Aspects juridiques du cloud computing

Le Cloud computing (« Informatique en nuage »), actuellement en plein développement, présente de nombreux avantages, en termes de coût et de souplesse. Mais il engendre de nouveaux risques tant du côté du prestataire que de celui de l'utilisateur.

par **Jean-Philippe Leclère et Josquin Louvier**

Qu'est ce que le Cloud computing ?

Il s'agit d'un nouveau modèle de fourniture de services informatiques qui permet de stocker des données et d'utiliser des logiciels sur des serveurs distants localisés dans le monde entier et accessibles par Internet. L'utilisateur n'a plus besoin d'investir dans l'acquisition d'une infrastructure informatique ou de licence de logiciels. Mais il va pouvoir accéder à distance à des services informatiques utilisables à la demande et qui lui seront facturés en fonction de sa consommation. Il existe sur le marché différentes offres de service Cloud computing : l'hébergement d'infrastructures de calcul et de stockage (IaaS - Infrastructure as a Service), la fourniture de plateformes de développement d'applications en ligne (PaaS - Platform as a Service), la fourniture d'applications logicielles en ligne (Software as a Service). Le Cloud computing est qualifié de « public » quand le service est partagé et mutualisé entre de nombreux clients, de « privé » lorsqu'il est dédié à un seul client et d'« hybride » quand un service est partiellement dans un Cloud public et partiellement dans un Cloud privé.

Les avantages du Cloud computing

Le Cloud computing, permet de fournir à l'utilisateur un service a priori équivalent à moindre coût. En effet, les prestataires de Cloud offrant les mêmes services standardisés à de très nombreux utilisateurs peuvent amortir les coûts et proposer des tarifs intéressants. Pour sa part, l'utilisateur qui sera facturé à la demande ou à la consommation sous forme d'abonnement disposera d'une très grande souplesse pour interrompre le service si elle n'en a plus besoin ou si elle souhaite recourir aux services d'un concurrent. Par ailleurs, le client pourra disposer en temps réel des évolutions de la plateforme par Internet sans avoir à installer sur ses propres serveurs des mises à jour ou des nouvelles versions de logiciel. Enfin, le service Cloud se caractérise par une très grande simplicité et rapidité dans la mise en œuvre.

Les risques juridiques relatifs aux données hébergées

Les principaux risques engendrés par le Cloud computing concernent d'une part la sécurité des données et plus particulièrement des données à caractère personnel, et d'autre part, la qualité et la continuité de service.

Les données étant externalisées et hébergées sur de multiples serveurs localisés, qui plus est dans le monde entier, les risques qu'elles soient perdues, modifiées ou rendues accessibles à des tiers non autorisés sont nettement amplifiés. Il convient donc de mettre en place un système de connexions sécurisées et d'authentification efficace des utilisateurs. Avant de sélectionner une offre de services Cloud, l'utilisateur devra vérifier ce que le prestataire a mis en œuvre et s'engagera à maintenir toutes les mesures de sécurité physique sur le site de l'hébergement (sécurité des accès…), de sécurité logique (chiffrement, connexion VPN, authentification, sauvegarde, réplication multi-site, etc.), nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des données. En outre, il est important d'exiger du prestataire qu'il organise une traçabilité des flux de données en nuage, c'est-à-dire des traitements effectués par les personnels du client et du prestataire. Il sera utile de prévoir la possibilité d'effectuer des audits externes. Enfin, il est essentiel pour le client d'avoir en permanence des informations précises sur la localisation géographique des serveurs, tout particulièrement lorsque ceux-

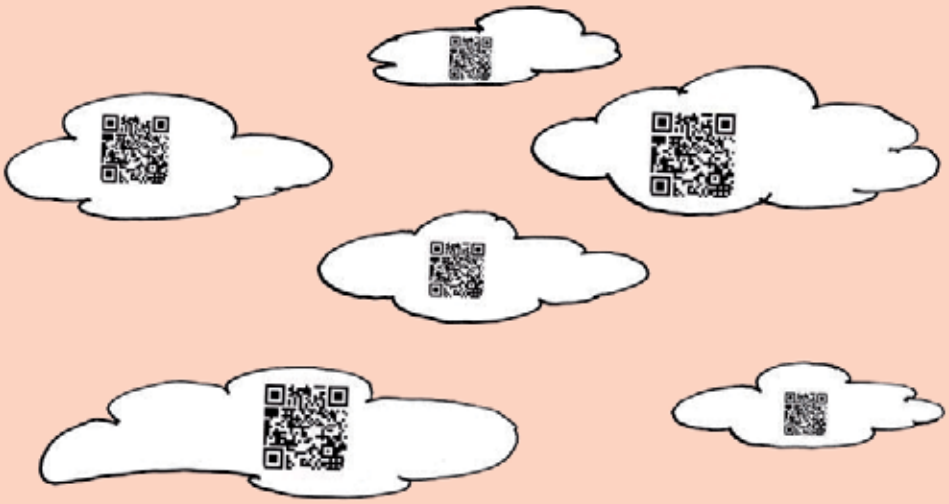
ci hébergent des données à caractère personnel.

