Encadrement juridique du Cloud : peut-on éviter l'orage ? (tribune)

La panne récemment observée sur une partie des services proposés par Microsoft via son Cloud, Azure, et surtout les réactions consécutives à cette panne, ont le mérite de remettre sur le devant de la scène l'importance d'un élément capital, mais que l'on ne regarde souvent qu'à partir du moment où la situation dégénère : le contrat.

Alors que, selon les chiffres du cabinet PAC (CloudIndex), les organisations françaises passent majoritairement au Cloud, 30 % seulement d'entre elles ont mis en place une stratégie Cloud. L'approche reste donc encore majoritairement opportuniste. Et **qui dit approche opportuniste, dit très souvent risques** (notamment juridiques) mésestimés.

Les risques liés à la valeur, à la localisation des données, à leur nature ou encore à l'immixtion de l'État d'origine du prestataire (cf. US Patriot Act et consorts) sont maintenant largement connus et illustrés d'exemples récents (saisie des serveurs de messagerie dans l'affaire Mega, etc.).

Paradoxalement toutefois, ce sont les risques plus « classiques » en matière d'externalisation qui ne doivent pas être sous-estimés, et qui le sont souvent, notamment dans l'hypothèse d'un « produit sur étagère » tel que le SaaS où le niveau d'engagement contractuel du prestataire est un critère s'effaçant devant les atouts majeurs du « Cloud computing » (coûts, élasticité, etc.)

Il n'en reste pas moins que l'histoire récente est émaillée de défaillances de petits comme de grands prestataires, parfois à répétition. Dans cette hypothèse, les conséquences peuvent être d'autant plus importantes pour l'entreprise cliente qu'elle n'a pas forcément intégré dans ses propres analyses le risque de défaillance du prestataire (défaillance qu'elle prenait en compte, à l'inverse, quand le service était internalisé, voire externalisé auprès de prestataires connus et strictement encadrés contractuellement). Un rapport récent chiffre ainsi à plus de 500 millions d'euros le coût des pannes dans le Cloud.

Tout le contrat, rien que le contrat

Dans ces situations où le voyage dans le nuage n'est pas toujours assuré, une lecture plus attentive du contrat conclu parfois avec hâte (notamment sur les engagements de services) peut sonner comme un **brusque retour sur terre** pour les entreprises clientes.

Que ce soit au niveau du **droit applicable** (droit de l'Etat du prestataire), de l'**information de l'entreprise cliente** au moment de l'incident, des **conditions de remboursement** du préjudice (souvent sur demande du client et parfois à la seule main du prestataire) ou encore du **montant** dudit remboursement (rarement plus de 25 ou 30 % du coût de la prestation, même en cas d'indisponibilité prolongée), peu de services de Cloud proposent des réponses contractuelles adaptées aux enjeux réels des entreprises… qui ont choisi de contractualiser malgré ces risques (à supposer qu'il étaient été évalués ou convenablement estimés).

Quand le droit français est applicable, la décision n'en est pas pour autant au bénéfice de la société

cliente, tenue par les termes du contrat souscrit : ainsi en a décidé le Tribunal de commerce de Paris le 12 juillet 2011. Après plusieurs défaillances, la messagerie « dans le Cloud » de l'entreprise n'a été rétablie qu'au bout de 5 jours par le prestataire. Beaucoup trop long pour le client qui résilie le contrat aux torts du prestataire… et est notamment condamné à payer le montant des trimestres de son abonnement restant à courir : le contrat stipulait noir sur blanc un délai de 30 jours ! **Attention donc à une lecture trop rapide des contrats** (et surtout des *Service Level Agreements*) qui ne seraient pas en adéquation ni avec les engagements espérés par l'entreprise, ni avec son évaluation des risques.

La qualité de service s'achète… et se contrôle

D'autant que parfois, l'issue peut être encore plus radicale pour l'entreprise cliente : le service d'hébergement en ligne de code source Code Spaces (« *Rock Solid, Secure and Affordable Svn Hosting, Git Hosting and Project Management*«) a ainsi dû fermer définitivement à la suite d'un piratage ayant conduit à l'effacement d'une grande partie des fichiers de ses clients (son comportement ayant été par ailleurs gravement défaillant en termes de sécurité et d'archivage).

A la lumière de cet exemple, le contrat doit prévoir des **moyens d'auditer la réalité des engagements** de services souscrits, afin de donner de la visibilité à « l'informatique en nuage ». On ne peut que saluer à ce titre les diverses initiatives de certification dans le Cloud, comme ceux de Cloud confidence pour les opérateurs de Cloud français et européens.

Pour ces raisons, afin de tirer la substantifique moelle du Cloud, l'entreprise devra au minimum, en amont de la décision d'investir et tout au long de la prestation, se livrer à une **étude fine** :

- du **patrimoine informationnel** qu'elle y fait traiter (vis-à-vis le cas échéant de ses régulateurs) ;
- de ses **risques**, notamment juridiques ;
-  des **audits** qu'elle doit faire effectuer pour s'assurer de la qualité de la prestation ;
- de ses **moyens d'action contractuels** en cas de manquement (performance, disponibilité, sécurité des données, notification des incidents, etc.).

Par François Coupez, Avocat à la Cour, Associé du cabinet ATIPIC Avocat et titulaire du certificat de spécialisation en droit des nouvelles technologies

Crédit photo de haut de page : Shutterstock