DE GAULLE
FLEURANCE
& ASSOCIÉS

SOCIÉTÉ D'AVOCATS

07 Juin 2011

CERT Ist - Forum 2011

Cloud Computing*: questions juridiques

Jean-Marie Job
Avocat associé
de Gaulle Fleurance & Associés
jmjob@dgfla.com

* Informatique en nuage

Ateliers ADIJ

Solutions aux risques juridiques et recherche des meilleures pratiques contractuelles

- *Groupe de travail: de 20 à 30 participants par séance dont:*
  Représentants des diverses parties (éditeur, clients, …)
  - CNIL
  - Avocats / Directeurs Juridiques
  - DSI
  - Assureurs
  - Experts en sécurité des systèmes d'informations

- *Objectifs:*
  ***Débattre** des problématiques juridiques générées par le Cloud Computing*
  *Etablir des **Bonnes Pratiques** en matière de contrats de Cloud Computing*

- *Blog et résumés de chaque séance:*

http://cloudcomputingadij.eklablog.fr

DE GAULLE FLEURANCE & ASSOCIÉS

SOCIÉTÉ D'AVOCATS

Le Cloud Computing : éléments de définition

« Le Cloud Computing est un concept désignant de nouvelles pratiques et services numériques reposant sur l'utilisation d'internet et de réseaux étendus et sur la mise en commun de ressources numériques et matérielles, qui se caractérisent par :

- *une flexibilité immédiate,*
- *une possibilité de paiement à la demande et*
- *une virtualisation des systèmes»* [AFDEL]

Dans la pratique, ce concept recouvre une multitude de scénarios variés et différents, du plus simple au plus complexe, visant des usagers allant du particulier à l'administration publique en passant par l'entreprise et les groupes d'entreprise. Cependant, la base commune de ces scénarios est contractuelle.

Quel environnement règlementaire pour le Cloud Computing ?

➢ Absence (à ce jour) de régime règlementaire spécifique

➢ Le Cloud Computing s'inscrit néanmoins dans un cadre règlementaire complexe

Contraintes règlementaires principales (en France) :

- Loi Informatique et Libertés : traitement des données à caractère personnel
- Règlementation sur les communications électroniques
- Commerce électronique et protection des consommateurs
- Règlementation des services financiers
- Règlementation fiscale et comptable
- Règlementations sectorielles (pour l'audit et la conservation de données sensibles: bancaires, santé…)

➔ **Il est donc impératif que l'objet et le périmètre du contrat soient très précisément définis.**

Protection des données personnelles

« *Bien souvent, les données personnelles sont difficiles à localiser du fait du recours à des services dits de Cloud Computing. Ces situations mettent en avant une double exigence: assurer la protection des droits des citoyens tout en limitant, pour les entreprises,* ***une application excessive d'une multitude de lois nationales*** »

➢ *Une difficulté : déterminer le responsable du traitement*

- ✓ *Les critères*
- ✓ *la CNIL envisage la possibilité d'une dualité de responsables de traitement*

Attention: application de la loi américaine (*Patriot Act*) qui autorise les autorités américaines à procéder à des contrôles sur les serveurs basés aux Etats-Unis

Protection des données personnelles

Le transfert des données personnelles hors Union Européenne

➢ Une conception large de la notion de transfert par les autorités de protections

➢ **Principe d'interdiction** de transférer des données personnelles hors UE sauf si :

- Protection « adéquate » dans le pays de destination
- Signature des Clauses Contractuelles Types de la Commission Européenne
- *Binding Corporate Rules* (BCR) mais uniquement au sein d'un même groupe donc ne peut pas inclure les prestataires
- L'entreprise d'accueil aux USA a adhéré au *Safe Harbor*
- Article 69 de la loi Informatiques et Libertés

➢ Travaux actuels entre la CNIL et ses homologues européens du G29 aux multiples objectifs :

- Présenter un cadre juridique **harmonisé** en matière de Cloud Computing afin de renforcer la sécurité juridique
- **Etendre** aux sous-traitants les BCR et / ou la protection du Safe Harbor

Multitude de scénarios Cloud, multitude de contrats possibles

➢ *Pas de contrat type unique*

➢ *Rattachement aux différents types de contrats connus et disponibles en matière d'informatique et d'Internet*

- *Infogérance*
- *Licence de logiciel*
- *Développement, maintenance*
- *Hébergement*

Fondamentalement, aucun des risques associés au Cloud Computing n'est « nouveau », tous ces risques peuvent être « contractualisés »

« Sans tomber dans l'angélisme, nous pouvons affirmer qu'en matière de sécurité, le Cloud Computing n'est pas un agent supplémentaire »

Philippe Hedde (Président du comité Infrastructures Syntec numérique)

➔ **La nouvelle donne, c'est l'ampleur possible des défaillances dans le nuage**

Les principaux outils contractuels au service du Cloud Computing

- **Plan d'assurance sécurité** (PAS): rédigé par le prestataire, il décrit l'ensemble des dispositions spécifiques que celui-ci prendra pour garantir le respect des exigences de sécurité du donneur d'ordre

- **SLA**s (contrats de niveau de service) en annexe du contrat principal dont l'objectif est de définir principalement les indicateurs de performance (qualité, disponibilité, temps de réponse, outils de mesure…)

