Le cloud à l'épreuve du droit : sécuriser et manager ses contrats

0

26 Nov 2015 | cloud, contrat, Iaas, Paas, Saas | by Aurelie Magniez

Le cloud computing bouleverse le droit applicable en transcendant les frontières géographiques des nations ce qui pose de graves questions sur la protection des données personnelles, en virtualisant serveurs et espaces de stockages au moyen d'hyperviseurs, ce qui pose des questions en termes de respect des contrats de licence ne connaissant pas cette métrique, ou encore en mutualisant des ressources, ce qui pose des questions de confidentialité et de sécurité.

La réciproque est vraie : le cloud computing est aussi mis à l'épreuve du droit. Cette technologie a connu ou va connaître de nombreux bouleversements normatifs : adoption récente de normes ISO dédiées, abrogation de la tolérance légale de migration des données vers les Etats-Unis ("Safe Harbor"), nouvelles dispositions légales et réglementaires attendues dans les lois Lemaire et Macron 2.

Plus que jamais, le client utilisateur du cloud doit pouvoir sécuriser son contrat et le manager dans le temps. Après un bref panorama de ces grandes interactions entre technique et droit, cet article présente les meilleures pratiques contractuelles pour apporter sécurité et pérennité de l'usage du cloud.

Prémices de la normalisation du cloud

Pour répondre à la multiplication des plateformes cloud avec leur bouquet de services (IaaS, PaaS, SaaS…), l'Union Internationale des Télécommunications (UIT) et l'ISO ont travaillé de concert pour publier trois normes fin 2014 :

- **la norme ISO 17788** définit les cinq types d'intervenant sur le marché du cloud computing (auditeurs, partenaires, clients, fournisseurs, intermédiaires), les trois types de services proposés (infrastructure as a service ou « IaaS », platform as a service ou « PaaS » et Software as a Service ou « SaaS ») ;

- **la norme ISO 17789** s'attache à définir l'architecture fonctionnelle de référence, c'est-à-dire la façon de construire une plateforme de services cloud computing, dans un souci d'interopérabilité ;
- **la norme ISO 27018** fixe les règles de sécurité à appliquer pour les fournisseurs de cloud public afin d'assurer la protection des données personnelles, garantir la transparence et se conformer à leurs obligations réglementaires.

Progressivement, les principaux acteurs (dont, par exemple, Microsoft pour les services 365) se sont appropriés ces normes, en tant que label qualité.

La grande évolution attendue est l'adoption d'une norme sur les engagements de performance du cloud (projet de norme ISO 19086), cependant les travaux tardent à être publiés et, en pratique, benchmarker les offres cloud reste toujours très délicat, tant les paramètres sont nombreux et particuliers à chaque opérateur.

Nullité du Safe Harbor

Le mécanisme du Safe Harbor résultant de l'accord signé en juillet 2000, permettait les transferts de données vers les Etats-Unis. Or, la Cour de justice de l'Union européenne (CJUE) a considéré, par arrêt du 6 octobre 2015, qu'il n'était pas conforme au droit européen.

Elle a en effet estimé que ce mécanisme de protection des données à caractère personnel, auquel les entreprises américaines peuvent adhérer afin de recevoir des données de pays appartenant à l'Union européenne, ne permettait pas de garantir, de manière effective, un niveau de protection adéquat des données à caractère personnel. Toutes les offres dans le cloud proposés par les Gafa (Google, Amazon Web Services, Facebook et Apple) sont donc particulièrement visées.

Suite à l'invalidation de l'accord Safe Harbor, il n'est plus possible de réaliser un transfert de données à destination des Etats-Unis par le biais de l'adhésion au Safe Harbor. A défaut d'un nouvel accord, actuellement en discussion entre administrations américaines et européennes, seul le contrat permet d'envisager légalement ce type de transfert (voir infra).

