Le Cloud Act et ses effets sur les entreprises européennes

Auteur : Philippe CHORBAJY et Maitre Michael AMADO

Le Clarifying Lawful Oversas Use Of Data Act (Cloud Act) est l'ensemble des règles promulguées par le président des Etats-Unis le 23 mars 2018, afin de faciliter l'accès par les autorités américaines aux données stockées à l'étranger par les entreprises américaines au sens du droit américain[1].

La promulgation du Cloud Act a donné lieu à un débat juridique important dans la mesure où beaucoup de juristes considèrent ces règles comme une nouvelle illustration de l'extraterritorialité des lois des Etats-Unis. A cet effet, certains auteurs européens pensent que le Cloud Act a pour but premier de diminuer et anticiper les effets du RGPD[2].

Quelle que soit la finalité du Cloud Act - soit de contrarier ou de limiter les effets du RGPD soit de faciliter l'accès aux données accordées aux autorités américaines, la mise en œuvre de ces règles aura un effet direct et inévitable pour les entreprises européennes et ce, dès qu'une part importante des affaires de ces entreprises entre dans ce qu'on appelle la définition d'une société incorporée aux Etats-Unis impliquant pour ces entreprises d'être soumises aux règles du Cloud Act.

Afin d'analyser l'effet du Cloud Act sur les sociétés européennes et notamment en ce qui concerne leur Compliance et leur conformité, il appartiendra de comprendre dans un premier temps ces règles, leurs contenus, leurs champs d'application, et leurs mises en œuvre, avant d'analyser dans un second temps les effets de ces règles sur les entreprises européennes.

A. Qu'est-ce que le Cloud Act ?

Il s'agit de règles qualifiées d'outils permettant aux autorités américaines d'accéder aux données personnelles de n'importe quel citoyen, peu importe sa nationalité, dès lors que les données personnelles sont stockées par une entreprise incorporée aux Etats-Unis et ce, peu importe la localisation géographique de leur data center. Il est à préciser que par le biais de ce système les autorités américaines ont accès aux données personnelles sans avoir à saisir au préalablement un tribunal ou une autorité étrangère et de surcroît sans en avoir notifié au préalablement les personnes concernées.

[1] Une société au sens du droit américain est une société incorporée aux Etats Unis ainsi que les sociétés contrôlées par elles.

[2] Le RGDP ou le Règlement Européen sur la Protection des Données est l'ensemble des règles entrées en application le 25 mai 2018 par un Règlement Européen.

Pourtant, derrière ces règles, il y a une volonté de renforcer le système d'accès aux données personnelles accordées aux autorités américaines. A cet effet, il appartient de comprendre dans un premier temps le système du Cloud Act du passé avant d'analyser dans un second temps le système du Cloud Act du présent.

1. Qu'est-ce que change le Cloud Act ?

Le Cloud Act vient remplacer le chapitre 121 du Titre 18 du United States Code. Le Titre 18 du United States Code constitue l'équivalent de notre code Pénal et de notre Code de procédure Pénale réunis.

Ce chapitre 121 connu sous le nom de Stored Communications Act ou le SCA, a été introduit dans la législation américaine en 1986.

Ce texte fixe un principe de confidentialité et de protection des données de communication, et prévoit également un certain nombre d'exceptions au principe telles que les divulgations nécessaires à la fourniture du service, les divulgations à la demande de l'utilisateur, ainsi que la possibilité pour les autorités américaines, sous certaines conditions, de requérir des fournisseurs de ces services la communication de données concernant leurs clients pour les besoins de procédures répressives. Cette possibilité est accordée aux autorités américaines dans le cadre d'investigations criminelles au Quatrième amendement à la Constitution des Etats-Unis[3].

Malgré ses exceptions et le pouvoir qu'il a accordé aux autorités américaines, le SCA ne permettait pas aux autorités américaines un certain type d'accès, notamment aux données qui sont stockées à l'étranger.

Une affaire particulière dite affaire Microsoft qui concernait des données stockées en dehors du territoire américain a fait polémique aux Etats-Unis. Cette affaire est considérée par certains auteurs américains comme l'une des raisons principales de l'adoption du Cloud Act.

2. L'affaire Microsoft :

C'est à l'occasion d'une affaire de trafic de stupéfiants que les autorités américaines ont demandé en 2013 à la société Microsoft Corporation de lui communiquer des données de communication concernant un ressortissant non américain.

