LA CONFIDENTIALITÉ DES DONNÉES

M. Ludovic HAYE

La confidentialité des données dans le cloud : utopie ou réalité ?

La réalité est que la confidentialité reste le 1er frein à l'adoption

Plus généralement: le manque de sécurité est de loin l'objection que l'on entend le plus souvent dans la bataille que se livrent opposants et défenseurs du cloud computing.

(*véritable crainte ou excuse pour ne pas y aller ?)*

Le cloud « 100% secure »
reste en effet une utopie…

Paradigme du Cloud

« Comment tirer profit des avantages du Cloud tout en conservant mes données commerciales de façon sûre et confidentielle ? »

2 solutions :

- l'architecture de l'application est hébergée en Pure Cloud.
- Soit en Hybrid Cloud ce qui signifie que l'utilisateur peut conserver les données ayant le plus de valeur (Clients, Contrats, Données financières, etc.) sur son réseau et utiliser du Cloud uniquement des données non marquées, anonymes.

Support de stockage	Sécurité	Accès	Coût	Remarque d'utilisation
 Ordinateur professionnel	★★☆☆ Sujet au piratage informatique, aux détériorations et pannes	★☆☆☆ Pas adapté au partage, nécessite l'utilisation d'un support externe ou d'Internet (mail, cloud…)	★★★★ Pas de coût supplémentaire ou coût peu important	- Pour un stockage temporaire - Nécessité de crypter les données confidentielles et sensibles
 Support externe	★☆☆☆ - Sujet au vol, à la perte du support - Durée de vie limitée (dégradation du matériel)	★★★☆ Facilement transportable, il permet de transférer les données vers un autre ordinateur	★★★★ Pas de coût supplémentaire ou coût peu important	- Pour un stockage temporaire - Nécessité de crypter ou de sécuriser physiquement les données confidentielles et sensibles
 Serveur institutionnel	★★★★ Stockage fiable, durable et sécurisé (contre le vol, le piratage, les incendies…)	★★☆☆ La connexion au serveur institutionnel ne facilite pas le travail avec des personnes extérieures	★★☆☆ Coût assez important mais pas forcément répercuté sur l'usager	- Pour un stockage plus pérenne - Adapté pour le stockage de données sensibles et des versions « stables » de vos données - Toutes les institutions ne proposent pas ce service
 Serveur Cloud	★★☆☆ On ne sait pas vraiment où sont stockées les données, ni ce qu'elles deviennent	★★★★ Permet un travail synchronisé avec toutes les personnes ayant été autorisées au partage	★★☆☆ Payant à partir d'une certaine limite de stockage	- Pour un partage avec des personnes externes à l'institution - Ne pas y mettre de données sensibles ou confidentielles - Pas de contrôle sur la procédure de sauvegarde des données

Bref historique de l'évolution des mentalités

- 8-9 ans on ne parlait pas encore de cloud ss (stockage propriétaire)
- 4-5 ans certains y sont allés frileusement (pas tjs avec les bonnes données)
- Enfin depuis 3 ans, la question n'est plus de l'utiliser ou non, mais comment y aller (pure cloud ou hybrid)

