Every Cloud Has a Silver Lining : Une analyse contextualisée de l'extraterritorialité du Cloud Act

Régis Bismuth

Every Cloud Has a Silver Lining : Une analyse contextualisée de l'extraterritorialité du Cloud Act

Régis Bismuth
Professeur à l'École de Droit de Sciences Po

Publié in
JCP(E), 2018, n° 40, p. 35-47

Résumé : Le Congrès américain a adopté en mars 2018 le *Clarifying Lawful Overseas Use of Data Act* (Cloud Act) qui encadre l'accès par les autorités américaines aux données stockées à l'étranger par les prestataires de services électroniques dans le cadre de procédures pénales. S'il a été vilipendé pour son extraterritorialité, il s'avère qu'une analyse attentive de cette loi, notamment en ce qu'elle permet de tenir compte des exigences des droits étrangers, conduit à nuancer les positions radicales jusqu'alors exprimées. Ce dispositif doit aussi être évalué à l'aune de la proposition de la Commission européenne d'avril 2018 de règlement « E-evidence » qui repose sur des mécanismes similaires. Il en ressort que le Cloud Act, combiné aux initiatives européennes, permet d'envisager un cadre coopératif UE/États-Unis qui poserait les jalons d'un droit global de l'accès aux preuves électroniques.

1. – Introduction

« *A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States* »[1]. La première disposition du *Clarifying Lawful Overseas Use of Data Act* (Cloud Act) promulgué par le président américain le 23 mars 2018[2] donne la possibilité aux autorités américaines, dans le cadre d'une procédure pénale, d'exiger des prestataires de services électroniques la divulgation de données quel que soit le lieu où se situent les serveurs sur lesquels elles sont stockées. S'agit-il d'un nouveau dispositif extraterritorial par le biais duquel les États-Unis imposent de manière invasive et brutale leur droit au reste du monde en faisant peu de cas de la souveraineté des autres États et de la protection des libertés individuelles ?

La presse a relayé à ce propos des messages alarmistes[3]. C'est sans surprise que le *Canard Enchaîné* annonçait que le Cloud Act « permet aux États-Unis de pomper – à notre insu – tous nos secrets stockés sur Internet »[4]. Annonciateur du même péril, un sénateur français interrogeait le gouvernement sur les initiatives susceptibles d'être prises en réponse à « cette loi [qui] marque un recul sans précédent tant du point de vue des libertés que du point de vue

[1] 18 U.S.C. § 2713. (Nous soulignons).
[2] Le Cloud Act est la section V du *Consolidated Appropriations Act* de 2018 (H.R. 1625, Pub.L. 115-141).
[3] V. par ex., « "Cloud Act" : Malgré le RGPD, les États-Unis à l'assaut de vos données personnelles », *Marianne.fr*, 19 juin 2018.
[4] *Le Canard Enchaîné*, n° 5092, 30 mai 2018.

du droit international »[5]. Certains dénonçaient aussi « une ingérence juridique jamais vue »[6] ou un « nouvel instrument de guerre économique renforçant l'ingérence des autorités américaines sur les prestataires de services de communication électroniques américains »[7].

Une analyse du Cloud Act conduit toutefois à nuancer les positions radicales jusqu'alors exprimées. Cette législation ne peut être réduite à un dispositif extraterritorial et n'a pas été conçue afin de donner la possibilité aux autorités américaines de siphonner les données personnelles sans contrôle ni limite. D'ailleurs, certains de ses mécanismes sont similaires à ceux envisagé par la Commission européenne dans sa proposition d'avril 2018 de règlement relatif à l'accès aux preuves électroniques en matière pénale (projet de règlement « E-evidence »)[8], une sorte de Cloud Act à l'échelle de l'UE qui produit également des effets extraterritoriaux[9].

Si plusieurs critiques méritent d'être formulées à l'endroit du Cloud Act, il faut se garder d'un catastrophisme stérile. Cette législation inclut certaines garanties de même qu'elle constitue, à condition d'être exploitée, une base intéressante de développement de la coopération internationale en matière d'accès aux preuves numériques. Ce n'est pas tant une analyse littérale du texte qui doit être opérée mais davantage une tenant compte du contexte plus large dans lequel il s'inscrit, qu'il soit technologique, normatif ou institutionnel.

S'il convient dans un premier temps de rappeler le contexte dans le cadre duquel le Cloud Act a été adopté (2), l'analyse de cette législation montre qu'il faut réévaluer la dimension extraterritoriale de cette législation en tenant compte de la spécificité de l'accès aux preuves numériques, domaine dans lequel le principe de territorialité perd de sa pertinence (3). Elle analyse montre également que le champ d'application personnel du Cloud Act pourrait aussi concerner des prestataires qui ne sont ni des sociétés américaines ni leurs filiales à l'étranger (4). Il faut noter également que le Cloud Act laisse un rôle important au juge dans le cadre de la production du titre exigeant la communication sollicitée par les autorités (5) et aussi pour modérer les effets extraterritoriaux de certaines demandes (6) qui peuvent présenter un risque de conflit avec un droit étranger (7). L'analyse du Cloud Act, jointe à celle de la proposition de règlement E-evidence, conduit à penser qu'un accord États-Unis/UE permettant d'intégrer les exigences découlant du droit de l'UE constituerait un cadre coopératif utile et intéressant permettant de poser les jalons d'un droit global de l'accès aux preuves numériques (8).

2. – Le Cloud Act : Une conséquence de l'affaire *Microsoft v. United States*

La recherche de preuves électroniques stockées sur des serveurs localisés à l'étranger ouvre la voie à deux possibilités pour les autorités. Il peut être envisagé, outre les commissions rogatoires internationales, d'emprunter les voies prévues par les traités d'entraide judiciaire (*mutual legal assistance treaties* ou MLAT) en demandant aux autorités de l'État étranger sur le territoire duquel les données sont stockées de solliciter leur divulgation auprès du prestataire concerné. Les procédures MLAT peuvent toutefois être longues et manquer de souplesse

[5] Question écrite n° 5765 de M. Pierre Laurent, *JO Sénat*, 21 juin 2018, p. 3052.
[6] L. Ackerman, « Cloud Act, L'offensive américaine pour contrer le RGPD », 22 juin 2018, <https://portail-ie.fr>.
[7] O. Dorgans, « Le Cloud Act : Nouvel instrument de guerre économique renforçant l'ingérence des autorités américaines sur les prestataires de services de communication électroniques américains », *Revue Internationale de la Compliance et de l'Éthique des Affaires*, n° 26, 2018, p. 24 et s.
[8] Commission européenne, Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM(2018) 225 final, 17 avril 2018.
[9] S. Peyrou, « *Le projet de règlement "E-evidence" (preuves électroniques) présenté par la Commission européenne : Un "Cloud Act" européen* », 24 avril 2018, <http://www.gdr-elsj.eu>.

lorsqu'il s'agit de collecter des preuves pour une procédure pénale. Il n'est donc pas surprenant que les autorités préfèrent parfois requérir directement ces données auprès des prestataires. C'est le recours à cette dernière possibilité par les autorités américaines qui a été au cœur de l'affaire *Microsoft v. United States*.[10]

Cette affaire trouve son origine dans un mandat (*warrant*) émis par le *Department of Justice* à destination de Microsoft afin que cette société communique aux autorités des informations associées au compte email d'une personne suspectée de trafic de stupéfiants. La demande était fondée sur le *Stored Communications Act* (SCA) encadrant la divulgation de données électroniques aux autorités dans le cadre d'une procédure pénale[11]. Le SCA avait été adopté en 1986 et n'envisageait pas l'accès à des données stockées sur des serveurs à l'étranger.

