Ateliers *Cloud Computing* / ADIJ / [Atelier n°4 – 20 janvier 2011]

# *Solutions aux risques juridiques et catalogue des meilleures pratiques contractuelles*

Co-animés par Helle Frank Jul-Hansen , Béatrice Delmas-Linel et David Feldman

Blog : http://cloudcomputingadij.eklablog.fr

ADIJ
Association pour le Développement de l'Informatique Juridique
http://www.adij.fr

# *Atelier n° 4*

**Le 20 janvier 2011, Maison du Barreau, Paris**

Intervenant principal :

- Frédéric Connes, Consultant Hervé Schauer Consultants (HSC)

**Thème** : **Identifier les problématiques juridiques et techniques liées à la sécurité du *Cloud Computing*.**

Nous reprenons ci-dessous les points de discussion les plus marquants de la réunion, en remerciant à nouveau nos invités pour leurs témoignages de qualité.

***

## Synthèse

### 1. Introduction

A l'heure où le *Cloud Computing* s'impose peu à peu comme la façon incontournable de « consommer de l'informatique » pour les entreprises de toutes tailles, la question de la sécurité qu'il offre cristallise les débats. Si cette question est loin d'être nouvelle, force est de constater que le Cloud Computing semble agir comme un révélateur d'un débat latent en informatique.

Ainsi, « *Sans tomber dans l'angélisme, nous pouvons affirmer qu'en matière de sécurité, le Cloud Computing n'est pas un agent « anxiogène » supplémentaire* »[1] nous explique Philippe Hedde, Président du Comité Infrastructures Syntec Numérique.

A l'inverse, l'ANSSI (Agence Nationale pour la Sécurité des Systèmes d'Informations) considère qu' « *il est plus difficile* [ndlr : dans le *Cloud Computing*] *de se prémunir de ces risques que dans l'infogérance classique. En effet, le client souscrit le plus souvent à des offres par validation d'un contrat type qu'il est souvent impossible de personnaliser en y intégrant des clauses particulières en matière de sécurité*.»[2]

Si ces divergences de position s'expliquent notamment par la fonction et le rôle de leurs auteurs, on constate qu'il n'existe à ce jour aucun consensus parmi les experts quant au fait de savoir si le *Cloud Computing* présente moins, tout autant, ou au contraire davantage, de sécurité que l'infogérance traditionnelle. Quant au point de vue juridique, les problématiques sont-elles nouvelles et suscitent-elles des solutions différentes de l'arsenal existant en matière de niveau et partage des responsabilités, contrôles et audits, indemnisation et certification ?

La question centrale pour les prestataires est donc la suivante : comment encourager l'adhésion au *Cloud Computing* tout en permettant aux clients de bénéficier de la sécurité nécessaire à leurs données ?

---

[1] Syntec Numérique : Livre Blanc Sécurité du *Cloud Computing* – Analyse des risques, réponses et bonnes pratiques – 2010.
[2] ANSSI : Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information - Décembre 2010 http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf

Afin de poser les fondamentaux du débat, M. Connes a partagé une présentation qui s'est attachée à refléter les définitions et l'expérience des spécialistes de la sécurité informatique (voir ci-joint le document « ADIJ Cloud Comp. Présentation F. Connes HSC 20 janvier 2011 »).

Les questions suivantes ont été abordées :

2. **Comment se définit la sécurité ?**

La sécurité se définit par la réunion des trois éléments suivants :

- Confidentialité : les données ne doivent pas être divulguées à des tierces parties ;
- Intégrité : les données ne doivent pas être déformées par l'usage et/ou par le temps ;
- Disponibilité : les données doivent être accessibles par le client en permanence, à sa convenance (la sécurité est ici entendue au sens large, la disponibilité pouvant également être considérée comme relevant de la qualité de service).

3. **Le *Cloud Computing* privé est- il une étape ou un aboutissement ?**

Dans la mesure où le modèle économique du *Cloud Computing* repose sur une mutualisation des ressources, les intervenants s'accordent sur le fait que le *Cloud Computing* privé, susceptible d'offir une sécurité acrrue, n'est pas du « vrai » *Cloud Computing* et ne serait en réalité qu'une étape vers la généralisation du *Cloud Computing* public, seul modèle véritablement proposant cette mutualisation.

