FIDAL

CLOUD ACT : TOUJOURS DES INCERTITUDES NOTAMMENT VIS-A-VIS DU RGPD

I. L'incertitude des transferts de données vers les Etats-Unis en provenance de l'Union européenne avec le Cloud Act

En premier lieu, il revient d'analyser si cette loi pourrait remettre en cause les transferts de données à caractère personnel depuis l'Union européenne vers les Etats-Unis (fondés aujourd'hui sur l'accord « *Privacy Shield* ») ; autrement dit, si elle garantit un niveau de protection adéquat des données à caractère personnel communiquées aux autorités américaines au sens de la Cour de Justice de l'Union Européenne (CJUE).

On se souvient de l'arrêt *Schrems*[1] où la CJUE avait invalidée la décision du 26 juillet 2000 « *Safe Harbor* » car les autorités américaines, dans le cadre de leur programme de collecte de renseignements à grande échelle (PRISM), pouvaient intercepter de manière massive et indifférenciée des données transférées, sans garantir une protection juridique efficace aux personnes concernées.

Or, cette décision de la CJUE ne semble pas transposable à la procédure de communication de données prévue par le *SCA,* telle que modifiée par le *Cloud Act*.

En effet, le *SCA* prévoit que les autorités américaines peuvent requérir la communication de données de la part de prestataires de services électroniques dans le cadre d'une procédure judiciaire et, à cette fin, doivent obtenir un mandat (un « *warrant* ») conformément au Quatrième Amendement de la constitution des Etats-Unis (ce dernier protège le citoyen contre toutes perquisitions et saisies non motivées et prévoit qu'aucun mandat ne peut être délivré sans présomption sérieuse, ni sans qu'il indique le lieu ou les choses à saisir).

De surcroît, le prestataire de services électroniques peut contester dans un délai de 14 jours la demande de communication de données lorsqu'il estime que l'utilisateur n'est pas une personne américaine et ne réside pas aux Etats-Unis[2]ou que la demande de communication pourrait créer un risque de violation de « *laws of a qualifying foreign government* »[3].

Ce dernier critère signifie, le cas échéant, qu'il pourra être tenu compte du droit de l'Etat étranger dans une certaine mesure en vertu de 3 critères légaux :

- le prestataire viole le droit d'un Etat étranger,

[1] CJUE, 6 Oct. 2015, aff. C-362/14, Maximillian Schrems c/ Data Protection Commissioner.
[2] *Cloud Act*, 18 U.S.C. § 2703(h)(2)(i)
[3] *Cloud Act*, 18 U.S.C. § 2703(h)(2)(ii)

- l'utilisateur concerné n'est pas une personne américaine et ne réside pas aux Etats-Unis, et
- l'intérêt de la justice[4] (« *the interests of justice* ») justifie d'annuler ou de modifier la demande de communication de données (autrement dit, exercer une balance des intérêts entre ceux de l'Etat étranger et ceux des Etats-Unis).

A la différence de l'affaire *Schrems*, la communication des données est faite dans le cadre d'une procédure judiciaire (et non dans le cadre d'un programme de renseignement) et elle ne peut avoir lieu qu'après la délivrance d'un mandat judiciaire.

De même, dans cette affaire, la CJUE reprochait au programme de surveillance américain de ne pas prévoir « *pour les personnes concernées, de voies de droit administratives ou judiciaires permettant, notamment, d'accéder aux données les concernant et, le cas échéant, d'obtenir leur rectification ou leur suppression* ». Or, le *Cloud Act* prévoit précisément la possibilité d'exercer un recours judiciaire pour demander la modification ou l'annulation du mandat délivré.

Néanmoins, la CJUE exige, concernant le programme de surveillance américain, et conformément au principe de proportionnalité, que :

- les interceptions diligentées présentent « *un caractère ciblé* »,
- la surveillance « *soit objectivement justifiée dans l'intérêt de la sécurité nationale ou de la répression de la criminalité* » et,
- qu'il soit prévu « *des garanties adéquates et vérifiables* ».

Si le *Cloud Act* a pour objectif de protéger la sécurité publique et de lutter contre les infractions les plus graves[5], il ne prévoit pas de « *ciblage* » des données pouvant être communiquées. En effet, le *Cloud Act* à la lumière du Quatrième Amendement de la constitution américaine exige seulement que le mandat judiciaire soit justifié par des présomptions sérieuses et indique le lieu ou les choses (en l'occurrence, les données) à saisir ; l'étendue des saisies de communications de données reste alors à la discrétion du juge.