La société Microsoft exécuta le mandat pour ce qui concerne les informations stockées sur des serveurs localisés sur le territoire américain. Elle déclina de divulguer celles stockées dans son *data center* en Irlande, soulignant qu'il ne pouvait être conférée une portée extraterritoriale au mandat.

Un juge fédéral saisi en première instance confirma la légalité du mandat[12]. Cette décision fut contestée devant la Cour d'appel du 2nd circuit qui, dans une décision de 2016, annula l'ordonnance précédente et fit droit aux positions de Microsoft. La juridiction considéra que le SCA ne pouvait revêtir une portée extraterritoriale et que la question décisive était celle de la localisation des données et pas celle de la possibilité pour Microsoft d'accéder à ces données depuis le territoire américain[13]. Après un refus de la même cour d'appel de réexaminer l'affaire dans sa composition plénière (*rehearing en banc*)[14], le gouvernement américain porta l'affaire devant la Cour suprême qui accepta d'instruire ce contentieux en octobre 2017.

La position de la cour d'appel divergeait de celles, postérieures, d'autres juridictions de première instance, notamment dans des affaires visant Google et Yahoo[15]. Cette situation générait une incertitude et une décision défavorable de la Cour suprême était susceptible d'affecter l'efficacité des procédures pénales, même dans des cas où les faits se sont produits aux États-Unis ou impliquent des américains[16]. Le Congrès a ainsi souhaité adopter le Cloud Act avant l'issue de la procédure dans l'affaire *United States v. Microsoft*. Il a ainsi été élaboré dans la précipitation, sans débat, et intégré comme un cavalier législatif dans la loi de finances

---

[10] Sur cette affaire, v. R. J. Currie, « Cross-Border Evidence Gathering in Transnational Criminal Investigation : Is the *Microsoft Ireland* Case the "Next Frontier" ? », *Canadian Yearbook of International Law*, vol. 54, 2017, p. 63 et s. ; T. Christakis, *Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques*, CEIS, The Chertoff Group, 2017, p. 18 ; P. Jacob, « Quand les nuages ne s'arrêtent pas aux frontières – Remarques sur l'application du droit dans l'espace numérique à la lumière du Cloud Act », *Cahiers de Droit de l'Entreprise*, 2018, n° 4, p. 35.

[11] 18 U.S.C. § 2703.

[12] *In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

[13] *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016) ; v. *Harvard Law Review*, vol. 130, 2016, pp. 769-776.

[14] *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft*, 855 F.3d 53 (2d Cir. 2017).

[15] *In the Matter of Search of Content that is Stored at Premises Controlled by Google*, 2017 WL 1487625 (N.D. Cal. 2017) ; *In re Information Associated with One Yahoo Email Address That Is Stored at Premises Controlled by Yahoo*, 2017 WL 706307 (E.D. Wis. 2017) ; *In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564 (E.D. Pa. 2017) ; *In the matter of the search of premises located at: [redacted]@yahoo.com, stored at premises owned, maintained, controlled, or operated by Yahoo, Inc.*, Case No. 6:17-mj-1238 (M.D. Fla. 2017).

[16] V. l'audition devant un comité du Sénat de Brag Wiegmann (Deputy Assistant Attorney General) qui expose les difficultés résultant de la décision de la Cour d'appel du 2nd circuit (24 mai 2017, <https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Wiegmann%20Testimony.pdf>).

de 2018. En établissant une procédure claire permettant de solliciter auprès du prestataire la communication de données quelle que soit leur localisation, la promulgation du Cloud Act a permis aux autorités d'émettre un nouveau mandat, ce qui a conduit la Cour suprême à mettre fin à l'instance en avril 2018 alors qu'une décision était attendue quelques semaines plus tard[17].

3. – Une extraterritorialité du Cloud Act à reconsidérer au regard de la spécificité des preuves électroniques

Alors que le SCA était silencieux quant à sa portée territoriale, le Cloud Act corrige cette ambigüité et indique que peuvent être ciblées les données « *whether such communication, record, or other information is located within or outside of the United States* »[18]. Cette possible portée extraterritoriale mérite d'être nuancée lorsque l'on examine de plus près certains aspects d'ordre technologique et l'intention des autorités à l'origine de telles demandes.

Lorsque, dans le cadre d'enquêtes pénales, la divulgation de données électroniques d'une personne est sollicitée auprès des prestataires, le lieu de stockage des données (parfois fragmentées et dispersées sur des serveurs localisés dans des États différents) est généralement inconnu des autorités. La territorialité des données est le plus souvent déconnectée de la réalité des relations sociales dans le cadre desquelles ces données sont générées et exploitées. Il n'y a à l'origine pas d'intention extraterritoriale dans la démarche des autorités consistant à les solliciter.

L'intention extraterritoriale pourrait être caractérisée à la suite d'un examen de certains aspects de l'infraction poursuivie (concerne-t-elle des faits s'étant déroulés sur le territoire de cet État ? Concerne-t-elle des ressortissants ou des résidents de cet État ?). Il faut distinguer, d'une part, la conduite litigieuse qui fait l'objet des poursuites et qui doit avoir un lien avec l'État exerçant sa compétence pénale et, d'autre part, les données permettant de caractériser les faits constitutifs de l'infraction.

Si la localisation du stockage des données peut parfois être choisie par l'utilisateur, elle est le plus souvent décidée par le prestataire selon un ensemble de processus algorithmiques. Les prestataires ne peuvent installer des *data centers* dans chaque État et leur localisation dépend d'une série de contraintes techniques ou économiques. Par exemple, les États où l'électricité est d'un plus faible coût pourront être privilégiés. Les données sont parfois dupliquées et stockées sur des serveurs différents afin de les préserver[19].

Cette répartition spatiale presque aléatoire des données a donné lieu à des difficultés aux autorités américaines lorsqu'il s'agissait par exemple de collecter des informations dans des affaires d'exploitation sexuelle de mineurs ou de pédopornographie visant des résidents américains : de nombreux contenus n'avaient pu être divulgués par les prestataires car les fichiers photo et video étaient stockés à l'étranger[20]. Il s'est aussi avéré que des prestataires stockaient le contenu du texte de courriels d'utilisateurs américains sur des serveurs localisés aux États-Unis alors que les pièces jointes l'étaient sur des serveurs situés à l'étranger[21]. On comprend la complexité des démarches devant être entreprises s'il fallait déclencher plusieurs procédures MLAT pour obtenir la divulgation de courriels d'un résident américain suspecté d'infraction.

Il faut aussi envisager la situation des États qui n'hébergent pas de *data centers* de certains prestataires de dimension globale. Google dispose par exemple de huit *data centers*

---

[17] *United States v. Microsoft Corp.*, No. 17–2, 584 U. S. ___ (2018).
[18] 18 U.S.C. § 2713.
[19] T. Christakis, *op. cit.* note 10, p. 25 et s.
[20] B. Wiegmann, *op. cit.* note 16, p. 5-6.
[21] *Ibid.*, p. 4.

aux États-Unis, quatre en Europe, deux en Asie et un au Chili[22]. Un utilisateur de Google résidant sur le continent africain, en Inde ou au Brésil ne peut avoir ses données stockées dans son État de résidence. Un État souhaitant y accéder dans le cadre d'une procédure pénale serait obligé d'activer des procédures MLAT avec plusieurs États si l'on s'en tient au seul critère formel du lieu de stockage des données. Il en découlerait une inégalité entre États difficilement justifiables : ceux sur le territoire desquels sont localisés les serveurs des principaux prestataires de services auraient en pratique davantage la possibilité d'obtenir la communication des données tandis que les autres devraient emprunter des procédures plus longues qui entravent l'efficacité de leur justice. De la fracture numérique découlerait donc une fracture juridique.