Il est cependant probable que certains clients (administration publiques, institutions financières et autres) seront contraints d'adapter des solutions de cloud privé, communautaires et/ou hybrides et ne passeront pas en mode cloud public. Les autres utilisateurs adopteront probablement des solutions diversifiées, dites cloud hybrides, en fonction de la nature de leurs données et des applications utilisées.

En tout état de cause, la mutualisation des données, et le caractère collaboratif des solutions de *Cloud Computing*, va de pair avec un accroissement du risque sécuritaire, puisque l'isolation des données n'est par définition pas garantie.

4. **Quel est le ressenti des prestataires du *Cloud Computing* quant aux craintes de leurs clients ?**

Au-delà du point de savoir si le *Cloud Computing* est plus ou moins sécurisé que l'infogérance traditionnelle, les témoignages des intervenants représentants des prestataires de services en matière de *cloud* révèlent que le *Cloud Computing* a exacerbé les craintes de leurs clients, qui existaient déjà en matière d'infogérance. Les intervenants prestataires ont témoigné d'une certaine frustration à cet égard : « Nos clients nous demandent de devenir assureurs plutôt que d'être responsables en matière de sécurité du *Cloud Computing*. »

Ainsi, la perte de contrôle liée à la mutualisation des ressources et à une localisation plus incertaine des données renforcerait les exigences de ces clients.

Est-il pourtant raisonnable d'exiger un niveau de sécurité supérieur au niveau pouvant être assuré par des solutions comparables internalisées ? D'aucuns, parmi les intervenants, soutiennent que les attentes des entreprises clientes doivent être relativisée et qu'elles doivent prendre conscience de ce que le « 100% sécurité » n'est qu'illusoire.

5. **Quels sont en revanche les avantages du *Cloud Computing* pour la sécurité ?**

Sans en dresser une liste exhaustive, les avantages suivants ont été évoqués :

- La capacité d'augmenter quasi-instantanément les ressources offre une meilleure disponibilité de celles-ci. Le risque de saturation est dès lors minimisé.

- La duplication des données en diverses zones géographiques permet de pallier le risque lié à la défaillance d'une de ces zones. Il est intéressant de noter ici le paradoxe lié à cette ubiquité : ainsi alors que celle-ci constituerait un avantage en matière de sécurité, elle est problématique du point de vue du transfert des données personnelles transfrontalier et hors Union Européenne (cf. la synthèse de la troisième réunion de l'Atelier).

- La virtualisation des machines offre également l'avantage, par rapport à une machine physique, de permettre en cas de défaillance, de restaurer plus facilement son système par back-up.

- Un autre avantage indirect est propre à toute opération d'externalisation de services, à savoir que le risque lui-même est externalisé (et peut donc être géré et encadré contractuellement).

- Enfin, le *Cloud Computing* peut présenter un avantage en matière probatoire. La virtualisation permet de prendre une image (« *snapshot* ») du système sans que celui-ci ait à être interrompu. Il n'est donc plus besoin par exemple d'interrompre les serveurs et de placer les machines sous scellés. A terme, se posera assurément la question de la force probante de ces *snapshots* au plan judiciaire (ce qui pourra faire l'objet d'un autre débat, en dehors du cadre de cet atelier). Mais dans l'immédiat, cette possibilité de réaliser des s*napshots* permet de procéder à l'analyse du système par exemple pour de déterminer les causes d'une défaillance.

## 6. Quels sont les risques du *Cloud Computing* pour la sécurité ?

- Le principal inconvénient, et en tous les cas perçu comme tel par les clients utilisateurs, tient naturellement à la perte de maîtrise par le client de certains éléments (matériel, logiciel, réseau) jusqu'alors détenus ou contrôlables « *on premise* » par ce dernier. Autrement dit, sur ces éléments, le client se retrouve dans une dépendance vis-à-vis de son prestataire.

C'est au final cette perte de contrôle et de maîtrise qui chez le client exacerbe sa perception de risque de sécurité plus important dans les offres de *Cloud Computing*, les poussant à renforcer leurs exigences en matière de sécurité.

Et naturellement, cette inquiétude augmente dans l'hypothèse de plusieurs sous-traitances puisque le client doit non seulement gérer la perte de maitrise mais également la multiplication des acteurs de la chaîne contractuelle (et le risque juridique lié à celle-ci).

