Image not found or type unknown

Le Cloud Computing est en vogue

publié le **05/05/2010**, vu **6516 fois**, Auteur : Murielle Cahen

Le monde est fait de révolutions industrielles. 1990 : le PC Windows, 2000 : Internet dans les entreprises, et … 2010 : le Cloud Computing !

Déjà lancés par un certain nombre de sociétés dont Amazon et Google, et même Microsoft avec sa plateforme cloud Azure qui répond déjà aux attentes des développeurs, les services de cloud computing, qui signifie « Informatique dans les nuages », pourraient bien révolutionner l'informatique des entreprises. Ce concept permet désormais d'externaliser l'utilisation de la mémoire ainsi que les capacités de calcul d\'ordinateurs et de serveurs répartis dans le monde entier. Il offre en effet aux entreprises une formidable puissance informatique s'adaptant de surcroît à la demande.

Cette technique diffère des contrats classiques d\'outsourcing aux termes desquels un prestataire tiers sera en charge du traitement technique des données. Le droit français et la majorité des lois nationales relatives à la protection des données personnelles au sens de la directive n° 95/46/CE du 24 octobre 1995, considèrent en principe ce prestataire tiers comme un sous-traitant des données agissant conformément aux instructions d\'un responsable du traitement.
Enfin, le cloud permet à l'entreprise de s'affranchir des contraintes traditionnelles, et d'avoir une approche modulaire en fonction des besoins. Sur le plan juridique, on se rapproche du cas dans lequel une entreprise déciderait d'externaliser tout ou partie de son système d'information. Une démarche prudente consiste à bien appréhender les risques et à prendre les mesures nécessaires.
Il conviendra donc d'exposer ce qu'est le concept de cloud computing (1), pour ensuite définir et se prémunir des risques juridiques liés à son utilisation (2).
Qu'est-ce que le cloud computing ?
Il faut définir le cloud computing (A), ainsi que ses avantages (B).
A. La définition du cloud computing
Le cloud computing est un concept récent permettant d'utiliser de la mémoire et des capacités de calcul d'ordinateurs et de serveurs répartis dans le monde entier et liés par un réseau tel Internet.
Le cloud computing permet ainsi de disposer, à la demande, de capacités de stockage et de puissance informatique sans disposer matériellement de l'infrastructure correspondante. L'accès aux données et aux applications peut ainsi se faire à partir de n'importe quel périphérique connecté, le plus souvent au moyen d\'un simple navigateur Internet.
Plus précisément, il existe des cloud computing publics qui constituent des services partagés auxquels toute personne peut accéder à l'aide d'une connexion Internet, sur une base d\'utilisation sans abonnement. Il y a aussi des clouds privés dont l'accès pouvant être limité à une seule entreprise ou à une partie de celle-ci. Ces derniers peuvent ainsi apparaître comme plus sûrs en termes de sécurité des données.
Le cloud computing constitue donc globalement une nouvelle forme d'informatique à la demande, à géométrie variable, que l'on pourrait classer d'un point de vue juridique, au croisement des services d'externalisation, et des services ASP et SaaS.
B. Les apports du cloud computing
Le cloud computing permet ainsi, sans investissement majeur en termes d'infrastructure et de dépenses en capitaux, de bénéficier d'un service à moindre coût fondé sur la consommation, de

type \"pay-per-use\", et par suite d’optimiser la gestion des coûts d’une entreprise.
Techniquement, il est possible de mettre n’importe quelle application dans un cloud computing. Néanmoins, ses usages principaux concerneront essentiellement le management lié aux nouvelles technologies, la collaboration, les applications personnelles ou d’entreprise, le développement ou le déploiement des applications et enfin les capacités serveurs et de stockage.
Le cloud computing constitue donc un service qu’il conviendra d\'encadrer spécifiquement sur un plan juridique.

Les risques juridiques liés à l\'utilisation du cloud computing

Les principaux risques juridiques du cloud computing concernent les données (A). Il convient de s’en prémunir dans des contrats sécurisés (B).

A. La sécurité et la sécurisation des données

L’accès aux données et aux applications est réalisé entre le client et la multiplicité des serveurs distants. Leur mutualisation et la délocalisation de ceux-ci multiplie donc les risques. L\'accès aux services induira donc des connexions sécurisées et une authentification des utilisateurs, induisant alors le problème de la gestion des identifiants et celui des responsabilités (accès non autorisé, perte ou vol d\'identifiants, etc.).
Pour les mêmes raisons, il existe également un risque de perte de données qu’il conviendra de prendre en considération, d’évaluer et d’anticiper dans le cadre de procédures de sauvegarde adaptées (stockage dans des espaces privés, en local, en environnement public, etc.). De même, il existe également des risques au regard de la confidentialité des données (fuites), vu le nombre de serveurs et la délocalisation de ceux-ci.
De plus, il existe des risques financiers liés aux outils de contrôle servant à évaluer la consommation du cloud computing, et sa facturation. Il conviendra ainsi de définir contractuellement une unité de mesure du stockage, et des ressources informatiques utilisées.
Enfin, la mise en place de services de cloud computing fait naître pour l’entreprise un certain nombre de risques au regard des données personnelles et des formalités imposées par la CNIL. Ces risques sont aggravés en cas de transfert de données hors de l’Union Européenne (UE). La rédaction de contrats de cloud computing devra donc également prendre en considération ces problématiques.Haut du formulaire

