La CNIL met en garde les entreprises sur les dangers du cloud

Après avoir lancé en 2011 une consultation publique sur le cloud computing, la Commission nationale informatique et libertés (CNIL) estime urgent de clarifier le cadre juridique applicable aux offres d'informatique distribuée, infrastructures (Iaas), plateformes de développement (PaaS) et logiciels en tant que service (SaaS).

Des risques en cascade

« Les questions de sécurité, de qualification du prestataire, de loi applicable et de transfert des données sont particulièrement délicates », a souligné la CNIL lundi 25 juin par voie de communiqué. Les difficultés sont plus marquées dans le cas d'offres standardisées, les contrats d'adhésion ne permettant pas aux clients de négocier. Par ailleurs, l'information fournie par les prestataires quant aux conditions de réalisation des prestations *« manquent de transparence »*, notamment sur le fait de savoir si les données concernées sont transférées à l'étranger.

La CNIL recommande donc à toute entreprise française qui envisage d'utiliser un service de cloud computing d'analyser les risques en amont et de choisir son prestataire avec précaution. Autrement dit, il revient à l'entreprise cliente de s'assurer que le service auquel elle a recourt lui permettra de respecter ses obligations au regard de la loi informatique et libertés française.

Concernant la sécurité, la CNIL constate que les offres de cloud *« reconnues »*, autrement dit celles proposées par des entreprises d'envergure internationale, peuvent présenter des niveaux de sécurité supérieurs à ceux que peuvent garantir les PME. Globalement, le cloud génère de nouveaux risques pour les clients et leurs prestataires, notamment en ce qui concerne la pérennité des données. Pour tirer profit du cloud tout en limitant les risques, la Commission informatique et libertés préconise les mesures suivantes :

- *Identifier clairement les données et les traitements qui passeront dans le cloud;*
- *Définir ses propres exigences de sécurité technique et juridique;*
- *Conduire une analyse de risques afin d'identifier les mesures de sécurité essentielles pour l'entreprise;*
- *Identifier le type de cloud pertinent pour le traitement envisagé;*
- *Choisir un prestataire présentant des garanties suffisantes en déterminant sa qualification juridique;*
- *Revoir la politique de sécurité interne;*
- *Surveiller les évolutions dans le temps;*

Des contrats renforcés

En outre, les informations relatives aux traitements des données, les garanties mises en oeuvre par le prestataire, les obligations lui incombant en matière de sécurité et de confidentialité ou encore la localisation et les transferts doivent figurer dans un contrat de prestation de services de cloud computing. Enfin, lorsque le prestataire est sous-traitant, il est dans l'obligation de fournir à son client toute information utile permettant de procéder à la déclaration du traitement auprès de la CNIL. Lorsque le prestataire est responsable conjoint du traitement, le client et le prestataire doivent déterminer quelle partie sera en charge des formalités pour son compte et pour celui de l'autre partie.

Ces précisions ne devraient pas limiter l'engouement des entreprises pour l'informatique distribuée. Vice-présidente de la Commission européenne, Neelie Kroes s'est déjà prononcée en faveur d'une Europe « cloud active ». Elle a déclaré, le 25 juin, lors d'une intervention à Bruxelles : *« 2012 est l'année où le cloud prend son envol. Un véritable marché en ligne nous donnera l'élan économique dont nous avons besoin maintenant. »* D'après IDC, grâce au cloud computing près de 14 millions d'emplois dans le monde seront créés d'ici à 2015, dont 189 000 en France.

crédit photo : © Beboy – Fotolia.com