- **Audits** par le client des mesures de sécurité (mais la mise en œuvre pratique peut être difficile surtout s'agissant d'un prestataire ou sous-contractant installé à l'étranger)

- **Certifications** d'audits de sécurité: ex., SAS70, ISO 27001

Mais aussi

- **Garanties** contractuelles

- **Polices d'assurance**

Définir les besoins en amont de la relation contractuelle Client/Prestataire du Cloud

Inventaire et analyse de ses besoins par l'entreprise utilisatrice

Analyse des offres disponibles

Points d'attention

Ne pas sous-estimer l'investissement en ressources et en temps nécessaire pour définir le cahier des charges et accompagner la transition

➔ le client peut se voir reprocher par le prestataire un manquement à son **obligation de collaboration**, facteur possible d'exonération de responsabilité pour le prestataire

Le client doit aussi pouvoir compter sur le prestataire lui-même pour éclairer son choix

➔ En droit français, ce dernier est en effet tenu d'une **obligation de conseil n**:

I

- fournir au client une information complète et objective sur la solution proposée
- évoquer les risques liés à cette solution
- préconiser la solution la mieux adaptée aux besoins du client

La sécurité dans le Cloud Computing

➢ La sécurité des systèmes d'information doit permettre de garantir :

- La **disponibilité** des données et systèmes
- **L'intégrité** et l'authenticité des données (ni perte, ni dégradation)
- La **confidentialité** (vis-à-vis des tiers non-autorisés)

Le prestataire doit mettre en œuvre les moyens techniques, juridiques et organisationnels permettant d'assurer le niveau de sécurité attendu par le client tout au long de la vie du contrat

➢ **Points d'attention :**

- Taux de disponibilité du service et temps de réponse
- Localisation des données (Gestion des flux transfrontaliers, conformité avec la loi Informatique & Libertés)
- Préservation des données, gestion des interfaces web et intrusions (Gestion des niveaux d'habilitation, gestion des mots de passe, …)
- Réversibilité (transférabilité) et Interopérabilité

Responsabilité et assurances

➢ Evaluer les niveaux relatifs à chacune des **obligations des parties** (moyens ou résultats) et qui permet une meilleure appréhension des clauses limitatives de responsabilité

➢ Prévoir le respect par le prestataire, son personnel et l'ensemble de ses sous-traitants d'une stricte confidentialité, et plus généralement, l'**extension aux sous-traitants** des obligations incombant au prestataire.

➢ Délimiter précisément les **dommages couverts** en cas d'atteinte à la sécurité des données (traditionnellement, sont couverts les dommages directs et prévisibles)

➢ Traiter la question des **dommages « indirects »** notamment par suite de l'affaire Sony-Playstation Network (gains manqués, perte de chiffre d'affaires, frais d'assurance complémentaire)

❖ Traiter aussi la question du **risque pénal** (ex. piratage, hacking…)

Chaine des contrats et cascade des responsabilités

Complexité = risques juridiques

Pluralité d'intervenants avec des engagements propres (SLAs) qui ne peuvent être nécessairement répercutés sur le client final, ou acceptés par ce dernier

La défaillance d'un « maillon » de cette chaine impacte toute l'offre

Par principe, le prestataire principal est en première ligne

Quelques Conseils :

Choisir des partenaires solides offrant de fortes garanties

Construire et documenter un « schéma » contractuel cohérent (contrats « miroirs ») en anticipant les scénarios « catastrophes »

Rechercher les bonnes polices d'assurance

Réversibilité / Interopérabilité:
Eviter la Dépendance (Vendor/Technology Lock-In)

➢ L'enjeu est la possibilité de changer de prestataire de service Cloud en transférant le service et les données

➢ Définition en amont des critères de sortie du contrat (durée, renouvellement, résiliation, coût …)

➢ Quelles obligations attacher à cette réversibilité ?

- Définition du domaine d'application

(Restitution des données à leur titulaire, transfert à un prestataire tiers,…)

- Définition d'un plan de réversibilité (si approprié)

(Assistance à la réversibilité, mise en place de comités spécifiques,…)

- Extension aux sous-traitants

➢ Cette réversibilité ou transférabilité soulève la question des formats des services concernés et de l'interopérabilité

C'est sans doute avec la sécurité l'un des domaines où pourraient intervenir des normes spécifiques au Cloud

- Open Cloud Manifesto: www.opencloudmanifesto.org
- Cloud Security Alliance: www.cloudsecurityalliance.org

Conclusion

- L’enjeu économique étant ce qu’il est le développement du Cloud va se poursuivre
- Une diversité dans les besoins selon la taille de l’entreprise, les types de données et les applications
- Une diversité dans l’approche et les offres des prestataires de Cloud
- Les choix des prestataires notamment en ce qui concerne la localisation des serveurs (au regard des questions de données personnelles) et les engagements contractuels peuvent être des éléments de différentiation importants
- Les travaux au sein de l’ADIJ se poursuivent

de Gaulle Fleurance & Associés
9, rue Boissy d'Anglas
75008 Paris

Tel. : +33 (1) 56 64 00 00
Fax : +33 (1) 56 64 00 01

www.dgfla.com

DE GAULLE
FLEURANCE
& ASSOCIÉS

SOCIÉTÉ D'AVOCATS