B. Les précautions juridiques nécessaires à la rédaction d’un contrat de cloud computing

Pour pallier les risques précédemment évoqués, il conviendra de conclure une convention de niveau de service, ou « SLA » (pour « Service Level Agreement ») qui pourra comporter des indications quant aux attentes du client, au sujet de la réalisation des obligations du prestataire (malus ou pénalités).
Par ailleurs, pour assurer une pérennité des services de cloud computing, il s\'avère primordial de contractualiser un plan de réversibilité permettant d’assurer le transfert des services à d’autres prestataires. Il faudra donc prévoir les facteurs déclencheurs de cette réversibilité (carence du prestataire, libre choix du client après un certain nombre d’années), et ses conditions, ainsi que son coût.
En cas de perte de données, il sera préconisé de prévoir la réplication de celles-ci sur plusieurs sites ou l’obligation de résultat de restauration des données dans des délais contractuels définis.
Par ailleurs, le contrat prendra soin de préciser que l\'ensemble des traitements ne seront opérés par l\'hébergeur que sur instructions et contrôle des utilisateurs, c\'est-à-dire sans prise d\'initiative sans instructions expresses des utilisateurs considérés comme responsables de traitements.
Enfin, pour ce qui est de l\'intégrité et de la confidentialité des données, il pourra être prévu une clause d’audits externes, ainsi qu’une clause de responsabilité dont il faudra s’assurer de la rigueur, pour encadrer tout particulièrement la traçabilité, l’accès frauduleux, l\'atteinte à l\'intégrité, voire la perte de données sensibles.

En ce qui concerne plus particulièrement les données personnelles, le client pourra exiger que celles-ci restent localisées sur des serveurs exclusivement situés dans l'UE. Le client s'exonérera ainsi d'un ensemble de formalités CNIL liées au transfert de données personnelles en dehors de l'UE.
Le cloud computing reste complexe. C'est pourquoi un cadre contractuel adapté est nécessaire pour prévenir les risques liés à ce service, qui, d'ici 2020, permettra aux entreprises de faire migrer l'essentiel de leurs applications dans les « nuages ».Bas du formulaire

Déjà lancés par un certain nombre de sociétés dont Amazon et Google, et même Microsoft avec sa plateforme cloud Azure qui répond déjà aux attentes des développeurs, les services de cloud computing, qui signifie « Informatique dans les nuages », pourraient bien révolutionner l'informatique des entreprises. Ce concept permet désormais d'externaliser l'utilisation de la mémoire ainsi que les capacités de calcul d\'ordinateurs et de serveurs répartis dans le monde entier. Il offre en effet aux entreprises une formidable puissance informatique s'adaptant de surcroît à la demande.

Cette technique diffère des contrats classiques d\'outsourcing aux termes desquels un prestataire tiers sera en charge du traitement technique des données. Le droit français et la majorité des lois nationales relatives à la protection des données personnelles au sens de la directive n° 95/46/CE du 24 octobre 1995, considèrent en principe ce prestataire tiers comme un sous-traitant des données agissant conformément aux instructions d\'un responsable du traitement.

Enfin, le cloud permet à l'entreprise de s'affranchir des contraintes traditionnelles, et d'avoir une approche modulaire en fonction des besoins. Sur le plan juridique, on se rapproche du cas dans lequel une entreprise déciderait d'externaliser tout ou partie de son système d'information. Une démarche prudente consiste à bien appréhender les risques et à prendre les mesures nécessaires.

Il conviendra donc d'exposer ce qu'est le concept de cloud computing (1), pour ensuite définir et se prémunir des risques juridiques liés à son utilisation (2).

Qu'est-ce que le cloud computing ?

Il faut définir le cloud computing (A), ainsi que ses avantages (B).

A. La définition du cloud computing

Le cloud computing est un concept récent permettant d'utiliser de la mémoire et des capacités de calcul d'ordinateurs et de serveurs répartis dans le monde entier et liés par un réseau tel Internet. Le cloud computing permet ainsi de disposer, à la demande, de capacités de stockage et de puissance informatique sans disposer matériellement de l'infrastructure correspondante. L'accès aux données et aux applications peut ainsi se faire à partir de n'importe quel périphérique connecté, le plus souvent au moyen d\'un simple navigateur Internet.

