Le point sur...

NUMÉRIQUE ET NOUVELLES TECHNIQUES

Cloud computing : dans le nuage, comment éviter la tempête ?

Par Benjamin Jacob, avocat associé.
PDGB

Extrait du magazine
Décideurs N°123
janvier 2011

NUMÉRIQUE ET NOUVELLES TECHNIQUES

Cloud computing : dans le nuage, comment éviter la tempête ?

Le « cloud computing », ou « informatique dans les nuages », offre des perspectives particulièrement intéressantes pour les entreprises utilisatrices d'importantes ressources informatiques. Le contrat de prestation de services de « cloud computing » mérite une attention toute particulière, compte tenu des risques liés à la dispersion des données en dehors de l'entreprise, inhérente à ce service innovant.

Benjamin Jacob, avocat associé

SUR L'AUTEUR

Benjamin Jacob, avocat au barreau de Paris, est associé au sein du cabinet PDGB, dont il anime le département IP-IT. Titulaire d'un DESS de droit du numérique et des nouvelles techniques, Il intervient régulièrement dans le cadre de la négociation de contrats informatiques portant sur des projets informatiques critiques pour les grandes et moyennes entreprises.

Le « cloud computing » (nous parlerons du « cloud »), désigne un service informatique permettant aux entreprises d'externaliser en totalité ou en partie leur infrastructure informatique.
Le cloud n'est pas une révolution, il est l'évolution logique des services d'outsourcing informatique que nombre d'entreprises utilisent de longue date (« facilities management ») ou depuis peu (« ASP », « SaaS »).

Le graal de l'externalisation informatique

Pour autant, le cloud se distingue de ses prédécesseurs par une caractéristique notable : il repose en principe sur l'utilisation de diverses ressources matérielles (tels que CPU ou serveurs) non nécessairement réunies en un seul et même lieu physique. La démultiplication de ces ressources et leur répartition en plusieurs lieux géographiques sont censées constituer l'atout du cloud, dès lors qu'il peut permettre aux entreprises utilisatrices d'atteindre le graal de l'externalisation informatique : un taux de disponibilité proche de 100 %. Reste qu'en l'absence de réglementation internationale, la dispersion géographique des données n'est pas sans risques. Les avantages du cloud doivent donc être contrebalancés par les risques qui lui sont inhérents.
La rédaction du contrat de cloud a donc une importance capitale. Bien évidemment, chacune des clauses du contrat de cloud - comme pour tout contrat - a son importance. Cependant, les conditions de sécurisation et les modalités de restitution des données nécessitent une attention particulière.
Les services de cloud impliquent le plus souvent un transfert des données de l'entreprise vers les serveurs de son prestataire de cloud (ou de ses sous-traitants). De ce fait, l'entreprise encourt un certain nombre de risques liés à la dépossession de ses données, laquelle implique un traitement au sens de la loi informatique et libertés[1].
La question de la responsabilité du traitement des données à caractère personnel émanant du client doit être posée, étant précisé que la loi du 6 janvier 1978 s'applique aux traitements de données personnelles dont le responsable est établi sur le territoire français (y compris dans le cadre d'une installation, quelle qu'en soit la forme juridique), ou dont le responsable recourt à des moyens de traitement situés sur le territoire français (à l'exclusion des traitements ayant pour seul objet le transit des données)[2].
Le responsable du traitement étant la personne, l'autorité publique, le service ou l'organisme en déterminant ses finalités et ses moyens[3], il s'agira, dans le cadre du service de cloud, du bénéficiaire de ce service. Au sens de la loi informatique et libertés, le prestataire de services de cloud est pour sa part le sous-traitant de son client.
De ce fait, le client demeure tenu de respecter les obligations légales mises à la charge de tout responsable de traitement (sécurité des données, information des personnes concernées, respect du droit d'accès, de rectification et d'opposition). Le bon sens exige donc de s'assurer contractuellement que le prestataire apporte des garanties suffisantes pour assurer la sécurité des données. Au demeurant, la loi l'exige expressément[4].

Ce d'autant plus que le cloud implique une dispersion des données sur plusieurs serveurs, potentiellement opérés par des tiers et répartis sur différentes zones géographiques. Cette dispersion géographique pourra être source de complications pour le client si les données sont amenées à être transférées vers des serveurs situés en dehors de l'Union européenne. En effet, s'agissant de tels transferts, la loi impose d'obtenir une autorisation de la Cnil

LES POINTS CLÉS

Quelques points-clés à surveiller dans le contrat de cloud :

- Le niveau de protection assuré aux données et les garanties associées ;
- La situation géographique des serveurs utilisés pour fournir la prestation ;
- L'intuitu personae et les conditions de recours à la sous-traitance ;
- Les niveaux de services fournis et les éventuelles pénalités applicables ;
- Les modalités de restitution des données en fin de contrat ;
- Le droit applicable au contrat et les tribunaux compétents, d'autant plus que la prestation peut être exécutée sur divers territoires.

(conditionnée par le degré de protection assuré aux données, principalement par voie contractuelle[5]), ou de recueillir l'autorisation de la personne concernée[6].

