



LES NOUVEAUX ENJEUX JURIDIQUES

Le recours au cloud computing est un incontournable. S'il présente des aspects pratiques indéniables, il n'est pas sans poser de nouvelles problématiques juridiques, notamment sur le plan de la responsabilité.

Un certain nombre de nouveaux dispositifs juridiques viennent impacter les conditions dans lesquelles s'inscrivent les enjeux juridiques de la responsabilité, notamment contractuelle, des acteurs concernés par le cloud.

À propos des aspects liés à la responsabilité dans les contrats de cloud, la question qui est posée est celle de la répartition des rôles entre le prestataire de services de cloud, d'une part, et son client, d'autre part, telle que cette répartition est appréhendée par le RGPD. Si ce dernier ne traite pas directement de cette question, pas plus d'ailleurs que ne le fait la Cnil dans son « *Guide du sous-traitant* » édité en septembre 2017, un certain nombre de lignes de force peuvent cependant être dégagées pour la rédaction des contrats de cloud.

- Tout d'abord, **l'article 28 du RGPD impose l'existence d'un contrat devant lier le client (en qualité de responsable de traitement) à son prestataire de services de cloud (en qualité de sous-traitant)**. Ce contrat doit définir l'objet et la durée des traitements confiés par le premier au second, la nature et la finalité des traitements réalisés, le type de données à caractère personnel concerné, les catégories de personnes concernées ainsi que les obligations et les droits du responsable de traitement, notamment.
- **L'article 82 du RGPD pose, quant à lui, les règles à respecter en matière de partage de responsabilité** entre le responsable du traitement et son sous-traitant.

À ce titre, la première règle est qu'il ne peut exister d'exclusion de responsabilité, ni envers la personne physique concernée par le traitement, ni envers l'autorité de contrôle prononçant une sanction. La seconde règle est que, si une partie a supporté à l'égard de la personne concernée, tout ou partie d'une indemnisation versée au profit de cette dernière, alors elle peut se retourner contre son sous-traitant pour que cette charge soit répartie à concurrence de la part de responsabilité respective de chaque intervenant au traitement. Cette seconde règle entraîne donc des répercussions majeures sur la manière dont doivent être rédigées les clauses de responsabilité dans les contrats de cloud, puisqu'elles posent les principes qui seront appliqués si la responsabilité de l'un, de l'autre ou des deux acteurs devait être mise en cause par un tiers.

Les exigences du Cloud Act face aux dispositions du RGPD

Au-delà de ces aspects, le cloud pose également de nouvelles questions quant à la capacité que devraient, ou pas, avoir les autorités judiciaires à se voir communiquer les informations hébergées par des entreprises auprès de prestataires de services de cloud dans le cadre de procédures. Les États-Unis ont réglé ce point, en adoptant, en avril 2018, le *Clarifying Lawful Overseas Use of Data Act*, encore



appelé *Cloud Act*, au titre duquel un prestataire hébergeant des données intéressant la justice américaine pour des infractions de droit commun est contraint de les fournir sur réquisition, même si les informations se trouvent physiquement hors des États-Unis et sous le contrôle d'une société n'étant pas de droit américain. Ainsi, sur simple réquisition judiciaire, toute société de droit américain doit désormais fournir de telles informations, indépendamment de leur localisation physique ou de la nationalité de la personne qui a fait héberger ces données, faisant légitimement craindre que des données fuient ainsi vers les autorités judiciaires américaines, hors de tout contrôle des clients des prestataires de services de cloud. Cette loi pose déjà des difficultés d'application, principalement car elle est incompatible avec les dispositions de l'article 48 du RGPD qui prévoit que « toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère

ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international [...] », lequel n'existe pas (encore).

Souveraineté de l'Union européenne

Néanmoins, les instances européennes sont en train de travailler sur un « Cloud Act européen » dont l'objectif serait d'établir un cadre juridique pour l'instauration d'une souveraineté de l'Union européenne sur « son » cloud, à l'instar de ce que les États-Unis ont réalisé. On le voit, si le recours au cloud présente la particularité d'être aisé et convivial, il se heurte toutefois à des difficultés juridiques de mise en œuvre, voire à des convoitises dont il est évidemment indispensable qu'elles soient régulées et coordonnées. ■

¹ Avocat à la Cour d'appel de Paris, Frédéric Forster dirige le pôle Télécoms du cabinet Alain Bensoussan Avocats Lexing depuis 2006. Il était précédemment directeur juridique du groupe SFR. Il est également vice-président du réseau international d'avocats Lexing.