A cette aune, deux constats peuvent être réalisés quant à l'extraterritorialité du Cloud Act.

En premier lieu, ce sont les critères de compétence utilisés par le juge pénal américain quant à l'infraction poursuivie qui constituent un filtre permettant de neutraliser une éventuelle extraterritorialité. Dans l'hypothèse d'un américain poursuivi pour des infractions commises aux États-Unis et ayant une partie de ses emails stockés par Google sur le site de Hamina en Finlande, on ne peut raisonnablement dire que la démarche des autorités américaines consistant à solliciter ces données auprès de Google constituerait un assaut manifeste à l'endroit de la souveraineté territoriale de la Finlande – tout en ne négligeant pas évidemment les impératifs découlant du RGPD qui doivent être pris en compte.

De même, pour montrer que le lieu de stockage « *irrelevant* »[23], on peut retenir l'hypothèse d'un français poursuivi aux États-Unis pour des actes commis en France et dont une partie des emails est stockée dans le data center de Google à Singapour ou, en allant plus loin dans l'absurde, dans un espace international tel que la Haute mer, si cela était possible. En retenant le lieu de stockage, on pourra certes gloser sur l'atteinte à la souveraineté de Singapour ou s'inquiéter du regard torve des grands requins blancs mais l'atteinte à la souveraineté française et le droit à la protection des données personnelles de ce ressortissant français resteront dans un angle mort du débat.

Il faut relever que le Cloud Act permet de tenir compte à la fois des liens de rattachement de la personne visée avec le forum américain (est-elle américaine ou réside-t-elle aux États-Unis ?)[24], des intérêts de l'État où les données sont stockées et, plus généralement, de l'ensemble des obligations légales qui pèsent sur les prestataires – par exemple celles du RGPD. Le Cloud Act permet ainsi d'intégrer une analyse plus subtile et substantielle afin de tenir compte des situations où se déploierait une extraterritorialité qui pourrait être problématique.

Le second constat est que la configuration actuelle du stockage des données par des prestataires opérant dans une logique transnationale rend incontournable la mise en place d'une procédure où ceux-ci sont les points de contact privilégiés pour répondre directement aux demandes, charge aux prestataires de les administrer en intégrant les contraintes réglementaires qui pèsent sur eux. C'est le modèle du Cloud Act et c'est aussi celui de la Commission européenne dans sa proposition de règlement E-evidence qui instaurerait une injonction européenne de production et de conservation de données dirigées directement vers un prestataire offrant des services dans l'Union, sans avoir à passer par les procédures MLAT[25].

Ce modèle implique une responsabilisation des prestataires et c'est pourquoi le Cloud Act a suscité certaines craintes. Le Cloud Act donne la possibilité aux gouvernement américain

---

[22] Liste consultable au lien suivant : <https://www.google.com/about/datacenters/inside/locations>.
[23] P. S. Berman, « Legal Jurisdiction and the Derritorialization of Data », *Vanderbilt Law Review*, vol. 71, 2018, p. 23.
[24] Critère pouvant être pris en compte lorsqu'il existe un accord avec un État étranger. 18 U.S.C. §2713(h)(2)(i).
[25] V. les articles 4 à 12 de la proposition de règlement E-evidence (*op. cit.* note 8).

de conclure des accords intergouvernementaux (*executive agreements*) permettant aux autorités étrangères de solliciter des informations détenues par des prestataires américains. Celles-ci pourront s'affranchir du filtre constitué par les procédures MLAT et placent les prestataires en première ligne. Qu'adviendrait-il si un gouvernement étranger répressif demandait la divulgation des emails d'un journaliste qu'il souhaite bâillonner ? Les prestataires de taille plus modeste disposeront-ils de l'expertise nécessaire afin d'évaluer le bien-fondé des demandes ? Le problème a été soulevé par certaines ONG américaines s'intéressant à la liberté de la presse[26]. Il devrait-être traité au moment de la négociation des accords intergouvernementaux et le Cloud Act prévoit d'ailleurs que de tels accord sont envisageables seulement avec les États étrangers dont le droit « *affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection* »[27].

Au demeurant, un problème similaire se pose pour projet E-evidence par le biais duquel les autorités de tous les États membres – y compris celles en délicatesse avec la liberté de la presse – auront la possibilité de solliciter la divulgation des données des utilisateurs auprès des prestataires. Un droit de recours pourra certes être exercé par la personne dont les données sont requises mais celle-ci pourra ne pas être tenue informée pendant un certain temps de la mesure la visant[28], affectant ainsi l'utilité et l'effectivité d'un tel recours.

4. – Un champ d'application personnel du Cloud Act potentiellement large

Le champ d'application personnel du Cloud Act demeure incertain mais pourrait s'avérer potentiellement large. Ce n'est que dans l'exposé des motifs de la loi qu'il est fait référence aux « *communications-service providers that are subject to the jurisdiction of the United States* »[29]. Le texte n'utilise quant à lui que l'expression « *provider of electronic communication service or remote computing service* ». Cela mérite d'être précisé lorsque l'on sait que des extraterritoriaux américains (par exemple en matière de sanctions) n'apportent pas de précision sur les limites de leur champ d'application personnel afin de bénéficier d'une marge de manœuvre lors de leur mise en œuvre[30].

L'expression « *subject to the jurisdiction of the United States* » laisse d'ailleurs aussi une certaine latitude aux autorités. Le *Code of Federal Regulations* inclut dans la catégorie « *Person subject to the jurisdiction of the United States* » les sociétés instituées en vertu du droit américain[31] ainsi que leurs filiales[32]. Cela signifie donc que les filiales européennes des géants américains de l'internet (Google, Microsoft, etc.) entrent en tout état de cause dans le champ d'application personnel du Cloud Act.

La question peut aussi se poser pour les sociétés établies en Europe qui ont une filiale aux États-Unis de même que celles qui n'ont pas de filiales mais qui y conduisent des activités. En effet, une « *Person subject to the jurisdiction of the United States* » peut aussi être « *Any person actually within the United States* »[33], étant entendu que le terme « *person* » désigne tout autant « *an individual, partnership, association, corporation, or other organization* »[34]. Si une

---

[26] P. Sterne & C. Fassett, « The Cloud Act : A Danger to Journalists Worldwide », *Freedom of the Press Foundation*, 22 mars 2018, <https://freedom.press>.
[27] 18 U.S.C. §2523(b)(1).
[28] Article 11(2) de la proposition de règlement E-evidence (*op. cit.* note 8).
[29] Cloud Act, Sec. 102(2).
[30] Sur ces aspects, v. R. Bismuth, « Pour une appréhension nuancée de l'extraterritorialité du droit américain », *AFDI (2015)*, vol. LXI, 2016, p. 785 et s.p. 792 et s.
[31] 31 C.F.R. §515.329(c).
[32] 31 C.F.R. §515.329(d).
[33] 31 C.F.R. §515.329(d) et 31 C.F.R. §515.330(a)(2).
[34] 31 C.F.R. §515.308.

entreprise non américaine offre depuis l'étranger des services électroniques ciblés vers le marché américain (par exemple en ayant recours à de la publicité sur des sites américains – on peut ici parler de focalisation ou de « *purposeful availment* »), les autorités pourraient la considérer comme étant « *within the United States* ».