[3] Protection contre les perquisitions et les saisies non ordonnées par l'autorité judiciaire et non fondées sur une présomption sérieuse que la personne concernée a commis ou est sur le point de commettre une infraction pénale et que les lieux, objets ou informations visées par le mandat sont utiles à l'enquête.

Microsoft Corporation a refusé au motif que les données étaient stockées en Irlande et qu'une telle demande de communication devait emprunter le canal judiciaire international[4].

La cour d'appel du 2nd Circuit de New-York a donné raison à Microsoft. Le Ministère de la justice des Etats-Unis a alors porté l'affaire devant la Cour Suprême des Etats-Unis.

Toutefois, le gouvernement américain a préféré, avant que la décision de la Cour Suprême ne soit rendue, faire adopter le Cloud Act par le Congrès réglant la question directement par la loi.

3. Le contenu du Cloud Act :

Le texte du Cloud Act prévoit essentiellement deux règles principales :

i. Toute société américaine au sens du droit américain, c'est-à-dire une société incorporée aux Etats-Unis ainsi que les sociétés contrôlées par elle, doit communiquer aux autorités américaines, sur leur demande, les données de communication placées sous son contrôle sans considération du lieu où ces données se trouvent stockées.
ii. La possibilité pour le gouvernement des Etats-Unis de signer avec des gouvernements étrangers des accords internationaux permettant aux autorités respectives de chaque pays de demander directement aux fournisseurs de services de communication, la divulgation des données de communication les intéressant, sans avoir à passer par les procédures de MLAT ou des commissions rogatoires internationales.
Par le biais de ces accords, le recours aux dispositions du Cloud Act est accordé aux autorités étrangères des gouvernements signataires de ces accords afin qu'elles puissent accéder aux données stockées aux Etats-Unis.

Les textes du Cloud Act, en plus d'avoir des effets sur les entreprises américaines et sur la confidentialité des données stockées par ces entreprises, ont des conséquences importantes sur les entreprises européennes et sur la protection des données au sens de l'Union européenne.

B. Les effets du Cloud Act sur les entreprises européennes :

Il convient dans un premier temps de comprendre la notion d'entreprise américaine selon les règles du Cloud Act avant de démontrer dans un deuxième temps les moyens de résistance des entreprises européennes puis d'évoquer dans un troisième temps les solutions envisagées par les entreprises européennes pour être en conformité avec les exigences des règles du Cloud Act.

[4] Au sens de droit américain : c'est-à-dire soit une procédure prévue par un Mutual Legal Assistance Treaty, les fameux MLAT, soit une commission rogatoire internationale.

1. Pourquoi les sociétés européennes sont concernées par le Cloud Act ?

La réponse à cette question se trouve dans les exigences du législateur américain et sa volonté d'étendre la force des lois américaines au-delà des frontières américaines pour que ses règles soient considérées comme des lois de police internationale, autrement dit pour que ses règles aient vocation à s'appliquer pour toute personne physique ou morale justiciable quelle que soit sa nationalité ou son pays de résidence. Cette vocation constitue ce qu'on appelle l'extraterritorialité des lois des Etats-Unis.

Dans cette perspective, le Cloud Act a fait référence à la notion d'entreprise américaine ou toute société incorporée aux Etats-Unis ; ce qui signifie que toute société qui travaille directement ou indirectement sur le sol américain avec des liens directs ou indirects avec les Etats-Unis, peut être sujet d'une demande des autorités américaines pour divulguer des données stockées par cette société pour le compte de ses clients.

Pour exemple, les sociétés visées par les autorités américaines dans le cadre d'une divulgation de données, peuvent être des fournisseurs d'accès à Internet, des banques, des sociétés d'assurance, des constructeurs automobiles, des fournisseurs de services de télécommunication, des sociétés fabricantes de systèmes d'alarmes ou de systèmes de programmation sur Internet, et également des sociétés (petites ou grandes) qui utiliseraient une adresse électronique hébergée chez un hébergeur américain, etc. Peu importe sa nationalité, la localisation géographique de son siège social, sa taille (petite ou grande), toute société peut entrer à un moment donné dans le champ d'application du Cloud Act.

