

Internet : Un Cloud Computing sans risque ?

Internet

Posté par : JPilo

Publié le : 25/2/2013 13:30:00

Le Cloud Computing est un sujet relativement récent, encore en pleine mutation mais déjà largement répandu dans les pratiques informatiques des entreprises autant que des particuliers.

Lors d'une conférence organisée par le cabinet Courtois Lebel, **Arnaud Tessalonikos** et **Cédric Frénel**, avocats associés, entourés de la société de services informatiques Gosis et du cabinet de courtage en assurance Bréchard, ont exposé **les diverses facettes du «nuage»**.

D'après le National Institute of Standards and Technology (NIST), le Cloud Computing se définit comme « l'accès via le réseau, à la demande et en libre-service, à des ressources informatiques partagées configurables ».

Le mot « Cloud », qui signifie « nuage » en anglais, correspond à l'image généralement utilisée dans le monde informatique pour symboliser le réseau Internet. Il symbolise ainsi, notamment, une certaine opacité et une incertitude des services et des données qui y sont placés.

De nombreuses personnes utilisent le Cloud au quotidien sans le savoir (messagerie, stockage chez Amazon, suite bureautique Google Apps, etc.). Le Cloud peut être public et mutualisé, comme chez Google par exemple, ou dédié et privé, dans un environnement propre à l'entreprise, afin de maîtriser la politique de sécurité.

Quelle est la réalité opérationnelle ?



Lorsqu'une entreprise décide de passer d'un serveur en interne au Cloud, elle est quasi certaine

d'obtenir de meilleures performances (quelle que soit sa taille, même pour une PME), une bonne « agilité », puisqu'il s'utilise sans enfermer le client dans un espace propriétaire, et une réduction aussi bien de ses coûts de consommation - puisque l'on ne paie que ce que l'on consomme - que de ses coûts de sécurité.

L'utilisateur peut avoir accès à toutes ses données, même personnelles, en tous lieux, à tous moments, et ce, de façon totalement sécurisée. La sécurité est un travail quotidien pour les opérateurs car les hackers font évoluer leurs techniques d'intrusion tous les jours ! En fonction des services souscrits, les données qui sont dans le nuage peuvent être sécurisées comme dans un véritable coffre-fort.

Dans une entreprise, les postes et le serveur doivent être sécurisés ; avec le Cloud, sous réserve de choisir les services appropriés, ces problèmes peuvent être résolus. Les données peuvent être cryptées, puis compressées, puis morcelées afin d'être quasiment impossibles à capter. Afin de minimiser les risques de ruptures de service, les connexions doivent être assurées par au moins deux opérateurs différents au cas où il y aurait des coupures. En fonction du prestataire et du niveau de service choisi, des tests d'intrusion, de traçabilité et de stockage sont réalisés régulièrement.

Enfin, le dernier point important à prendre en compte pour faire le choix du Cloud est la clause de réversibilité qui doit être prévue dans le contrat afin de pouvoir récupérer les données en cas de réinternalisation ou de changement de prestataire.

Dans quel cadre juridique ?

Ce sujet, particulièrement innovant, est encore mal circonscrit au plan juridique. Le droit intervient à double titre. D'une part, il impose le respect des contraintes légales et réglementaires propres aux secteurs d'activité qui ont recours au Cloud. D'autre part, il constitue, au moyen de la voie contractuelle, un outil de gestion des risques à part entière.

L'une des difficultés de ce sujet est qu'il n'existe pas de définition légale ou réglementaire du Cloud Computing, et il n'y a pas de jurisprudence non plus à ce jour. Le seul référentiel juridique existant est un avis de la Commission générale de terminologie et de nomenclature (juin 2010).

Le recours au Cloud s'inscrit dans le respect des contraintes légales et réglementaires applicables, qu'elles soient sectorielles ou générales. Ces contraintes sont dites sectorielles lorsqu'elles sont inhérentes au secteur d'activité d'une entreprise (banque ou santé par exemple). Sinon, elles sont d'ordre général, c'est-à-dire applicables à différents secteurs d'activités. Les deux se cumulent donc. Or, malgré le recours au Cloud, il demeure impératif de respecter le cadre juridique existant. Ne pas le respecter engagerait la responsabilité civile ou pénale de l'entreprise et de ses dirigeants, d'où l'intérêt d'être en conformité et de mettre en place le bon encadrement contractuel. S'agissant des traitements informatiques réalisés dans le Cloud, la question de savoir qui est le responsable n'est pas simple à résoudre. Parfois la CNIL (Commission Nationale de l'Informatique et des Libertés) considère que le prestataire et le client peuvent être co-responsables du traitement des données. Cette situation incertaine est encore complexifiée par les nombreux cas de transferts de données depuis l'Europe dans des pays de protection non équivalente.