Cela est d'ailleurs suggéré par d'autres dispositions du Cloud Act. Celui-ci permet aux autorités dans certaines situations (en présence d'un *executive agreement* conclu avec un État étranger) de demander à un prestataire, y compris « *a foreign electronic communication service or remote computing service* »[35], de contester une demande communication de données dont il est le destinataire et qui a été formulée par les autorités. Les juridictions doivent dans ce cadre suivre une *comity analysis* en tenant compte de plusieurs critères dont « *the nature and extent of the provider's ties to and presence in the United States* »[36]. Le texte n'envisage donc pas seulement une dichotomie parfaite entre prestataires américains et étrangers, mais davantage plusieurs nuances permettant de caractériser un certain degré de rattachement d'un prestataire avec le forum américain.

Il n'est donc pas exclu que des prestataires se considérant exclusivement européens puissent entrer dans le champ d'application du Cloud Act et être visés par des demandes des autorités américaines dès lors qu'ils présentent des éléments de connexité avec le forum américain[37]. Au demeurant, il serait surprenant que les États-Unis se limitent aux seules entreprises américaines et à leurs filiales, ce qui permettrait de contourner aisément le Cloud Act. Ce sera davantage la pratique des autorités qui devrait déterminer les limites du champ d'application personnel de cette législation. Il est donc risqué de considérer qu'opérer seulement avec des prestataires exclusivement implantés dans l'UE permet d'être immunisé du Cloud Act. Afin de ne pas être atteint par cette législation, ces prestataires devraient également s'isoler radicalement du marché américain.

La proposition de règlement E-evidence procède de la même démarche. Le texte indique qu'il « s'applique aux fournisseurs de services qui proposent des services dans l'Union »[38]. Son champ d'application personnel n'est donc pas limité aux seuls prestataires établis dans l'Union ou leurs filiales à l'étranger. D'ailleurs, la proposition envisage la situation où le prestataire étranger se placerait dans un conflit d'obligation lorsqu'une législation étrangère lui interdirait la communication des informations sollicitées[39]. Aussi, en imposant une obligation aux fournisseurs étrangers qui proposent des services dans l'UE d'y désigner un « représentant légal » vers lequel les demandes seront dirigées[40], ce dispositif créerait de toutes pièces un élément de rattachement territorial n'existant pas à l'origine et va en ce sens plus loin que le Cloud Act. Belle astuce pour ne pas être taxé d'extraterritorialité !

5. – Le rôle du juge dans le traitement des demandes formulées dans le cadre du Cloud Act : La production du titre exigeant la communication

Le Cloud Act ne consacre pas un droit immédiat d'accès aux données conservées par les prestataires au bénéfice des autorités exécutives américaines. Le titre par le biais duquel la

---

[35] 18 U.S.C. § 2703(h)(2)(A).
[36] 18 U.S.C. § 2703(h)(3)(E).
[37] En ce sens, v. R. Cheng, « Seizing Data Overseas from Foreign Internet Companies under the CLOUD Act », *Forbes.com*, 29 mai 2018.
[38] Article 3(1) de la proposition de règlement E-evidence (*op. cit.* note 8).
[39] V. *infra* n° (7).
[40] V. l'article 3 de la Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, COM(2018) 226 final, 17 avril 2018.

communication des données est demandée requiert l'intervention du juge ou est soumis à son contrôle[41].

Pour solliciter la communication de certaines données, l'autorité exécutive doit se prévaloir d'un titre dont la nature diffère en fonction de la nature des données sollicitées, principalement selon qu'il s'agit de données de contenu (par exemple le contenu d'un email ou une photo) ou de métadonnées (par exemple les informations relatives aux horaires de connexion).

Les données de contenu entrent dans le champ d'application du 4ème amendement de la Constitution américaine qui protège les citoyens contre les « *unreasonable searches and seizures* » (perquisitions et saisies non motivées). Ces données ne peuvent être sollicitées qu'en vertu d'un *warrant* (mandat) émis par une juridiction à certaines conditions (présomption sérieuse de réalisation de l'infraction, spécification des informations recherchées, etc.)[42]. Elles peuvent l'être aussi en vertu d'un *court order* (ordonnance) qui ne peut être émis que si les informations « *are relevant and material to an ongoing criminal investigation* »[43]. Dans les deux cas, le titre est délivré par un juge indépendant.

Selon la jurisprudence fédérale, les données de contenu ne peuvent être communiquées sur le fondement d'une simple *subpoena* (assignation) qui ne permet pas de garantir les exigences du 4ème amendement[44]. Il est utile de souligner que le récent arrêt de la Cour suprême des États-Unis *Carpenter v. United States* de juin 2018 a précisé que les données de géolocalisation produites par un téléphone portable (qui ne sont donc pas strictement des données de contenu) constituent néanmoins des informations protégées par le 4ème amendement, ne peuvent donc être exigées sur le fondement d'une *subpoena* et requièrent la production d'un mandat[45].

A titre de comparaison, le projet de règlement E-evidence indique qu'une injonction européenne de production pour les données relatives au contenu peut être émise par « (a) un juge, une juridiction ou un juge d'instruction compétents dans l'affaire concernée ; ou (b) toute autre autorité compétente telle que définie par l'État d'émission [et que cette] est validée, après examen de sa conformité aux conditions d'émission d'une injonction européenne de production […] par un juge, une juridiction ou un juge d'instruction dans l'État d'émission »[46]. L'autorité de poursuite aura la possibilité d'administrer les demandes de production des métadonnées dans le cadre de ces futures injonctions européennes[47]. Le cadre américain et le futur cadre européen présentent donc plusieurs similarités.

En somme, le Cloud Act ne permet pas aux autorités américaines de siphonner, et ce, à grande échelle via un clic de souris, les données localisées à l'étranger. Si l'on comprend les angoisses que peuvent susciter des précédents sérieux comme l'affaire Snowden, il serait caricatural de mettre en équivalence le Cloud Act avec les programmes de surveillance de la National Security Agency (NSA) tels que PRISM ou XKeyscore[48].

---

[41] V. aussi, E. Mignon & S. Dumontel, « Faut-il avoir peur du Cloud Act ? », 25 juin 2018, <https://www.august-debouzy.com/fr/blog/1193-faut-il-avoir-peur-du-cloud-act>.
[42] 18 U.S. Code § 2703(a), (b) et (c).
[43] 18 U.S. Code § 2703(d).
[44] *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).
[45] *Carpenter v. United States*, 585 U.S. ___ (2018).
[46] Article 4(2) de la proposition de règlement E-evidence (*op. cit.* note 8).
[47] Article 4(1) de la proposition de règlement E-evidence (*op. cit.* note 8).
[48] W. Maxwell, « Le Cloud Act américain ne permet pas d'espionner les entreprises européennes », <https://www.eurocloud.fr/le-cloud-act-americain-ne-permet-pas-despionner-les-entreprises-europeennes>.

6. – La possible modération par le juge des effets extraterritoriaux du Cloud Act (en présence et en l'absence d'un *executive agreement*)

Les prestataires de service peuvent s'opposer aux demandes de divulgation de données formulées par les autorités américaines, en particulier lorsque cela impliquerait pour eux de violer un droit étranger – les prestataires faisant face à deux obligations contradictoires. Cette question avait été au cœur des débats de l'affaire *United States v. Microsoft*[49]. Il faut néanmoins envisager deux situations en fonction de la conclusion ou non d'un accord international sur l'accès aux données avec l'État étranger.

