Cohabitation difficile entre Cloud Act et RGPD

les faits **Google, IBM ou encore Microsoft, nombreux sont les géants du net à installer leurs datacenters en Europe afin de rassurer leurs clients à l'aune des garanties prévues par le RGPD. Toutefois le Cloud Act, qui dote les autorités judiciaires américaines du pouvoir exorbitant d'obtenir de façon unilatérale les données stockées sur ces serveurs, s'entrechoque avec les dispositions du RGPD.**

Le Cloud Act, voté en toute discrétion le 23 mars 2018 par le Congrès américain, autorise les autorités judiciaires américaines, dans le cadre d'investigations criminelles, à obtenir auprès des entreprises de droit américain fournissant des services d'hébergement cloud les informations stockées sur leurs serveurs, y compris lorsque ces entreprises ou leurs filiales sont situées sur le sol européen. Ce transfert ne peut avoir lieu que sur autorisation judiciaire, par mandat ou court order, donc sous contrôle d'un juge qui en évalue la nécessité à la lumière des investigations menées. C'est ainsi que la justice américaine peut avoir légalement accès à ces bases de données, sans même en informer les personnes concernées. Cette réquisition est notamment susceptible de se heurter à la vie privée et au secret des affaires. De surcroît, il serait coûteux et complexe de saisir le juge américain pour en demander l'annulation, pour autant qu'on en soit informé. L'hébergeur américain dispose ainsi du choix de se soumettre à la décision du juge ou de faire valoir un conflit de loi, sans garantie de succès. Cette question devrait être réglée par un traité international, inexistant en l'état, comme le prévoit l'article 48 du RGPD (qui rend alors exécutoire une décision judiciaire américaine exigeant le transfert de données à caractère personnel hors Union européenne). La France s'est d'ailleurs saisie du

Me Pierre-Randolph Dufau
Avocat à la cour
Fondateur de la SELAS
PRD avocats

sujet, le ministre de l'économie ayant récemment annoncé travailler sur un dispositif permettant de prévenir les entreprises françaises si la justice américaine cherchait à obtenir leurs données stockées sur des serveurs américains. Ces hébergeurs doivent donc mettre en balance les risques encourus du fait du non-respect du Cloud Act et les sanctions records prévues en cas de violation du RGPD. Du point de vue des responsables de traitement, bien qu'il soit difficile de se prémunir complètement d'un texte aussi hégémonique, il est indispensable de prendre des mesures de protection minimales avant de confier l'hébergement de ses données à des prestataires américains ainsi pris en étau. La première consiste à sélectionner des entreprises certifiées par le Département du Commerce Américain en vertu du Privacy Shield, accord leur reconnaissant un niveau de protection des données équivalent à celui requis par le RGPD (informations disponibles sur le site www.privacyshield.gov). Il convient également d'adapter sa politique d'hébergement et de parcelliser le stockage des données en fonction de leur nature. Ainsi, les hébergeurs européens, soumis à de fortes exigences en matière de sécurité, apparaissent plus fiables concernant le stockage de données sensibles et/ou confidentielles. Les fournisseurs de cloud américains, plus compétitifs, restent intéressants pour des données ne nécessitant pas une protection particulièrement accrue. Vouloir négocier des clauses privilégiant l'application de l'une ou l'autre législation peut être envisagé, mais paraît très illusoire. ■

ce qu'il faut retenir **Le conflit de loi entre RGPD et Cloud Act vient nécessairement mettre en péril la sécurité et la confidentialité des données hébergées sur des serveurs américains. Face à ces incertitudes, il appartient aux DSI de diversifier les hébergeurs et de parcelliser les données stockées en cloud.**

Google condamnée par la Cnil

Cette sanction fait suite à la plainte déposée par la Quadrature du Net en mai 2018 contre le moteur de recherche. La Cnil lui reproche un manque de transparence quant à l'usage massif et intrusif des données des internautes et une absence de consentement univoque et différencié de ces derniers à chacun des traitements effectués, une seule case cochée par défaut portant en réalité sur plusieurs finalités.

Les chauffeurs Uber sont soumis au droit du travail

Par un arrêt du 10 janvier 2019, la Cour d'appel de Paris a jugé pour la première fois en France qu'un contrat de travail unissait Uber et ses chauffeurs. En effet, contrairement à ce que prévoit le statut d'auto-entrepreneur, ceux-ci n'ont aucune possibilité de développer leur propre clientèle. À l'instar d'un arrêt rendu le 28 novembre 2018 à l'encontre de Deliveroo, la décision remet à nouveau en question le modèle de l'«ubérisation».

La Cnil statue sur la transmission de données à des partenaires

La Cnil a récemment détaillé les obligations incombant aux sociétés dans le cadre de la transmission de données. Sans surprise, le consentement éclairé de la personne concernée est le maître-mot. Une liste à jour desdits partenaires doit ainsi lui être transmise. De même, aucune «transmission du consentement» n'est possible : les données ne pourront donc pas faire l'objet d'un nouveau transfert par le partenaire. Enfin, le droit d'opposition doit pouvoir être exercé tant auprès du partenaire que de la société à l'origine de la collecte.