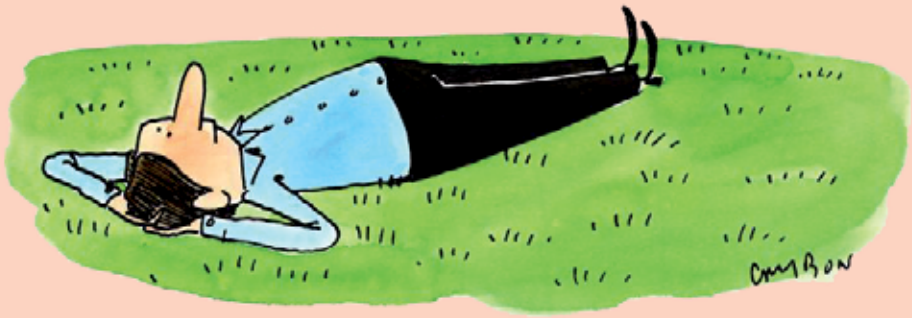
La protection des données à caractère personnel

En tant que responsable du traitement au sens de la loi Informatique et Libertés, le client est tenu de se conformer aux dispositions prévues par ladite loi, notamment en matière de formalités à accomplir auprès de la CNIL, ainsi que pour l'information des personnes.
Le prestataire Cloud, en tant que sous-traitant, sera tenu pour sa part, à des obligations renforcées en matière de sécurité des données. Par ailleurs, la localisation géographique de l'hébergement a une incidence directe sur le périmètre des obligations du prestataire et du client au regard des dispositions de la loi Informatique et Libertés. En effet, tout hébergement au sein des pays membres de l'Espace économique européen (EEE) ou dans des pays tiers reconnus comme assurant un niveau de protection adéquat par décision de la Commission européenne ne nécessitera qu'une simple déclaration à la CNIL. En revanche, pour tout transfert de données à caractère personnel vers des pays hors de l'EEE, l'autorisation de la CNIL sera requise ainsi que la signature de clauses contractuelles types ou l'adhésion à des règles contraignantes d'entreprise (BCR). Il est donc fondamental d'exiger de la part du prestataire Cloud une indication claire et exhaustive des pays hébergeant les centres de données Cloud.

La qualité et la continuité de service

Les services étant externalisés, l'utilisateur se retrouve confronté aux risques de pérennité du prestataire et de non qualité du service rendu. Pour pallier ces risques, il conviendra de mettre en place une convention de niveau de service (SLA- Service Level Agreement), qui intégrera des critères objectifs de performance (disponibilité, continuité, puissance, bande passante), dont le non-respect pourra entraîner l'application de pénalités. Par ailleurs, pour assurer la pérennité des services Cloud, le client aura tout intérêt à contractualiser un plan de réversibilité qui définira les modalités de récupération de ses données en termes de délais et de coûts, en vue d'un rapatriement en interne ou de l'exportation vers un nouveau prestataire Cloud. Enfin, le principe de paiement à l'usage inhérent aux services Cloud impose que soit prévue la mise en place d'outils de mesure d'utilisation des services du prestataire (unité de mesure du stockage, de la bande passante, du nombre d'utilisateurs actifs…) permettant à l'utilisateur de contrôler les coûts qui lui sont facturés par le prestataire.





Des recommandations

La plupart des risques évoqués peuvent être réduits par des dispositions contractuelles et par des mesures techniques et organisationnelles, tant au niveau du client que du prestataire. Certes, on constate la standardisation des offres faites par les principaux opérateurs du Cloud, tels qu'Amazon ou Google, ce qui réduit considérablement les marges de négociation des conditions contractuelles. Dans ce cas, le client devra analyser de manière détaillée les conditions proposées et les comparer avant de sélectionner son prestataire. Ceci présuppose que l'utilisateur aura fait préalablement une analyse des risques lui permettant de définir ses propres exigences. Il pourra être recommandé de procéder par étapes et de ne recourir au Cloud computing, dans un premier temps, que pour le traitement des données les moins sensibles. ■