Nomos
société d'avocats

nomosnetcom.fr **Juillet 2012**

La CNIL et le Groupe de travail de l'Article 29 livrent leurs premières analyses sur le cloud computing

[DONNEES PERSONNELLES]
Synthèse et recommandations de la Cnil sur le cloud computing, juin 2012
Opinion du Groupe Article 29, 1er juillet 2012

La CNIL et le Groupe de travail de l'Article 29 ont publié à quelques semaines d'intervalle leurs analyses et recommandations pratiques sur les risques et enjeux du cloud computing en matière de protection des données personnelles.

Les deux documents publiés abordent sans surprise les mêmes thèmes. Il convient néanmoins de souligner que l'Opinion du Groupe Article 29 expose la position des autorités de protection européennes en matière de données personnelles alors que le document publié par la CNIL a été établi en tenant compte des avis et suggestions exprimés par les clients et prestataires de services cloud computing suivant la consultation publique lancée fin 2011. La synthèse de la CNIL résulte donc d'une approche plus collaborative.

La diversité des services cloud rend difficile l'établissement d'une analyse totalement uniforme des responsabilités respectives des clients et prestataires en matière de conformité à la législation encadrant les données personnelles.

Le développement exponentiel de ces services, caractérisés notamment par l'externalisation des ressources de stockage et la localisation multiple de ces ressources, impose en outre l'adaptation des modèles contractuels encadrant classiquement les relations entre clients et prestataires en matière d'outsourcing.

L'apport décisif de la synthèse de la CNIL et de l'Opinion du Groupe Article 29 porte sur la qualification du rôle du prestataire puisque de celle-ci découle l'essentiel du régime applicable en matière de données personnelles (détermination de la loi applicable au traitement, répartition des obligations de sécurité pesant sur les parties, des obligations d'information à l'égard des personnes dont les données sont traitées, et règles régissant le transfert des données hors UE).

A cet égard, la CNIL et le Groupe Article 29 soulignent que le client est *par principe* le responsable du traitement dans la mesure où il est à l'origine de la collecte des données et de la décision d'externalisation du traitement auprès du prestataire, qui agit dès lors en qualité de sous-traitant (tenu à ce titre par les obligations prévues à l'article 26 de loi Informatique et Libertés). Cette analyse s'impose sans difficulté pour le cloud dit « privé » c'est-à-dire les services exclusivement dédiés à un client qui est dès lors en mesure de maîtriser et déterminer les caractéristiques du service demandé au prestataire.

Mais la CNIL et le Groupe Article 29 admettent également que l'application du principe s'avère plus délicate en matière de cloud « public » où les conditions de la prestation et l'organisation fonctionnelle sont déterminées par le prestataire, dans le cadre d'offres standard mutualisées auprès de multiples clients. Dans cette dernière hypothèse, la CNIL estime que le client et le prestataire pourraient être considérés *conjointement responsables* du traitement. Le Groupe Article 29 complète cette analyse en observant que ceci ne doit en aucun cas aboutir à une dilution de la responsabilité.

- Les parties doivent en conséquence définir contractuellement et avec précision la répartition des obligations attachées à la responsabilité qu'elles assument, de même que le contrat doit prévoir l'ensemble des mesures techniques et organisationnelles (en particulier, les mesures d'audit) permettant au client de s'assurer que le service mis en œuvre par le prestataire est conforme aux exigences réglementaires encadrant la protection des données personnelles et qu'il permet de garantir la sécurité des données traitées.

- La transparence doit constituer un impératif partagé par le client et le prestataire tant au stade de la négociation des conditions du service qu'au stade de la formalisation contractuelle. Notamment, la localisation des infrastructures de stockage du prestataire, comme les mesures de sécurité mises en œuvre, doivent impérativement être exposées clairement.

- Le Groupe Article 29 insiste également sur le fait que, dans la mesure où les prestataires de services cloud sous-traitent très souvent une partie des prestations à d'autres sous-traitants, la chaîne de sous-traitance doit être détaillée par la convention de sorte que le client puisse s'assurer que les sous-traitants sélectionnés par son prestataire respectent la législation en matière de données personnelles.

- La détermination de la loi applicable constitue une autre problématique importante en matière de cloud computing compte tenu notamment de la multi-localisation des infrastructures. La plupart des contributeurs à la consultation publique de la CNIL proposent de ne retenir que la loi du responsable de traitement. Cette approche a le mérite de la clarté mais elle est inefficace dans l'hypothèse où le prestataire et le client seraient conjointement responsables et ne se trouveraient pas établis sur le même territoire. La CNIL propose de retenir le critère du public ciblé par le traitement mais l'on sait que cette voie, inspirée du projet de Règlement européens sur les données personnelles, est loin de faire l'unanimité et qu'elle ne peut en tout état de cause être effective à ce jour en l'absence d'adoption du Règlement.

  Il faut donc conclure que la détermination de la loi applicable doit systématiquement faire l'objet d'un examen au cas par cas, au regard des dispositions légales actuellement en vigueur. Cette question revêt évidemment une importance capitale aux fins d'assurer la conformité réglementaire du traitement mais elle peut également être déterminante en cas de réquisitions judiciaires ou gouvernementales aux fins de communications des données personnelles stockées par le prestataire.

- Une autre difficulté résultant de la multiplication des lieux potentiels de stockage (et de leur instabilité) concerne l'encadrement des transferts de données intervenant entre le client et le prestataire mais également entre ce dernier et les possibles sous-traitants.

  La CNIL propose que les prestataires intègrent dans leurs contrats de prestations de services les clauses contractuelles types adoptées par la Commission européenne pour l'encadrement des transferts et qu'ils mettent en œuvre des Binding Corporate Rules avec leurs sous-traitants.

Les deux documents publiés par la CNIL et le Groupe de travail Article 29 sont incontestablement utiles pour guider la rédaction et la négociation des contrats en matière cloud computing. Mais ils démontrent également que la règlementation actuelle ne permet pas d'appréhender l'ensemble des problématiques posées par ces services et qu'elle est dès lors source d'insécurité.

Hélèna DELABARRE