Si toutefois, une société européenne ne souhaite pas répondre favorablement à la demande des autorités américaines, est-ce possible et par quel mécanisme ?

2. Comment une société européenne peut contester ou refuser d'accorder l'accès aux données dont elle dispose, aux autorités américaines ?

Les conditions d'opposition d'une entreprise européenne à l'autre sont différentes selon qu'il existe ou non un accord international entre les Etats-Unis et le pays de l'entreprise européenne dont la loi est susceptible d'être méconnue[5] :

a. Analyse de courtoisie[6] : en cas d'accord international entre les Etats-Unis et le pays en cause, la demande d'opposition doit être formée dans un délai de 14 jours devant la juridiction de première instance compétente ou devant la cour d'appel ou par voie d'action ou par voie

[5] Voir le paragraphe « ii » page 3.
[6] En anglais : Comity Analysis.

d'exception selon le cas. Cette requête doit montrer le caractère sérieux du risque de sanction auquel est exposée la société dans l'autre pays et l'intérêt qui s'attache, pour demander la modification ou l'annulation de la demande de l'autorité américaine. La cour américaine étudiera la proportionnalité de la demande en fonction des critères suivants : l'intérêt des Etats-Unis, notamment celui de l'entité cherchant à obtenir communication des informations litigieuses ; l'intérêt du gouvernement étranger de l'entreprise à empêcher la communication illégale selon sa législation, des informations litigieuses ; la localisation et la nationalité du client et la nature des connexions de ce client avec les Etats-Unis ; la nature des liens de la société avec les Etats-Unis ; l'importance des investigations menées et des informations dont la communication est demandée pour ces investigations ; les possibilités qu'a l'entité gouvernementale d'obtenir de manière tout aussi acceptable les informations demandées par des moyens présentant moins de conséquences négatives[7].

b. en l'absence d'un accord international, la société peut également refuser de communiquer les données sollicitées sur le fondement des *common law principles of comity*, c'est-à-dire sur le fondement du principe de courtoisie internationale reconnu par les juridictions américaines selon lequel, pour l'application du droit des Etats-Unis, il convient de tenir compte des intérêts importants des autres pays et, le cas échéant, ne pas appliquer ou appliquer de manière nuancée la législation américaine. A la différence de la procédure précédente, les critères que le juge devra utiliser pour se prononcer sur le bien-fondé d'une telle opposition ne sont pas précisés par la loi car elles sont jurisprudentielles.

3. RGPD ou Cloud Act, comment peut-on être Compliant ?

Selon l'article 48 du RGPD : « les demandes de données par un Pays tiers doivent être effectuées dans le cadre d'un accord international ». Aussi, en absence d'un accord entre l'Union Européenne et les Etats Unis, toute société européenne qui serait amenée à divulguer des données suite à une demande formulée par une autorité américaine, prendrait le risque d'être en infraction vis-à-vis des RGPD. La violation des règles du RGPD conduit à de lourdes amendes.

La solution "simple" de trouver un accord entre les Etats-Unis et l'Union Européen est loin d'être trouvée, surtout dans le contexte politique et économique actuel.

[7] Cette procédure d'opposition n'est pas applicable lorsque les données dont la communication est demandée concerne une United States Person, c'est-à-dire un citoyen des Etats-Unis, une personne admise à résidence permanente, une association non enregistrée dont un nombre important de membres sont des citoyens américains ou des personnes admises à résidence permanente, ou toute société enregistrée aux Etats-Unis.

Pourtant, pour les sociétés européennes, la question d'être en conformité avec les exigences des textes américains est une priorité absolue, vu les amendes énormes envisagées par les autorités américaines en cas d'infraction.

Pour certaines sociétés, telles que les fournisseurs de services de communication Internet, une mention légale dans les conditions générales expliquant la possibilité de divulgation des données en cas de demande formulée par les Etats-Unis, peut être la solution d'une exonération ou d'une limitation de responsabilité vis-à-vis des personnes concernées. Cette solution sera-t-elle acceptée par les institutions européennes ?

Quelques mois après la promulgation du Cloud Act et l'adoption du RGPD, des doutes subsistent en l'absence de cas pratiques. En attendant, les sociétés européennes doivent être vigilantes, et elles sont invitées à continuer de renforcer leurs systèmes de compliance avec toute régularité, précision et efficacité possibles.