A moins qu'il faille opérer une distinction entre les saisies effectuées en matière de communication de données dans le cadre d'un programme de renseignement (sans intervention du juge) et celles effectuées dans le cadre d'une procédure judiciaire (avec intervention du juge), le *Cloud Act* parait ne pas répondre aux exigences posées par la CJUE.

[4] Le Cloud Act prévoit que l'intérêt de la justice doit être apprécié à l'aune de 8 critères légaux, par exemple, l'ampleur et la nature des liens et de la présence du prestataire avec les Etats-Unis, l'importance de l'information sollicitée pour les investigations, la localisation et la nationalité de la personne dont les données sont sollicitées ainsi que l'ampleur et la nature de ses liens avec les Etats-Unis etc.
[5] *Cloud Act*, 18 U.S.C. Sec. 2(1).

En outre, la possibilité d'exercer un recours est réservé aux prestataires de services électroniques qui doivent « *reasonably believes* »[6] que l'un des deux critères évoqués plus haut (à savoir, que l'utilisateur n'est pas une personne américaine et ne réside pas aux Etats-Unis ou que la demande de communication pourrait créer un risque de violation de « *laws of a qualifying foreign government* ») est satisfait.

Or, ce second critère s'applique lorsqu'un Etat étranger a conclu avec les Etats-Unis un accord bilatéral (un « *executive agreement* ») conformément aux conditions prévues par le *Cloud Act* (ce qui n'est pas actuellement le cas pour la France ou l'Union européenne).
En l'absence d'un tel accord, l'Etat étranger pourra seulement se prévaloir des principes de courtoisie internationaux (« *common law principles of comity* ») reconnus par la jurisprudence américaine ; dans une telle situation le respect des exigences de la CJUE est incertain au regard de la large marge d'appréciation dont dispose le juge américain.

Puis, on peut également douter de la conformité du recours judiciaire exercé par le prestataire de services électroniques au regard de l'arrêt *Schrems* rendu par la CJUE.

Selon elle, la possibilité d'exercer des voies de droit administratives ou judiciaires doit être reconnue aux « *personnes concernées* ».
En effet, le prestataire de services électroniques ne formule pas un recours au nom de la personne concernée mais dispose de sa propre marge d'appréciation puisqu'il doit lui seul raisonnablement penser que la demande de communication de données n'est pas justifiée (que se passera t-il en cas de désaccord entre la personne concernée et le prestataire ?).

De plus, le *Cloud Act* ravive les griefs présentés par le G29 au sujet de l'accord « *Privacy Shield* » dans son avis du 13 avril 2016 :

> « *Même si le G29 prend acte des possibilités nouvelles de recours offertes aux individus pour exercer leurs droits, il remarque que* ***ce mécanisme risque d'être complexe*** *en pratique et difficile à utiliser pour les personnes, notamment du fait qu'il ne s'exercerait* ***qu'en anglais*** *et qu'il pourrait, de ce fait, ne pas offrir une garantie effective. Des précisions doivent donc être apportées sur ces procédures de recours ; en particulier* ***les autorités nationales de protection des données qui le souhaitent devraient pouvoir servir de point de contact pour les citoyens européens et avoir la possibilité d'exercer les recours en leur nom***. ».

Bien que l'on ne connaisse pas encore les réponses que l'Union européenne entend apporter à cette nouvelle loi américaine, on peut penser que celle-ci pose avec encore plus d'acuité la

[6] Cloud Act, 18 U.S.C. § 2703(h)(2)

question du maintien de l'accord « *Privacy Shield* », le Parlement européen ayant dès juillet 2018 adopté une résolution[7] (non contraignante) exigeant la suspension de cet accord à compter du 1er septembre 2018.

Pour l'heure, et à titre préventif, il est donc recommandé aux entreprises transférant des données à caractère personnel relatives à des citoyens européens vers les Etats-Unis de ne pas se fonder sur l'accord « *Privacy Shield* » mais de privilégier les mesures prévues par le RGPD encadrant les transferts de données vers un pays tiers.

Rappelons, à ce titre, que les articles 44 et suivants du RGPD prévoient qu'un transfert de données à caractère personnel vers un pays tiers est possible, notamment, si le transfert :

- présente des garanties appropriées (au moyen de clauses contractuelles types), ou
- fait l'objet de règles d'entreprise contraignantes (les « *Binding Corporate Rules* »).

II. L'existence de mécanismes juridiques contrariant la mise en œuvre du Cloud Act

En second lieu, on peut craindre que l'effet extraterritorial du *Cloud Act* entre en conflit avec

- le Règlement Général sur la Protection des Données (RGPD) n°2016/679,
- la directive 2016/943 du 8 juin 2016 sur la protection des secrets d'affaires, et
- la loi française n° 68-678 du 26 juillet 1968 *relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.*

Tout d'abord, le RGPD prévoit en son article 48 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****, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre* ».