Le Cloud Act donne la possibilité à un prestataire de contester dans un délai de 14 jours la demande de divulgation dès lors que celui-ci considère (i) que l'utilisateur concerné n'est pas une personne américaine et ne réside pas aux Etats-Unis et (ii) que cette communication « *would create a material risk that the provider would violate the laws of a qualifying government* »[50] – un *qualifying government* étant défini comme un État ayant conclu un *executive agreement* avec le gouvernement américain en conformité avec les conditions fixées par le Cloud Act[51]. Il faut à ce stade préciser dans quelle mesure les exigences des droits étrangers peuvent être prises en compte. La législation liste les trois conditions : (1) le prestataire est en situation de violer le droit de l'État étranger, (2) l'intérêt de la justice (« *the interests of justice* ») exigent d'annuler ou de modifier la demande des autorités et (3) l'utilisateur concerné n'est pas une personne américaine et ne réside pas aux États-Unis[52].

Afin de caractériser cet « intérêt de la justice », en d'autres termes, effectuer une balance entre les intérêts des États-Unis et ceux d'autres juridictions, le Cloud Act mentionne huit éléments[53], lesquels traduisent une « *comity analysis* » existant déjà en droit américain. Ces critère sont : (1) les intérêts des États-Unis, y compris ceux de l'autorité américaine sollicitant l'information, (2) les intérêts de l'État étranger au non-dévoilement de l'information, (3) la probabilité, l'ampleur et la nature des sanctions auxquelles s'exposent les prestataires ou leurs employés, (4) 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 États-Unis et l'État étranger, (5) l'ampleur et la nature des liens et de la présence du prestataire avec les États-Unis, (6) l'importance de l'information sollicitée pour les investigations, (7) la possibilité d'obtenir l'information par des moyens qui seraient moins dommageables et, cas plus particulier, (8) les intérêts de l'autorité d'un État tiers qui a sollicité les informations auprès des États-Unis dans le cadre de la coopération internationale en matière pénale.

En l'absence d'*executive agreement* conclu entre les États-Unis et l'État étranger, l'analyse des juridictions américaines ne serait pas fondamentalement différente[54] et, d'ailleurs, le Cloud Act indique que les « *common law standards governing the availability or application of comity analysis* » restent applicables[55]. La *comity analysis* déclinée dans le Cloud Act se retrouve dans la jurisprudence fédérale, en particulier la décision *Aérospatiale* de la Cour suprême qui concernait la possibilité de solliciter des informations sans passer par les procédures de la Convention de La Haye de 1970 sur l'obtention de preuves à l'étranger en matière civile ou

[49] T. Christakis, *op. cit.* note 10, p. 32 et s.
[50] 18 U.S.C. § 2703(h)(2)(ii).
[51] 18 U.S.C. § 2703(h)(1)(A)(i).
[52] 18 U.S.C. § 2703(h)(2)(B).
[53] 18 U.S.C. § 2703(h)(3).
[54] P. Jacob, *op. cit.* note 10.
[55] Cloud Act, Sec. 6.

commerciale[56]. En écartant les procédures coopératives internationales, les juridictions doivent tenir compte des principes d'*international comity* qui exigent « *a particularized analysis of the respective interests of the foreign nation and the requesting nation* »[57]. Dans le sillage de la jurisprudence *Aérospatiale*, les juridictions ont mis en œuvre une analyse multi-factorielle tenant compte notamment des intérêts essentiels des États intéressés par la procédure, de la nature et de l'ampleur des sanctions auxquelles s'expose la personne ou entité qui dévoile les informations sollicitées, de la mesure dans laquelle la communication requiert une intervention sur le territoire de l'État étranger ainsi que la nationalité de la personne visée dans le cadre de la procédure[58].

7. – Les règles de droit étranger susceptibles de faire obstacle aux demandes formulées dans le cadre du Cloud Act

La similarité des critères retenus dans le Cloud Act et ceux de la jurisprudence conduit à envisager les règles de droit étranger que le prestataire de services pourrait violer en accédant à une demande de communication de données formulée par les autorités américaines.

Du point de vue du droit français, on peut brièvement mentionner la loi de blocage du 26 juillet 1968 qui, sous réserve des accords internationaux, interdit notamment, sous peine de sanctions, à toute société ayant son siège ou un établissement en France de communiquer à des autorités publiques étrangères « 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 »[59]. Un prestataire de services pourrait dès lors l'invoquer devant les juridictions américaines. Celles-ci avaient dans un premier temps refusé d'en tenir compte car la méconnaissance de cette loi n'entrainait aucune poursuite[60]. Des décisions plus récentes, postérieures à des sanctions prononcées en France, les ont conduites à revoir leur position en intégrant les exigences de la loi française, notamment en s'employant à renvoyer dans un premier temps les requérants vers procédures coopératives internationales[61]. La loi de blocage du 26 juillet 1968 pourrait donc être utile aux prestataires de services souhaitant contester les demandes des autorités. Encore faut-il que les menaces de sanctions soient crédibles[62].

Du point de vue du droit de l'UE, outre la directive 2016/943 dite « secrets d'affaires » qui est en cours de transposition[63], le nouveau Règlement général sur la protection des données (RGPD)[64] constitue un autre dispositif permettant aux prestataires de s'opposer aux demandes des autorités américaines. Le RGPD dresse une liste limitative des situations dans lesquelles des données à caractère personnel peuvent être transférées vers un pays tiers[65], étant entendu

---

[56] *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa*, 482 U.S. 522 (1987).
[57] *Ibid.*, 482 US 522, 543-544.
[58] V. par ex., *Wultz v. Bank of China Ltd*, 910 F.Supp.2d 548 (S.D.N.Y. 2012).
[59] Artice 1bis de la loi n° 68-678 du 26 juillet 1968.
[60] *Aérospatiale*, *op. cit.* note 56, 482 US 522, 565-567.
[61] V. par ex., *In re Activision Blizzard, Inc.*, 86 A.3d 531 (Del. Ch. 2014).
[62] V. par ex., *Connex Railroad LLC v. AXA Corporate Solutions Assurance*, 2017 WL 3433542 (C.D. Cal. 2017).
[63] Sur ces aspects, v. O. Dorgans, *op. cit.* note 7, p. 28 ; E. Mignon & S. Dumontel, *op. cit.* note 41.
[64] Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *JOUE*, 4 mai 2016, L 119/1.
[65] RGPD, articles 44 et s.

que les « données à caractère personnel » intègrent aussi bien les données de contenu que les métadonnées se rapportant à des personnes physiques[66].

Le champ d'application territorial du RGPD est particulièrement vaste puisqu'il s'applique aux établissements traitant des données personnelles situés dans l'Union ainsi qu'au traitement des données personnelles relatives à des personnes qui se trouvent sur le territoire de l'Union, et ce, quel que soit le lieu de l'établissement qui effectue ce traitement[67]. Le RGPD peut avoir une portée extraterritoriale car il a ainsi vocation à s'appliquer dans la situation où les données d'un américain vivant aux États-Unis et qui n'a jamais été en Europe sont stockées dans un serveur situé dans l'UE. Même dans ce cas, un prestataire tel que Facebook, Google ou Microsoft ne pourrait accéder à la demande des autorités américaines de transférer directement ces données sans contrevenir aux disciplines du RGPD.

