

Date : 22/09/10

Cloud computing : les freins contractuels et juridiques

Par Thierry Lévy-Abégnoli



Des problématiques à la fois juridiques et contractuelles entravent l'essor du cloud computing. Localisation des données, sécurité, réversibilité, auditableté ou qualité de services doivent être formalisées.

1. La localisation physique des données personnelles

"Les aspects juridiques sont l'une des raisons majeures pour lesquelles une entreprise renonce au cloud", constate Marc Boullier, responsable de l'offre cloud computing chez Solucom. Principale problématique : la réglementation sur la protection des données personnelles. "Selon la loi Informatique et Libertés, récemment mise à jour, le prestataire gérant des données à caractère personnel doit garantir leur confidentialité et leur sécurité", précise Murielle-Isabelle Cahen, avocate à la cour d'appel de Paris. Il en résulte une interdiction de transférer ces données vers des pays n'offrant pas un niveau de protection adéquat.



"Les États-Unis n'ont pas été reconnus par la Commission Européenne comme offrant ce niveau et les fournisseurs sont loin d'avoir intégré cette problématique", ajoute Murielle-Isabelle Cahen (photo). A minima, ceux-ci doivent préciser où sont situés les serveurs. S'ils sont en

Évaluation du site

Indexel s'intéresse à l'informatique professionnelle. Le site diffuse d'assez nombreuses brèves couvrant l'actualité des métiers, du matériel et des entreprises.

Cible
Professionnelle

Dynamisme* : 1
* pages nouvelles en moyenne sur une semaine

Europe, l'obligation déclarative est allégée. De fait, l'infrastructure de Microsoft Azure est située aux États-Unis et en Europe (à Dublin et Amsterdam). "Nous donnons le choix du lieu d'hébergement", commente Bernard Ourghanlian, directeur technique et sécurité chez Microsoft France. Il reste que seul le client est responsable de la déclaration à la CNIL. "Les données sont en effet celles de l'entreprise et de ses clients", précise **Olivia Flipo**, avocate en nouvelles technologies et consultante auprès de Syntec Informatique.

2. Des types de données très contraignants



Certaines données imposent des contraintes particulières. "Pour les données de santé, il faut un agrément national qui impose en pratique un stockage en France", affirme Olivia Flipo (photo). Cet agrément est toutefois partagé. "Le décret correspondant précise 74 exigences dont certaines concernent l'application métier donc notre client, alors que notre service est de type infrastructure, mais nous devons par exemple nous engager sur la durée de conservation", explique Dominique Vo, manager IT & sécurité, cloud computing chez Orange. De même, les factures électroniques sont soumises à un régime particulier. "Le pays d'accueil doit être lié à la France par une convention prévoyant une assistance mutuelle en matière de fiscalité", affirme Murielle-Isabelle Cahen.

3. Des contrats de service avec pénalités



Comme dans les offres d'infogérance, les clauses des contrats de services ciblent performances, disponibilité, garantie de restauration, confidentialité et sécurité. Mais leur respect est rendu plus difficile par la mutualisation, qui pose la question de l'étanchéité entre clients. "C'est un faux problème car la virtualisation gère bien cette problématique", assure Marc Boullier (photo). Orange affiche ainsi sa confiance dans la technologie VMware mais propose aussi de dédier dynamiquement des ressources physiques puisées dans un pool. Des pénalités sont prévues par certains prestataires. "Nous garantissons 99,95 % de disponibilité pour notre bus de services et 99,9 % pour les instances Azure. En cas de non-respect, nous réduisons de 10 % la facture du mois suivant, et même de 25 % si l'on descend sous 99 %", explique Bernard Ourghanlian.

4. Réversibilité : évaluer son coût et sa complexité

En vue d'un retour en arrière ou d'un changement de prestataire, l'entreprise doit prévoir une clause de réversibilité. "Il faut en chiffrer le coût et prévoir un système fonctionnant en parallèle,

le temps de convertir les données", explique **Olivia Flipo**. La complexité de la réversibilité doit être bien évaluée. "Par exemple, avec Google App, la récupération des e-mails ne pouvant s'effectuer que message par message, il faut réaliser un programme batch", prévient Marc Boullier. La question des formats se pose moins pour l'laaS que pour le Saas.



"Avec notre offre Flexible Computing, de type laaS et basé sur l'hyperviseur de VMware, Orange garantit simplement la restitution des données dans leur format d'origine, par exemple SQL ou Web. Quant aux VM, nous les restituons dans le format de VMware", explique ainsi Daniel Chiossi (photo), responsable marketing des services en lignes, division entreprises chez Orange.

5. Conformité réglementaire et auditabilité

L'offre de cloud doit garantir la conformité par rapport au droit. "Il y a obligation légale de ne pas entraver l'exercice de la justice, qui doit le cas échéant accéder à certaines données, ce qui peut être impossible si le service est hébergé hors de l'UE", explique Marc Boullier.



Cela revient à un problème d'auditabilité par un tiers. Certaines entreprises peuvent aussi exiger la possibilité de réaliser elles-mêmes un audit. "L'infrastructure d'Azure étant très partagée, nous essayons plutôt de nous mettre d'accord avec nos clients sur des auditeurs tiers et des normes comme ISO 27001, reconnus par les deux parties", répond Bernard Ourghanlian (photo).

6. Des contrats trop standardisés

On constate par rapport à tous ces aspects, un rapport de pouvoir entre client et fournisseur. "Face à Google ou Microsoft, seuls les très grands comptes peuvent obtenir un contrat spécifique. En attendant une certification européenne ou un label, il faut impérativement faire auditer le contrat par un cabinet d'avocats", conclut Marc Boullier.