Lois Lemaire et Macron 2 : les nouveautés attendues sur le cloud

Le projet de loi pour une République numérique porté par Axel Lemaire, secrétaire d'Etat au numérique, vise à développer et sécuriser les nouveaux usages du numérique, en particulier pour l'open data et le big data. Sur le cloud, les apports sont timides et ne concernent a priori que le consommateur : droit à la portabilité et à la réversibilité des données, droit à l'oubli numérique pour les mineurs devenus majeurs. Les prestataires du cloud pour le grand public devront prendre en compte cette nouvelle donne juridique et concevoir des services nativement « privacy by design. » Ce projet de loi devrait être adopté au premier trimestre 2016.

Le projet de loi sur les nouvelles opportunités économiques, dite « Macron 2 » ou « Noé » devrait être plus ambitieux et relancer l'idée d'un cloud souverain basé sur la régionalisation des données. La clarification du contexte juridique sur le coffre-fort numérique devrait donner un nouveau souffle à de nombreux projets de dématérialisation. Cette loi ne serait pas adoptée avant la fin d'année 2016.

Le projet de loi sur les nouvelles opportunités économiques, dite « Macron 2 » ou « Noé » devrait être plus ambitieux et relancer l'idée d'un cloud souverain basé sur la régionalisation des données. La clarification du contexte juridique sur le coffre-fort numérique devrait donner un nouveau souffle à de nombreux projets de dématérialisation. Cette loi ne serait pas adoptée avant la fin d'année 2016.

Solutions contractuelles

Face aux incertitudes portées par ces nombreuses interactions entre cloud et le droit, le contrat est l'outil le plus adapté pour sécuriser le client comme le prestataire. Tel est d'ailleurs l'un des nombreux enseignements du dernier rapport du Cigref, club d'utilisateurs SI sur « la réalité du cloud dans les grandes entreprises ». Chacun des points évoqués, ci-dessus fait l'objet d'un développement, ci-après.

Sur les obligations liées à la confidentialité et à la sécurité des données, le prestataire cloud doit prendre la mesure qu'il est le seul à pouvoir contrôler les ressources qu'il met à la disposition de ses clients. En lien avec des engagements de disponibilité et de performance mesurés et mesurables, une obligation de résultat doit prévaloir dans les relations entre les parties. La garantie du respect de certaines normes techniques (dont celles précitées) outre les garanties de performance et de robustesse doit être explicitement mentionnée au contrat.

Sur la gestion de la propriété intellectuelle, tout projet SaaS, présuppose que les logiciels qui y sont installés puissent faire l'objet d'une telle installation dans le Cloud. Un complément de licences devra être souscrit, le cas échéant. La même vigilance doit être de mise pour les clauses prix et modalités de paiement afin que le budget cloud reste sous contrôle.

Sur la question particulière des flux transfrontières de données personnelles, à défaut d'un contrat organisant le cloisonnement des données par région, il faut insérer dans le contrat des clauses contractuelles types autrement appelées des BCR (pour « Binding Corporate Rules ») au sein de sociétés appartenant à un même groupe. Sauf exception expresse prévue par la Cnil (exemple : article 9 de la norme simplifiée n°48 pour la gestion de données clients ou prospects), une autorisation préalable devra être obtenue avant tout transfert.

Parce que le cloud computing est désormais incontournable, face à un contexte juridique mouvementé, le contrat personnalisé et négocié par chaque partie est le principal facteur clé d'une relation pérenne et équilibrée.

Eric Le Quellenec
Directeur du département Informatique conseil

Alain Bensoussan Avocats
Le droit du numérique et des technologies avancées

Alain Bensoussan-Avocats est un cabinet d'avocat entièrement dédié au droit des technologies avancées depuis 1978. Pour la 5e année consécutive depuis 2010, il a été distingué par ses pairs, « Best Lawyer » de l'année en « Droit des Technologies ».
Site : **http://www.alain-bensoussan.com/**