De tels transferts vers un pays tiers ne sont en effet possibles que dans les cas suivants : lorsqu'ils sont fondés sur une décision d'adéquation adoptée par la Commission qui constate que le pays tiers assure un niveau adéquat de protection (article 45) ; lorsque des garanties appropriées ont été prévues et que les personnes concernées disposent de droits opposables et de voies de droit effectives (article 46) ; lorsque l'autorité nationale de contrôle approuve des règles d'entreprise contraignantes (article 47) ; lorsque le transfert est fondé sur un accord international, tel qu'un traité d'entraide judiciaire, conclu entre l'État tiers et l'UE ou un État membre (article 48) ; pour toute une série de dérogations spécifiques prévues par l'article 49, notamment lorsque le « le transfert est nécessaire pour des motifs importants d'intérêt public » (article 49(1)(d)).

Un transfert de données vers les États-Unis réalisé dans le cadre du Cloud Act ne pourrait en l'état être justifié sur le fondement de l'une de ces dispositions : la Commission n'a pas adopté de décision d'adéquation s'appliquant aux transferts vers les autorités américaines, il n'existe pas de mécanisme conférant aux personnes concernées des garanties appropriées et équivalentes à celles du RGPD, l'article 47 ne trouve pas à s'appliquer de même que la situation envisagée par l'article 48 puisqu'il s'agirait d'un transfert direct de données du prestataire de services vers les États-Unis sans passer le biais d'un accord international.

L'ultime hypothèse envisageable est celle prévue par l'article 49(1)(d) lorsque le transfert « est nécessaire pour des motifs importants d'intérêt public ». Cet argument avait été utilisé par les autorités américaines dans l'affaire *Microsoft* en indiquant que la société ne risquait pas de violer le RGPD car l'article 49 permet « *to transfer of data for important public interest purposes, for establishing legal claims, and for "compelling legitimate interests"* »[68]. Cette interprétation est toutefois erronée car elle suggère que le pays tiers peut faire valoir son intérêt public qu'il pourrait d'ailleurs définir unilatéralement[69]. Or, le RGPD précise que l'intérêt public visé à l'article 49 est celui « reconnu par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis »[70], ce qui inclut néanmoins la coopération en matière de lutte contre le terrorisme ainsi que la criminalité grave[71] et transnationale[72]. Cette dérogation ne permet pas de court-circuiter les règles de l'article 48 fixant le principe du recours à l'accord international d'entraide judiciaire lorsqu'il s'agit de

---

[66] RGPD, article 4(1).
[67] RGPD, articles 3(1) et 3(2).
[68] *United States (Petitioner) v. Microsoft Corporation*, *Petition for a writ of certiorari*, *In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation*, juin 2017, p. 32-33.
[69] T. Christakis, *op. cit.* note 10, p. 33.
[70] RGPD, article 49(4).
[71] CJUE, 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland Ltd* et *Kärntner Landesregierung*, § 42.
[72] CJUE, 26 juillet 2017, Avis 1/15, § 148.

satisfaire de manière permanente l'intérêt public de l'État tiers. Cela a d'ailleurs été confirmé par les lignes directrices sur l'article 49 de l'European Data Protection Board[73].

Les risques de conflits d'obligations entre le Cloud Act et le RGPD ne sont pas théoriques pour les opérateurs concernés par les mandats des autorités américaines et qui s'exposent à des sanctions allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial[74]. Ils sont immédiats et sérieux et pourraient être pris en considération par les juridictions américaines dans le cadre d'une *comity analysis* lorsque la demande de divulgation a été effectuée en l'absence d'*executive agreement*. Encore faut-il que les prestataires s'emploient à contester ces demandes si celles-ci s'avèrent contraires au droit de l'UE. Une attention particulière devra donc être apportée aux diligences effectuées.

A titre de comparaison, la proposition de règlement E-evidence repose sur des considérations similaires. L'article 3 du projet précise que le règlement « s'applique aux fournisseurs de services qui proposent des services dans l'Union ». Le texte aura donc vocation à s'appliquer à une entreprise américaine qui ne dispose pas nécessairement d'une filiale ou d'une succursale dans l'un des États membres et qui stocke ses données hors de l'UE.

L'article 15 du projet envisage la situation où le destinataire de l'injonction « considère que le respect de l'injonction européenne de production serait contraire aux lois applicables d'un pays tiers interdisant la divulgation des données concernées au motif que cela est nécessaire pour protéger les droits fondamentaux des personnes concernées ou les intérêts fondamentaux du pays tiers en matière de sécurité ou de défense nationales ». Dans cette hypothèse, une procédure « d'objection motivée » est prévue par le projet, laquelle est examinée par la juridiction qui « évalue s'il existe un conflit, en examinant (a) si la législation du pays tiers s'applique en fonction des circonstances spécifiques de l'affaire en question et, si tel est le cas, (b) si la législation du pays tiers, lorsqu'elle est appliquée aux circonstances spécifiques de l'affaire en question, interdit la divulgation des données concernées »[75]. Cette évaluation repose sur des critères qui ne sont pas éloignés de ceux de la *comity analysis* des juridictions américaines et aurait pour fonction de tenir compte, et si besoin d'atténuer, les effets extraterritoriaux du futur règlement E-evidence.

8. – Un *executive agreement* comme nouveau cadre coopératif États-Unis/UE ?

Une mise en œuvre unilatérale du Cloud Act et du projet de règlement E-evidence ne se fera pas sans placer les prestataires dans un conflit d'obligations. Cette question présente un enjeu pour l'efficacité des procédures pénales aussi bien pour les États-Unis que pour les États membres de l'UE qui sollicitent de manière significative les géants américains de l'Internet sans passer par les procédures MLAT. Les parties à la Convention de Budapest sur la cybercriminalité[76] autres que les États-Unis (au sein desquelles les États membres de l'UE) envoient en moyenne 150.000 demandes annuelles aux principaux prestataires de services américains qui communiquent volontairement les informations requises par les autorités judiciaires dans 60% des cas[77].

---

[73] European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 mai 2018, p. 10.
[74] RGPD, article 83(5).
[75] Article 15(3) de la proposition de règlement E-evidence (*op. cit.* note 8).
[76] Convention de Budapest sur la cybercriminalité, STE n°185, 23 novembre 2001.
[77] Comité de la Convention sur la cybercriminalité (T-CY), T-CY(2018)16, 21 mai 2018, p. 6.

En présence d'un *executive agreement*, le Cloud Act dresse une liste précise des critères permettant aux juridictions de prendre en compte les exigences du droit étranger lorsqu'un prestataire de service s'emploie à faire opposition à une requête de communication des autorités américaines. En explicitant cette *comity analysis*, rendant ainsi plus prévisibles les standards appliqués par les juridictions américaines, les auteurs de cette législation entendaient certainement inciter les autres États à conclure de tels *executive agreements*.

Le Cloud Act délègue à l'exécutif la compétence de conclure des accords internationaux en forme simplifié permettant aux autorités étrangères de solliciter directement des informations auprès des prestataires américains avec, en contrepartie, de permettre aux autorités américaines de solliciter la communication de données détenues par des prestataires étrangers. S'il semble que l'ensemble s'intègre dans une dynamique de réciprocité, cela n'est pas tout à fait exact. Les prestataires américains bénéficient en effet d'une position dominante. Ces *executive agreements* visent en réalité moins à permettre le transfert de données par des prestataires étrangers aux autorités américaines qu'à sécuriser juridiquement les demandes formulées par celles-ci. La mise en place d'une démarche coopérative permettrait aux principaux prestataires d'éviter de possibles conflits d'obligations. Relevons aussi que le projet E-evidence de l'UE a été proposé dans le sillage du Cloud Act afin de faire « d'un danger une opportunité »[78]. La question qui se pose est de savoir si un *executive agreement* tel qu'envisagé dans le Cloud Act pourrait être conclu entre les États-Unis et l'UE et/ou ses États membres, et dans quelle mesure il pourrait s'intégrer dans ou s'appuyer sur le cadre normatif existant.

