

JURIDIQUE



Christiane Féral-Schuhl,
avocate à la Cour, et associée fondatrice
du cabinet Féral-Schuhl Sainte-Marie

DR

Cloud computing : y voir plus clair dans la nébulosité juridique

LE FAIT : le cloud computing est présenté comme la prochaine mutation technologique majeure. Cette innovation s'accompagne néanmoins de nouvelles problématiques juridiques qu'il convient d'explorer.

Saas, IaaS, PaaS... Derrière ces acronymes, réunis sous le terme générique de cloud computing, se cachent de nouveaux modes de commercialisation des services informatiques. Les acteurs du secteur promettent une totale souplesse d'infrastructure en contrepartie d'une « évaporation » des données dans un « nuage » de serveurs. Cette mutation technologique pose quelques questions sur le plan juridique.

Ne pas stocker n'importe où

Le cloud computing n'est pas généralisable à tout type de données. Des tiers ou les pouvoirs publics ont parfois un droit de regard sur certaines d'entre elles, afin de mieux encadrer, ou d'interdire, le recours à cette technologie. Ainsi, l'article L. 102 C du livre des procédures fiscales prévoit que les assujettis ne peuvent pas stocker les factures transmises par voie électronique dans un pays non lié à la France par une convention en matière de fiscalité. Cela limite les lieux de stockage de ces documents à l'Union européenne.

De même, la loi informatique et libertés impose au responsable d'un traitement informatisé de données à caractère personnel de garantir

la confidentialité et la sécurité des informations conservées. Il en résulte une interdiction de les transférer vers des pays « n'offrant pas un niveau de protection adéquat ». Ils sont nombreux : Etats-Unis, Inde, Chine, continent africain... Le recours au cloud public doit alors être exclu, sauf s'il existe une convention spécifique, établie par la Commission européenne en accord avec le fournisseur et intégrant des clauses contractuelles types.

Précautions contractuelles

Lorsqu'une entreprise choisit de confier ses données à un prestataire, cette perte de contrôle doit s'accompagner de garanties juridiques, d'où l'importance du contrat. Cela est encore plus vrai dans le cadre d'une externalisation vers un cloud : le client pourra en effet ignorer jusqu'à la localisation physique des machines qui hébergent ses applicatifs et ses données. Il conviendra donc de porter une attention particulière aux engagements contractuels que le prestataire est prêt à prendre en matière de disponibilité, de sécurité, de confidentialité et de réversibilité. ■ CHRISTIANE FÉRAL-SCHUHL

CE QU'IL FAUT RETENIR

Le recours au cloud computing peut être limité par les dispositions légales existantes. Il doit en tout état de cause s'accompagner de garanties contractuelles en matière de disponibilité, de sécurité, de confidentialité et de réversibilité.

NUL N'EST CENSÉ...

Indépendance des autorités de contrôle

Dans un arrêt du 9 mars, la Cour de justice de l'Union européenne (CJUE) a considéré que les autorités de protection des données des Länder allemands, qui contrôlent les fichiers du secteur privé, n'agissaient pas en totale indépendance, mais sous la tutelle de l'Etat fédéral allemand. Et ce, contrairement aux dispositions de la directive européenne de 1995 sur la protection des données.

Les commentaires excessifs d'Academia

Le 22 avril, la Cnil a prononcé un avertissement public à l'encontre d'Academia, société spécialisée dans le soutien scolaire. En effet, à la suite d'un contrôle effectué en novembre dernier, la Commission a constaté la présence, dans ses fichiers, de centaines de milliers d'informations concernant à la fois les enseignants, les parents et leurs enfants. Elle a relevé de nombreux commentaires excessifs, des informations détaillées sur l'état de santé des personnes, ou encore des données relatives aux casiers judiciaires de certains élèves. La Cnil a également informé le parquet de ces différents manquements susceptibles de constituer des infractions pénales. La délibération sur <http://goo.gl/KpQ3>.

Usurpation d'identité numérique

Par un arrêt en date du 12 mars, la chambre sociale de la Cour de cassation a confirmé la décision rendue par la cour d'appel d'Aix-en-Provence le 13 avril 2008. Elle estime ainsi que le salarié qui, « sous des pseudonymes féminins, a entretenu pendant plus d'un an avec un de ses subordonnés une correspondance soutenue, avec son ordinateur professionnel et pendant son temps de travail », a commis une faute grave justifiant son licenciement. En créant ainsi une « correspondante féminine virtuelle », le supérieur hiérarchique avait tenté de manipuler un de ses employés.