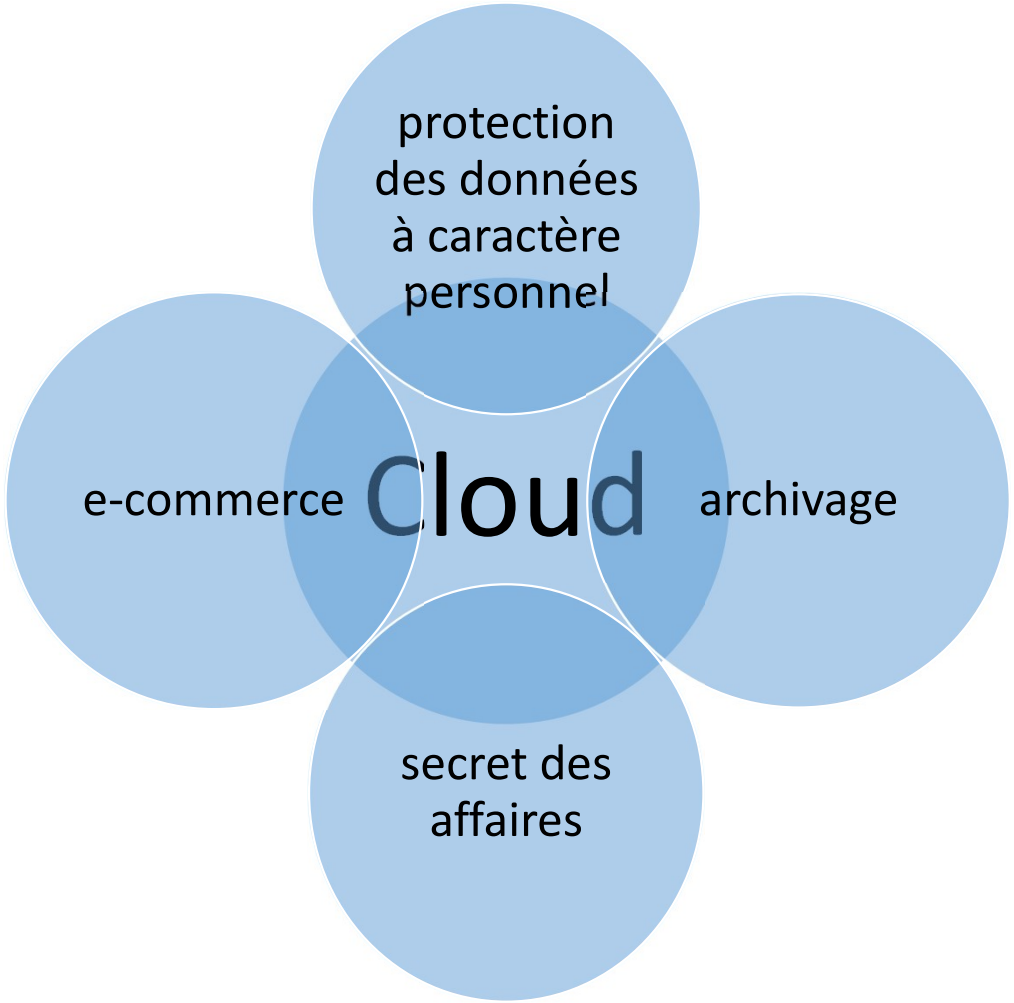
Le cloud lui-même a évolué :

- la baisse des prix du stockage
- l'amélioration de la bande passante
- Le développement des services proposés (infra diminue en interne / on demand)

De toute évidence, l'adoption des services cloud dépend avant tout des exigences réglementaires, des questions de confidentialité et de sécurité. Plus la réglementation va se développer et gagner en maturité, plus les entreprises profiteront pleinement des bénéfices du cloud computing.

La sécurité/confidentialité (angle juridique et législatif)

En Europe, tout particulièrement, les règles régissant la confidentialité sont on ne peut plus strictes et de nombreux gouvernements interdisent aux entreprises d'exporter les données au-delà des frontières (Longbottom 2008).


protection des données à caractère personnel
e-commerce
Cloud
archivage
secret des affaires

La sécurité/confidentialité (les questions à se poser)

- Quelles sont les technologies de sécurité particulières mises en place par le fournisseur ?
- Comment les sauvegardes de données sont-elles gérées et où les données sont-elles stockées ? (jeux de réplication)
- Comment le chiffrement est-il utilisé ?
- Où sont situés les datacenters ?

La sécurité/confidentialité (angle technique)

- TRANSMISSION DES DONNÉES (ligne chiffrée SSL ou data)

- STOCKAGE DES DONNÉES
- ✓ honnêteté du fournisseur …
- ✓ si chiffrement il y a, quid de la gestion des clés ?

- ACCÈS AUX DONNÉES (mécanismes d'authentification sont adéquats)
  - Identification classique (Ident. Mdp, Mdp SMS)
  - Authentification forte (Ident., Mdp, Mdp Token)

- DESTRUCTION DES DONNÉES (en fin de contrat)

La sécurité/confidentialité (angle technique):

Le chiffrement homomorphe très prometteur…

La sécurité/confidentialité (angle géographique)

- Cloud du GAFAM (sociétés américaines soumises au Patriot Act) (Cas SpideRoak (zero knowledge)

- Cloud Européen (Mozy (iso27001), OVH, Wimi, Wuala…)

Ce qu'il faut retenir

- Bien étudier les contrats en amont
- Le choix du fournisseur et surtout des sous-traitants
- Partir sur un « Cloud hybrid »
- Rester sur le territoire Européen
- Chiffrer ses données durant les transfert et dans le cloud
- S'assurer des conditions de stockage