De ce fait, pour éviter que le *Cloud Act* entre en contradiction avec le RGPD, il est nécessaire qu'un accord international prévoie la possibilité pour l'autorité judiciaire américaine d'exiger la communication des données.

[7] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0315+0+DOC+XML+V0//FR

Or, l'accord « *Privacy Shield* » ne peut constituer un tel accord, son champ d'application étant limité aux seules sociétés américaines qui sur la base d'une auto-certification ont adhéré à cet accord ; cet accord ne concerne donc pas les institutions américaines (qu'il s'agisse de l'autorité judiciaire ou gouvernementale).

Force est de constater l'absence de prise en compte des exigences du RGPD par le *Cloud Act* alors que certains Etats aux Etats-Unis comme la Californie ont voté une loi en juin 2018 se rapprochant du niveau de protection garanti par le RGPD (par exemple, la personne concernée a le droit de connaître les données collectées sur elle, le droit de s'opposer à la vente de ses données personnelles ou encore le droit de supprimer ses données personnelles).

Puis, en l'absence d'accord international conclu entre les Etats-Unis et l'Union européenne (ou la France), le *Cloud Act* pourrait également se heurter à la récente directive 2016/943 du 8 juin 2016 sur la protection des secrets d'affaires ainsi qu'à sa loi de transposition en France en date du 30 juillet 2018[8] prévoyant en son article 1 que :

> « ***Le secret des affaires n'est pas opposable lorsque l'obtention, l'utilisation ou la divulgation du secret est requise ou autorisée par*** *le droit de l'Union européenne,* ***les traités ou accords internationaux*** *en vigueur ou* ***le droit national,*** *notamment dans l'exercice des pouvoirs d'enquête, de contrôle, d'autorisation ou de sanction des autorités juridictionnelles ou administratives.* »[9].

A contrario, cet article signifie qu'en l'absence d'accord ou traité international, les secrets d'affaires sont pleinement opposables aux autorités américaines.

Toutefois, ces dernières pourraient se prévaloir de l'une des dérogations concernant la protection des secrets d'affaires visée à l'article 5 b. de la directive 2016/943 ; en effet, les Etats membres veillent à ce qu'une demande consistant à réclamer l'application des « *mesures, procédures et réparations* » de ladite directive soit écartée si l'obtention, l'utilisation ou la divulgation des secrets vise à « *révéler une faute, un acte répréhensible ou une activité illégale, à condition que le défendeur ait agi dans le but de protéger l'intérêt public général* ».
Or, c'est précisément l'objectif poursuivi par le *Cloud Act* qui est de protéger la sécurité publique et de lutter contre les infractions les plus graves[10].

Enfin, en l'absence d'accord ou traité international, le *Cloud Act* pourrait se heurter à la loi française n° 68-678 du 26 juillet 1968 *relative à la communication de documents et*

[8] Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires.
[9] Art. L. 151-7 du Code de commerce.
[10] *Cloud Act*, 18 U.S.C. Sec. 2(1).

renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères.

Cette dernière prévoit aux articles 1 et 1 bis qu'il est interdit :

- « *à toute personne physique de nationalité française ou résidant habituellement sur le territoire français et à tout dirigeant, représentant, agent ou préposé d'une personne morale y ayant son siège ou un établissement* ***de communiquer*** *par écrit, oralement ou sous toute autre forme, en quelque lieu que ce soit,* ***à des autorités publiques étrangères****,* ***les documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public,*** *précisés par l'autorité administrative en tant que de besoin* » ;
- « *à toute personne de demander, de rechercher ou* ***de communiquer****, par écrit, oralement ou sous toute autre forme,* ***des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères*** *ou dans le cadre de celles-ci.* ».

En cas de non-respect de l'une des ces dispositions, la sanction encourue est une peine d'emprisonnement de six mois et d'une amende de 18 000 euros ou de l'une de ces deux peines seulement.

Toutefois, cette loi est peu usitée par les entreprises, soit par simple ignorance de son existence, soit par crainte de se mettre en porte-à-faux vis-à-vis de la justice américaine.

D'ailleurs, le Gouvernement a manifesté sa volonté de moderniser cette loi dit de « *blocage* » avec la future loi PACTE (Plan d'Action pour la Croissance et la Transformation des Entreprises), actuellement en cours d'adoption devant l'Assemblée Nationale et le Sénat.