Ceci doit donc inviter le client du service de cloud à solliciter de son prestataire qu'il précise, dans le contrat, les territoires sur lesquels sont situés ses serveurs, voire de prévoir que les serveurs utilisés pour rendre le service de cloud soient systématiquement situés sur le territoire de l'Union européenne.

Les données de l'entreprise ne doivent naturellement pas être confiées à n'importe qui. Ce qui relève de l'évidence l'est un peu moins en matière de « cloud computing ». Le bénéficiaire du service aura donc intérêt à s'assurer que le contrat de cloud comporte une clause d'intuitu personae, à encadrer autant que possible les conséquences de la disparition de son cocontractant, voire à prévoir l'identification de ses sous-traitants. En outre, le client gagnera à bénéficier d'une clause d'audit.

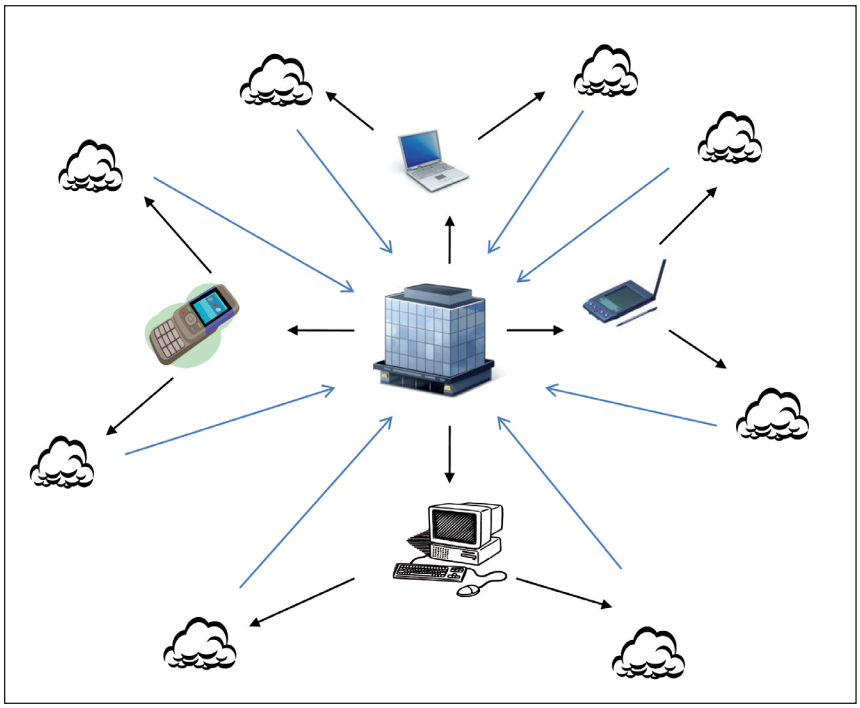
Précaution indispensable : prévoir la fin du contrat

La fin d'un contrat d'externalisation est souvent vécue comme une situation de crise pour le bénéficiaire. Un bon contrat d'outsourcing devrait toujours prévoir une clause encadrant le « backsourcing » ou la réversibilité, voire a minima la restitution des données dans un format courant, au plus tard au jour de prise d'effet de la résiliation. Le contrat de cloud ne devrait pas y faire exception.

La réversibilité est une notion protéiforme : il pourra s'agir tour à tour d'une simple restitution de données, d'un transfert de connaissances et/ou contrats, voire du transfert de propriété de certaines infrastructures informatiques physiques. Il convient donc de bien définir contractuellement l'étendue de la réversibilité et ce qu'elle recouvre. Outre les objectifs de la réversibilité, les parties gagneront à prévoir précisément ses modalités pratiques. Il est en effet courant que les parties à un contrat d'outsourcing éprouvent quelques difficultés à communiquer lorsque le contrat a été résilié ou n'est pas renouvelé. Pour pallier les conséquences d'une communication altérée, il peut être utile d'annexer au contrat un plan de réversibilité, plutôt que de prévoir une rédaction ultérieure.

Enfin, tout bon contrat se doit de prévoir la loi à laquelle il est soumis, ainsi que les tribunaux compétents en cas de litige. En matière de cloud, cette clause revêt évidemment une importance majeure, dès lors que le contrat de cloud est susceptible d'être exécuté sur une myriade de territoires.

L'informatique dans les nuages peut séduire, mais pour ne pas assombrir le tableau ou sombrer dans la tempête, son utilisateur doit bien identifier les risques qui en résultent et s'assurer que le contrat les traite efficacement.



[1] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*
[2] *Article 5 de la loi n° 78-17 du 6 janvier 1978*
[3] *Article 3 de la loi n° 78-17 du 6 janvier 1978*
[4] *Article 35 de la loi n° 78-17 du 6 janvier 1978*
[5] *A noter que la Commission européenne a adopté de nouvelles clauses types le 5 février 2010 (décision 2010-1987/UE)*
[6] *Articles 68 et 69 de la loi n° 78-17 du 6 janvier 1978*