratiques"

Une telle exigence de normalisation transverse permet sans doute de faciliter les convergences entre les processus des organisations amenées à travailler ensemble pour des périodes plus ou moins longues sur des opérations concernant les systèmes d'informations (contrat d'externalisation, d'intégration de systèmes, de tierce maintenance applicative…). De ce fait, le recours à des « bonnes pratiques » communes est de nature à optimiser la sécurité et la conformité.

Pour autant, il est nécessaire de prêter attention à ce que l'optimisation de la sécurité par le recours à des processus normés ne soit pas un facteur de rigidité trop important qui pourrait priver, par exemple, l'entreprise de la possibilité d'avoir recours à des produits ou services qui lui paraîtraient particulièrement adaptés et dont la conception et l'exécution ne seraient pas certifiées suivant les normes jugées compatibles par les règles de gouvernance adoptées en interne.

Les normes sont donc de plus en plus précises et efficaces, et constituent un facteur de progrès considérable, notamment en terme de mesure de la conformité, mais elles doivent cependant être implémentées et appliquées avec discernement. Ainsi, il conviendra de veiller à ce que, à périmètre qualitatif égal, les normes régissant les processus de production et/ou d'organisation des fournisseurs de services soient substituables les unes par rapport aux autres afin d'éviter un appauvrissement de l'offre concurrentielle d'une part, et que s'impose un standard unique d'autre part.■