Les *executive agreements* peuvent être conclus par l'exécutif sur la base de la délégation législative fournie par le Cloud Act. Cette délégation est fondamentale afin d'envisager un cadre harmonieux avec les exigences du droit de l'UE. En effet, selon la constitution américaine, les traités doivent être ratifiés par le président avec l'approbation des deux-tiers du Sénat[79]. Le Congrès peut aussi autoriser l'exécutif à conclure des *congressional executive agreements*, ce qui est notamment le cas lorsqu'il est question de sceller plusieurs accords bilatéraux similaires[80]. En l'absence d'accord du Sénat ou délégation du Congrès, les *executive agreements* ne pourraient être invoqués devant les juridictions américaines et les garanties qu'ils incluraient seraient donc inefficaces.

La présence de cette délégation législative a son importance si l'on compare le Cloud Act avec un autre dispositif extraterritorial américain, le *Foreign Account Tax Compliance Act* (FATCA). Le FATCA est une loi du Congrès de 2010 qui impose à toutes les institutions financières étrangères de transmettre aux autorités fiscales américaines des informations sur les comptes détenus par des personnes américaines. De tels transferts étant prohibés par certains droits étrangers, les autorités américaines ont ainsi lancé une campagne de conclusion d'*intergovernmental agreements* (IGAs) avec plus d'une centaine d'États afin de les encadrer[81]. Ces IGAs ont toutefois été conclus directement par l'exécutif américain, sans accord du Sénat et sans délégation du Congrès si bien qu'ils ne sont pas mis en œuvre réciproquement par les États-Unis et que les garanties qu'ils contiennent ne peuvent être invoquées devant les juridictions américaines[82]. En bénéficiant de la délégation conférée par le Congrès, les *executives agreements* conclus sous les auspices du Cloud Act pourraient donc intégrer des

[78] S. Peyrou, *op. cit.* note 9.
[79] Constitution des États-Unis, Article II, Section 2(2).
[80] R. E. Dalton, « United States », in D. B. Hollis, M. R. Blakeslee & L. B. Ederington (eds.), *National Treaty Law and Practice*, Leiden/Boston, Martinus Nijhoff, 2005, p. 770.
[81] R. Bismuth, « L'extraterritorialité du FATCA et le problème des "américains accidentels" », *JDI*, 2017, p. 1203 et s.
[82] *Ibid.*, p. 1221 et s.

garanties requises par le RGPD et voir celles-ci efficacement mises en œuvre devant les juridictions américaines.

La question qui se pose aussi est de savoir si un tel accord est possible. Le Cloud Act impose certaines exigences aux *executive agreements* qui seront conclus par le gouvernement américain, lesquels doivent être certifiés par l'*Attorney General* et le *Secretary of State*[83]. Le Cloud Act précise que le droit de l'État étranger souhaitant conclure un tel accord doit « *affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection* »[84] et établit une liste de facteurs pris en compte à cette fin par les autorités[85], parmi lesquels : cadre juridique approprié en matière de cybercriminalité et preuves électroniques (pouvant être établi par une adhésion à la Convention de Budapest), adhésion aux principaux droits fondamentaux internationalement reconnus (respect de la vie privée, procès équitable, liberté d'expression, droit à la sûreté, etc.), garanties en matière de protection des données personnelles et respect de la liberté de l'Internet.

Si deux États membres de l'UE ne sont pas parties à la Convention de Budapest (l'Irlande et la Suède), il ne fait guère de soutes que le droit de l'UE et ses États membres offre des garanties suffisantes au regard des exigences formulées par le Cloud Act[86]. La question qui mérite d'être soulevée est davantage celle de savoir si un *executive agreement* conclu dans le cadre du Cloud Act est susceptible de satisfaire aux exigences européennes.

Les États-Unis ont entamé des négociations avec le Royaume-Uni à ce sujet avant le Cloud Act[87] mais un accord conclu à l'échelle de l'UE apparait comme la meilleure option. Le projet E-evidence constitue une opportunité intéressante pour envisager un cadre harmonisé avec les procédures prévues par un futur *executive agreement*[88]. Celui-ci pourrait s'adosser à l'accord États-Unis/UE sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière[89]. Cet accord – qui n'organise pas l'échange d'informations – s'applique aussi bien aux informations à caractère personnel transférées entre autorités compétentes qu'à celles « transférées autrement conformément à un accord conclu entre les États-Unis et l'Union européenne ou ses États membres à des fins de prévention et de détection des infractions pénales, dont le terrorisme, d'enquêtes et de poursuites en la matière »[90]. Il mériterait toutefois d'être amendé en certains points afin d'assurer sa conformité au droit primaire de l'UE[91].

---

[83] 18 U.S.C. §2523(b).
[84] 18 U.S.C. §2523(b)(1).
[85] 18 U.S.C. §2523(b)(1)(B).
[86] Au-delà des garanties découlant du droit de l'UE, tous les États membres sont parties à la CEDH et à la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Cette convention a été complétée par un protocole additionnel (convention 181) concernant les autorités de contrôle et les flux transfrontières de données qui a été ratifié par tous les États membres de l'UE (sauf la Slovénie, le Royaume-Uni, l'Italie, la Grèce et la Belgique).
[87] V. l'audition devant un comité du Sénat de Jennifer Daskal, (24 mai 2017, p. 9, <https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Daskal%20Testimony.pdf>).
[88] Sur ces aspects, v. J. Daskal & P. Swire, « A Possible EU-US Agreement on Law Enforcement Access to Data ? », 21 mai 2018, <https://www.lawfareblog.com/possible-eu-us-agreement-law-enforcement-access-data>.
[89] *JOUE*, 10 décembre 2016, L 336/13.
[90] *Umbrella Agreement*, article 3(1).
[91] Le principe de non-discrimination inclus dans l'*Umbrella Agreement* ne fait référence qu'aux ressortissants des parties respectives à l'accord et ne tient pas compte par exemple des ressortissants non américains et non européens qui pourraient être concernés (article 4). Aussi, les droits au recours consacrés par l'accord ne sont réservés qu'aux seuls citoyens des parties (article 19). Cela pourrait être contraire avec la Charte des Droits fondamentaux de l'UE qui consacre le droit à la vie privée (article 7), le droit à la protection des données (article 8) et le droit à un recours juridictionnel effectif (article 47) à toute personne indépendamment de sa nationalité.

Le Cloud Act délimite aussi le champ matériel des *executive agreements*. Les demandes des autorités étrangères ne peuvent concerner que « *prevention, detection, investigation, or prosecution of serious crime, including terrorism* »[92]. L'expression « *serious crime* » n'est pas définie, étant entendu qu'elle pourra l'être dans les accords à conclure. La législation impose aussi certaines garanties additionnelles : la demande doit identifier précisément la personne concernée, son compte, l'équipement ou l'identifiant[93], doit être fondée « *on requirements for a reasonable justification based on articulable and credible facts* »[94] et doit pouvoir être soumise à un contrôle juridictionnel[95].