- Il existe également un risque lié à la perte de contrôle sur les données qui sont stockées chez le prestataire. Le client n'a aucune maitrise sur les administrateurs du prestataire. De même, le client ne dispose d'aucun contrôle sur le sort de ses données en fin de contrat (expiration, résiliation). L'objectif est de parvenir à un effacement définitif des données pour éviter que celles-ci ne demeurent sur un espace de stockage qui pourrait être mis à disposition d'un nouveau client.

- Il existe un risque lié à l'interface web de gestion des services. En effet, les données d'authentification peuvent être compromises ou détournées. Cependant, il s'agit d'un risque propre à toute interface protégée par mot de passe.

- Le risque de dépendance à son prestataire prend également la forme du phénomène de Vendor/ Technology « Lock-in », à savoir l'impossibilité ou l'extrême difficulté à changer de fournisseur ou de technologie, ou encore de revenir à des solutions internes. Ce défi de la réversibilité tient, à ce jour, à l'absence de normes sur l'interopérabilité et la migration dans le contexte du *Cloud Computing*. Nous rappelons à cet égard que lors de notre prochaine réunion, nous traiterons les questions de la réversibilité et de l'interopérabilité (standards) en matière de *Cloud Computing*.

La question des certifications a également été rapidement évoquée. Dès lors qu'elles sont délivrées par des organismes indépendants, ces certifications doivent être encouragées.

Néanmoins, à ce jour, elles ne suffiraient toutefois pas à rassurer intégralement les DSI. A ce jour, les deux principales sont les normes SAS 70[3] et ISO 27001[4].

Il convient de noter que sur tous les points relevés ci-dessus, les participants de l'Atelier ont longuement débattu sur la pertinence de rattacher certains concepts à la notion de Sécurité dans le *Cloud Computing* : par exemple la disponibilité des ressources, ou la réversibilité. Par ailleurs, tout au long de cette discussion est revenue la question de savoir en quoi ces avantages et risques étaient spécifiquement liés au Cloud Computing et présenteraient un caractère nouveau. Les animateurs de l'Atelier précisent à cet égard qu'à partir du moment où le *Cloud Computing* exacerbe les problématiques de sécurité, il est important de traiter cette question dans le cadre des travaux de notre Atelier.

### 7. Le 100% sécurité peut-il être garanti ? Comment se mesure cette sécurité ?

Bien qu'à notre connaissance, un seul acteur du *Cloud Computing* se soit engagé sur ce point à ce jour[5], ce niveau d'exigence serait illusoire. Parmi les trois critères de définition de la sécurité (cf. point 2 ci-dessus), seule la disponibilité serait susceptible d'être mesurée. Il serait difficilement concevable de garantir l'atteinte à l'intégrité dans la mesure où celle-ci ne se révèle que dans l'hypothèse où les données sont corrompues et/ la confidentialité dans la mesure où cette dernière ne se révèle que dans l'hypothèse d'une fuite.

En conclusion, les débats ont été vifs et n'ont pas permis d'approfondir les questions plus concrètes du traitement juridique et contractuel des engagements et responsabilités des prestataires du *Cloud Computing* en matière de Sécurité, afin de permettre un équilibre contractuel satisfaisant et opérationnel. Un sous-groupe sera mis en place sur cette question par les co-animateurs de l'Atelier grâce aux volontaires qui se sont manifestés en fin de réunion.

Les co-animateurs ont également indiqué que la prochaine réunion de l'Atelier abordera les questions de réversibilité et interopérabilité dans le *Cloud Computing*, et tout volontaire intéressé à intervenir sur le sujet, ou connaissant un spécialiste capable d'aider le groupe a comprendre les concepts techniques en jeu et la résonance que ces concepts peuvent prendre dans le cadre de la mise en œuvre de solutions de *Cloud Computing*, est chaleureusement invité à les contacter.

***

***Prochain Atelier : Jeudi 3 mars 2011,***

***de 17h30 à 20h30***

***[Lieu à confirmer : Espace Hamelin, Paris 16è]***

[3] http://sas70.com/index.html
[4] http://www.iso.org/iso/fr/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103
[5] http://www.ovh.com/fr/private_cloud/reseau/fiche_technique.xml