Parmi les contraintes légales et réglementaires, notons également l'obligation de notification des failles de sécurité, aujourd'hui par les seuls prestataires de services de communications électroniques et demain par toutes les entreprises. Dans le cas où cette obligation ne serait pas remplie, la peine peut atteindre cinq ans de prison ou 300 000 euros d'amende.

Afin de faire les bons choix au regard de la réglementation applicable, la CNIL

recommande, dans chaque cas, de passer par sept étapes :

1. Cartographier les données et les traitements
2. Définir les exigences de sécurité technique et juridique
3. Faire une analyse des risques
4. Choisir des modèles de service et de déploiement pertinents
5. Choisir un prestataire présentant des garanties suffisantes
6. Réviser la politique de sécurité interne
7. Surveiller les évolutions

Ce sont des choix importants à faire par l'entreprise, son dirigeant et ses conseils. Plusieurs nouveaux métiers se sont créés et développés récemment autour du Cloud tels que les Cloud brokers qui sélectionnent les meilleurs services dans ce domaine ou encore les Cloud auditors (attention : il faut prévoir le statut de l'auditeur !). Au plan juridique, il est préférable que le client n'ait qu'un seul interlocuteur qui est à la fois revendeur et intégrateur de Cloud afin de simplifier les discussions en cas de litige, d'où le nécessaire encadrement contractuel qui impose de choisir, au cas par cas, la bonne architecture contractuelle entre opérateur(s), éditeurs, hébergeurs, le client et ses auditeurs externes. Il est également recommandé de mettre en place un SLA adapté (Service Level Agreement - en fait formalisation d'un accord négocié entre deux parties sur les niveaux de qualité de services), et d'établir des matrices de responsabilité.

Pour Arnaud Tessalonikos et Cédric Frenel : « Le plus important est la rigueur de la méthode. Le dirigeant doit faire une analyse des risques, identifier ses contraintes, choisir le bon prestataire et surtout se mettre en conformité avec la réglementation applicable et négocier le contrat adapté aux enjeux de son entreprise. »

Faut-il prendre une cyber assurance ?

Il est difficile d'obtenir des chiffres en France, car les sinistres ne sont en général pas déclarés, comme une sorte de déni. Néanmoins on peut en citer deux :

- le coût moyen d'une donnée perdue ou volée en 2012 est de 122 euros, chiffre en constante augmentation
- 43 % des violations de données sont faites par les hackers et 31 % par négligence.
- La question majeure reste la prise de conscience. Avec les nouvelles technologies d'Internet, les entreprises sont confrontées à de nouveaux risques : risques de responsabilité, risques d'atteinte à l'image ou risques d'extorsion. Pour les traiter, il faut appliquer les mêmes méthodes que pour les risques traditionnels : analyse, prise de conscience, plan de travail, transfert vers un assureur.

Il est donc essentiel, pour les entreprises, de se protéger. Or, en France, les assureurs traditionnels, à quelques exceptions près, ne sont pas encore sur ce marché. Les spécialistes sont des Anglo-saxons qui ont un retour d'expérience sur environ dix ans et qui commencent à s'intéresser au marché français. Les garanties proposées sont : un volet RC, vie privée, données personnelles, perte de revenu, atteinte à la réputation, etc. Avant de choisir un assureur, il faut réaliser un audit, faire intervenir un conseil pour vérifier que l'on est en règle,

et si possible faire appel à un CIL (Correspondant Informatique et Libertés).

Dans le cadre d'une cyber assurance, la responsabilité de l'assuré est engagée, non pas après une prestation, mais suite à l'utilisation par des tiers de données dont il avait la charge ou la garde. L'assurance couvre l'entreprise pour les conséquences financières qu'elle encourt du fait des dommages causés aux tiers mais également à elle-même. Il est donc essentiel pour l'entreprise de se protéger.