Plus précisément, il existe des cloud computing publics qui constituent des services partagés auxquels toute personne peut accéder à l'aide d'une connexion Internet, sur une base d\'utilisation sans abonnement. Il y a aussi des clouds privés dont l'accès pouvant être limité à une seule entreprise ou à une partie de celle-ci. Ces derniers peuvent ainsi apparaître comme plus sûrs en termes de sécurité des données.

Le cloud computing constitue donc globalement une nouvelle forme d’informatique à la demande,à géométrie variable, que l’on pourrait classer d’un point de vue juridique, au croisement des services d’externalisation, et des services ASP et SaaS.

B. Les apports du cloud computing

Le cloud computing permet ainsi, sans investissement majeur en termes d’infrastructure et de dépenses en capitaux, de bénéficier d’un service à moindre coût fondé sur la consommation, de type \"pay-per-use\", et par suite d’optimiser la gestion des coûts d’une entreprise.

Techniquement, il est possible de mettre n’importe quelle application dans un cloud computing. Néanmoins, ses usages principaux concerneront essentiellement le management lié aux nouvelles technologies, la collaboration, les applications personnelles ou d’entreprise, le développement ou le déploiement des applications et enfin les capacités serveurs et de stockage.

Le cloud computing constitue donc un service qu’il conviendra d\'encadrer spécifiquement sur un plan juridique.

Les risques juridiques liés à l\'utilisation du cloud computing

Les principaux risques juridiques du cloud computing concernent les données (A). Il convient de s’en prémunir dans des contrats sécurisés (B).

A. La sécurité et la sécurisation des données

L’accès aux données et aux applications est réalisé entre le client et la multiplicité des serveurs distants. Leur mutualisation et la délocalisation de ceux-ci multiplie donc les risques. L\'accès aux services induira donc des connexions sécurisées et une authentification des utilisateurs, induisant alors le problème de la gestion des identifiants et celui des responsabilités (accès non autorisé, perte ou vol d\'identifiants, etc.).

Pour les mêmes raisons, il existe également un risque de perte de données qu’il conviendra de prendre en considération, d’évaluer et d’anticiper dans le cadre de procédures de sauvegarde adaptées (stockage dans des espaces privés, en local, en environnement public, etc.). De même, il existe également des risques au regard de la confidentialité des données (fuites), vu le nombre de serveurs et la délocalisation de ceux-ci.

De plus, il existe des risques financiers liés aux outils de contrôle servant à évaluer la consommation du cloud computing, et sa facturation. Il conviendra ainsi de définir contractuellement une unité de mesure du stockage, et des ressources informatiques utilisées.

Enfin, la mise en place de services de cloud computing fait naître pour l’entreprise un certain nombre de risques au regard des données personnelles et des formalités imposées par la CNIL. Ces risques sont aggravés en cas de transfert de données hors de l’Union Européenne (UE). La rédaction de contrats de cloud computing devra donc également prendre en considération ces problématiques.Haut du formulaire

B. Les précautions juridiques nécessaires à la rédaction d’un contrat de cloud computing

Pour pallier les risques précédemment évoqués, il conviendra de conclure une convention de

niveau de service, ou « SLA » (pour « Service Level Agreement ») qui pourra comporter des indications quant aux attentes du client, au sujet de la réalisation des obligations du prestataire (malus ou pénalités).

Par ailleurs, pour assurer une pérennité des services de cloud computing, il s\'avère primordial de contractualiser un plan de réversibilité permettant d’assurer le transfert des services à d’autres prestataires. Il faudra donc prévoir les facteurs déclencheurs de cette réversibilité (carence du prestataire, libre choix du client après un certain nombre d’années), et ses conditions, ainsi que son coût.

En cas de perte de données, il sera préconisé de prévoir la réplication de celles-ci sur plusieurs sites ou l’obligation de résultat de restauration des données dans des délais contractuels définis.

Par ailleurs, le contrat prendra soin de préciser que l\'ensemble des traitements ne seront opérés par l\'hébergeur que sur instructions et contrôle des utilisateurs, c\'est-à-dire sans prise d\'initiative sans instructions expresses des utilisateurs considérés comme responsables de traitements.

Enfin, pour ce qui est de l\'intégrité et de la confidentialité des données, il pourra être prévu une clause d’audits externes, ainsi qu’une clause de responsabilité dont il faudra s’assurer de la rigueur, pour encadrer tout particulièrement la traçabilité, l’accès frauduleux, l\'atteinte à l\'intégrité, voire la perte de données sensibles.

En ce qui concerne plus particulièrement les données personnelles, le client pourra exiger que celles-ci restent localisées sur des serveurs exclusivement situés dans l’UE. Le client s’exonérera ainsi d’un ensemble de formalités CNIL liées au transfert de données personnelles en dehors de l’UE.

Le cloud computing reste complexe. C’est pourquoi un cadre contractuel adapté est nécessaire pour prévenir les risques liés à ce service, qui, d’ici 2020, permettra aux entreprises de faire migrer l’essentiel de leurs applications dans les « nuages ».Bas du formulaire