Le Cloud Act ne dit pas si, par le biais des *executive agreements*, les garanties imposées aux autorités étrangères pourront également être applicables aux autorités américaines. On ignore aussi si ces accords pourront être ajustés afin d'intégrer les exigences du droit de l'UE. Le Cloud Act précise par exemple qu'en présence d'un *executive agreement*, un prestataire pourra contester une demande s'il considère que l'utilisateur concerné n'est pas une personne américaine et ne réside pas aux États-Unis[96]. Cela signifie *a contrario* qu'un contrôle juridictionnel de la demande sollicité par le prestataire sera irrecevable si la personne concernée est américaine. Cela semble problématique au regard du respect du droit à un recours juridictionnel effectif pour une personne dont les données peuvent entrer dans le champ d'application du RGPD.

Le Cloud Act exige que les *executive agreements* prévoient que la requête des autorités étrangères ne peut concerner une personne américaine ou résidant aux États-Unis[97], ou une personne non américaine dans le but d'obtenir des informations sur une personne américaine[98]. Rien n'indique toutefois que les autorités américaines ne pourront solliciter des données concernant des personnes non américaines ou résidant à l'extérieur des États-Unis. Cette asymétrie peut néanmoins être corrigée dans les *executive agreements* : soit en supprimant les limitations liées à la nationalité et à la résidence ou soit en indiquant que les requêtes concernant les nationaux et résidents de l'autre partie doivent être administrées par le biais des MLAT, au besoin selon une procédure qui serait réformée. Cette dernière option poserait toutefois problème dans l'hypothèse d'accords conclus entre les États-Unis et des États membres de l'UE car il engendrerait un traitement différentiel de citoyens européens en fonction de leur nationalité. Cet obstacle pourrait être levé dans l'hypothèse d'un accord conclu par l'UE.

Il reste la question de la latitude dont bénéficient les autorités américaines dans le cadre de la conclusion des *executive agreements*. Ceux-ci sont adoptés sur le fondement d'une délégation législative mais ils sont également soumis à une procédure de contrôle approfondi de la part Congrès (*congressional review*) qui a la possibilité de désapprouver l'accord par une résolution conjointe des deux chambres[99]. Il n'est pas exclu d'envisager que ce contrôle *ex post* constitue une manière d'homologuer des *executive agreements* qui dévient en certains points du Cloud Act afin de les ajuster aux contraintes et spécificités des autres États.

9. – Remarques conclusives

Vilipendé pour une extraterritorialité qui ne peut avoir le même sens dans l'environnement numérique[100], le Cloud Act pourrait constituer la rampe de lancement d'un cadre coopératif

[92] 18 U.S.C. §2523(b)(4)(D)(i).
[93] 18 U.S.C. §2523(b)(4)(D)(ii).
[94] 18 U.S.C. §2523(b)(4)(D)(iv).
[95] 18 U.S.C. §2523(b)(4)(D)(v).
[96] 18 U.S.C. § 2703(h)(2)(ii).
[97] 18 U.S.C. §2523(b)(4)(B).
[98] 18 U.S.C. §2523(b)(4)(C).
[99] 18 U.S.C. §2523(d)(4).
[100] J. Daskal, « Borders and Bits », *Vanderbilt Law Review*, vol. 71, 2018, p. 179 et s.

bilatéral États-Unis/UE. Associé à la proposition de règlement E-evidence à qui l'on pourrait faire certains des mêmes reproches, le Cloud Act peut poser les jalons d'un dispositif multilatéral sur la question de l'accès aux preuves électroniques.

Ce n'est pas la première fois qu'un dispositif à l'origine unilatéral et extraterritorial constitue l'élément déclencheur de réflexions et de négociations conduisant à l'établissement de disciplines transnationales. Le précédent de la lutte contre la corruption des agents publics étrangers est instructif : l'application unilatérale et étendue du Foreign Corrupt Practices Act (FCPA) a conduit à l'adoption de la Convention anti-corruption de l'OCDE[101]. Certaines expériences montrent toutefois que les dispositifs unilatéraux peuvent se révéler asymétriques et être appliqués de manière brutale. Les erreurs commises par les États membres de l'UE lorsqu'ils ont consenti à l'application extraterritoriale du FATCA concernant l'échange d'informations en matière fiscale constituent de précieux enseignements au moment d'évaluer les risques et opportunités du Cloud Act. Le Parlement européen a d'ailleurs adopté une résolution en juillet 2018 déplorant le manque de réciprocité des accords FATCA, demandant leur suspension collective et invitant à des négociations pour un accord États-Unis/UE « afin de garantir la pleine réciprocité de l'échange d'informations et de faire respecter les principes fondamentaux du droit de l'Union »[102].

L'expérience du FATCA suggère aussi qu'il faut prêter une attention particulière à deux choses : les intermédiaires et le contenu des accords bilatéraux.

Pour ce qui concerne les intermédiaires – c'est-à-dire les prestataires – la crédibilité du Cloud Act et des *executive agreements* adoptés sous ses auspices dépendra de la diligence et du sérieux avec lesquels ils administreront les demandes formulées par les autorités nationales. S'emploieront-ils à les contester lorsqu'elles servent à une procédure qui ne présente aucun lien avec l'État requérant ? Développeront-elles des procédures tenant compte des exigences de chaque pays afin de ne pas acquiescer à des demandes mettant en jeu la liberté de la presse ou le secret de certaines professions réglementées ?

Ces questions conduisent aussi à s'interroger sur le contenu des accords qui devront préciser avec minutie les éléments devant figurer dans les requêtes des autorités et les critères sur la base desquels les prestataires auront la possibilité de les contester. Un tel accord entre les États-Unis et l'UE devra également être pleinement symétrique et réciproque en n'instaurant pas des restrictions spéciales au profit des personnes ou résidents américains qui ne seraient pas applicables aux citoyens ou résidents européens. Il faut aussi s'interroger sur les mécanismes de transparence, de suivi et de règlement des différends qui pourraient être intégrés. Il est envisageable d'insérer des procédures intergouvernementales spécifiques, tel un droit d'opposition de l'État autre que celui sollicitant les données lorsqu'il est spécialement intéressé, par exemple lorsque la personne visée est résidente de cet État ou une société instituée selon le droit de cet État.

Face au Cloud Act, différentes attitudes sont envisageables. On peut faire preuve d'une naïveté béate en concluant des *executive agreements* la fleur au fusil, ce qui serait dangereux pour les intérêts de l'UE, de ses États membres et de leurs citoyens. Cela avait été le cas dans le cadre du FATCA avec le résultat que l'on connait. On peut éprouver une hostilité de principe improductive ayant pour effet de drastiquement limiter les marges de manœuvres et l'efficacité de nos propres autorités judiciaires et, possiblement, de conduire au développement de

---

[101] Sur ces aspects, v. M. Pieth, « Introduction », in M. Pieth, L. A. Mow & N. Bonucci (eds.), *The OECD Convention on Bribery – A Commentary*, Cambridge, Cambridge University Press, 2014, 2e éd., p. 11 et s.

[102] Parlement européen, *Résolution sur les effets néfastes de la loi des États-Unis relative au respect des obligations fiscales concernant les comptes étrangers (FATCA) sur les citoyens de l'Union européenne, et en particulier les "Américains accidentels"*, (2018/2646(RSP)), 5 juillet 2018, § 10.

« services territorialisés et étanches, au risque d'une balkanisation d'Internet »[103]. On peut aussi manifester une méfiance constructive, voire un optimisme lucide, en envisageant le Cloud Act comme une opportunité pour l'UE et ses États membres, leur permettant de façonner un futur droit global de l'accès aux preuves numériques. En définitive, *Every cloud has a silver lining*.

[103] P. Jacob, *op. cit.* note 10. V. aussi, T. Christakis, *op. cit.* note 10, p. 33 et s.