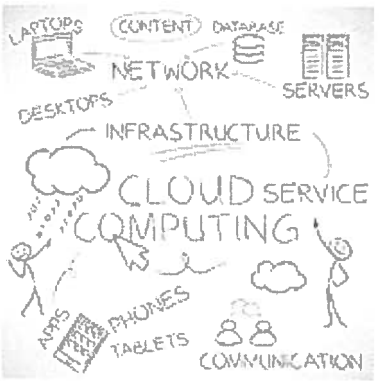
: : : : à la Une : : : :

09/05/2012 - Déontologie

# Le périlleux équilibre entre cloud computing et secret professionnel

**Mécanisme en plein développement et à l'origine de la création d'environ 15 millions d'emplois en trois ans, le cloud computing fait désormais partie du paysage informatique. Ses services proposent de stocker d'importants volumes de données sur plusieurs serveurs distants, uniquement accessibles via une connexion Internet.**




## *A lire également*

**La levée du secret de l'avocat n'entraîne pas la levée du secret médical**

**L'avocat lyonnais David Metaxas mis en examen à Dijon**

**Quand le contrôle fiscal se frotte au secret professionnel**

**Le secret professionnel n'est pas soluble dans le code des marchés publics**

Selon Google, prestataire dominant de ce service, le cloud représente la réponse aux problèmes de sécurité du Web. En effet, en dispersant les informations dans le monde ce système permet de diminuer les failles de sécurité informatique. A cet argument, Clarisse Berrebi, présidente de la commission Nouvelles Technologies du Conseil National des Barreaux, répond que "le cloud computing pose de nombreux problèmes majeurs pour l'avocat, nécessairement obligé par ses règles déontologiques dont le secret professionnel. L'avocat qui utilise les solutions libres actuelles s'expose et doit savoir qu'il s'expose. En l'état, il n'est pas possible que le CNB encourage un système totalement régulé par le marché libre. Les données sont stockées à l'étranger avec bien peu de garanties et, quelque fois dans des pays où notre secret peut être malmené". Car c'est là que la bât blesse : la protection du secret professionnel. "Je n'utilise pas le cloud pour le cabinet. Au contraire, j'ai tendance à internalisé les données confidentielles. Avec un serveur interne dédié, nous pouvons accéder à l'ensemble de nos données de façon totalement sécurisée, ce qui n'est pas le cas du cloud : nous ignorons où se trouvent les données et qui peut y avoir accès", estime Gilles Rouvier, avocat à Paris. Dans son cabinet lyonnais, Alain Devers avoue ne pas plus utiliser les mécanismes de cloud computing "pour des raisons de secret professionnel".

## Un secret illimité...

Au fond, le cloud et le secret seront-ils un jour compatible ? "Quand bien même il nous proposerait un contrat de sécurité, des accès sécurisés, etc. Internet reste du domaine public et nous ne pouvons pas confier des données aussi sensibles que celles des relations avec nos clients au domaine public", tranche Alain Devers. Selon la définition donnée par l'article 2 du code de déontologie, cite Gilles Rouvier, "le secret professionnel est d' «ordre public général, absolu et illimité dans le temps». Le client ne peut donc pas nous en relever, même s'il nous donne l'autorisation de stocker ses données sur un cloud". La Commission Nationale de l'Informatique et des Libertés (CNIL) s'inquiète, elle aussi, de la localisation des données dans des pays aux faibles garanties de protection. Consciente de la demande des professionnels, elle tente d'adopter une large interprétation de l'article 5 de la Loi Informatique et Libertés telle que modifiée le 06 avril 2004. La Commission Européenne, de son côté, veut établir un socle juridique, mais cela risque de ne pas être suffisant pour rassurer les avocats.

### Un cloud sous l'égide du CNB ?

La création d'un "nuage" dédié à la profession ne serait-elle pas un début de réponse ? Pour Alain Devers, "si le CNB validait un dispositif labélisé compatible avec le secret professionnel, dans ce cas nous pourrions peut être l'utiliser plus facilement". Sauf qu'il "ferait tout de même appel à un prestataire extérieur au sujet duquel nous n'aurions jamais suffisamment de garanties", ajoute Gilles Rouvier. "Seule une solution nationale, autour du RPVA, serait parfaitement protégée et permettrait de garantir l'égalité des confrères face aux technologies modernes. Le Conseil National doit s'en donner les moyens, c'est un objectif évident", conclut Clarisse Berrebi.

Par Marie Bucaille

---

## *Réactions des lecteurs*

1 · **Domjohn** le *mercredi 9 mai 2012* - 9h03

### Erreur d'analyse

En premier lieu, Il existe aujourd'hui,des solutions cryptées qui ont pour conséquences que même le prestataire n'a pas accès à vos données. Ainsi si vous perdez votre mot de passé, vous perdez l'accès à vos données. En deuxième lieu, les fuites de données viennent souvent de l'intérieur. Il est donc illusoire de penser que les données,seront nécessairement mieux conserver en les "internalisant". Bref, il ne faut pas donner ses data à Google qui les considèrent comme sa propriété, mais choisir son prestataire. Enfin il va bien nous falloir le cloud pour,partager nos dossiers pièces souvent énorme non? Votre bien devoué

Haut de page