3

Revue critique de droit international privé - juillet-septembre 2019 - pages 643 à 924

RGPD versus CLOUD : vrai conflit ou saine concurrence ?

Rev. crit. DIP

Revue critique de droit international privé

647 D'une diversité à l'autre
Marie-Élodie Ancel

665 La compétence des États à l'égard des données numériques
Patrick Jacob

681 Le *Cloud Act* face au projet européen *e-evidence* : confrontation ou coopération ?
Régis Bismuth

695 La communication aux autorités américaines de données sur la base du *Cloud Act* est-elle en conflit avec le règlement général sur la protection des données ?
Théodore Christakis

ref : 541903

9 782995 419036

DALLOZ

Le *Cloud Act* face au projet européen *e-evidence* : confrontation ou coopération[1] ?

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

Résumé
Adopté par le Congrès américain en mars 2018, le Cloud Act *permet d'encadrer l'accès par les autorités américaines aux preuves électroniques stockées à l'étranger dans le cadre de procédures pénales. Alors que cette loi a été particulièrement critiquée en Europe pour son extraterritorialité, qui mérite d'ailleurs d'être nuancée, l'Union européenne a rendu public au même moment un projet de règlement e-evidence sur le même sujet et qui repose d'ailleurs sur des mécanismes similaires. Alors que ces deux initiatives unilatérales semblent* prima facie *difficilement compatibles, elles devront néanmoins servir de base à un cadre coopératif UE/Etats-Unis et pourraient même constituer une opportunité de façonner un droit global de l'accès aux preuves numériques.*

Summary
Enacted by the US Congress in March 2018, the Cloud Act regulates cross-border access to electronic evidence in US criminal proceedings. While strongly criticized in Europe for its extraterritoriality, which besides deserves to be nuanced, the European Commission, on the same matter, released its e-evidence regulation proposal which relies on similar mechanisms. Although these two unilateral initiatives do not seem compatible one with another, they may serve as a basis for an EU/US cooperative framework and can even provide an opportunity to shape a global law on the cross-border access to electronic evidence.

(1) Cette étude reprend certains éléments d'une publication précédente : *Every Cloud Has a Silver Lining* : une analyse de l'extraterritorialité du *Cloud Act* au regard du projet européen *E-evidence*, JCP E 2018, n° 40, p. 35-47.

Une enquête pénale sur deux requiert dorénavant la saisie de preuves électroniques stockées sur des serveurs localisés dans un autre État [2]. Pour obtenir de telles preuves, en particulier les données dites « de contenu » (messages, documents, photos, vidéos, etc.), il peut être envisagé d'emprunter les voies prévues par les traités d'entraide judiciaire (*mutual legal assistance treaties* ou MLAT) et demander dans ce cadre aux autorités de l'État étranger sur le territoire duquel les données sont stockées de solliciter leur divulgation auprès du prestataire concerné. Ces procédures MLAT sont toutefois longues et manquent de souplesse. Il n'est donc pas surprenant que les autorités préfèrent parfois requérir directement ces données localisées à l'étranger auprès des prestataires. Alors que de telles démarches se déroulaient jusqu'à récemment dans un cadre juridiquement incertain, des initiatives ont été prises de part et d'autre de l'Atlantique afin de clarifier celui-ci. C'est ce que permettent ainsi deux dispositifs législatifs, le *Cloud Act* [3], promulgué par le président américain le 23 mars 2018 et, ce qui n'est encore qu'à l'état de projet, la proposition de la Commission européenne d'avril 2018 de règlement relatif à l'accès aux preuves électroniques en matière pénale (projet de règlement « *e-evidence* ») [4]. Alors qu'ils s'inscrivent dans une logique unilatérale, ces deux dispositifs sont susceptibles de servir de base à un futur droit global de l'accès transfrontière aux preuves électroniques (III). Il faudrait toutefois que soient surmontées quelques incompatibilités et dissonances entre la législation américaine et celle de l'Union européenne (II). Avant d'aborder ces aspects, il convient de revenir brièvement sur le contexte de ces initiatives législatives (I).

I – Le contexte : *Microsoft v. United States*, *Cloud Act* et projet *e-evidence*

A – À l'origine du *Cloud Act* et du projet *e-evidence*

Le *Cloud Act* (pour *Clarifying Lawful Overseas Use of Data Act*) est une conséquence directe de l'affaire *Microsoft v. United States*. Celle-ci trouve son origine dans un mandat (*warrant*) exigeant que Microsoft communique aux autorités plusieurs informations associées au compte email d'une personne suspectée de trafic de stupéfiants. La demande était fondée sur le *Stored Communications Act* (SCA) [5] adopté en 1986 et qui n'envisageait pas à l'époque la situation où les données électroniques sont accessibles depuis les États-Unis mais 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 mais refusa de divulguer celles stockées dans son *data center* en Irlande, soulignant qu'il fallait emprunter les voies prévues par les traités d'entraide judiciaire (MLAT).

(2) European Commission, Recommendation for a Council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM(2019) 70 final, 5 févr. 2019, p. 1.
(3) Le *Cloud Act* est la section V du *Consolidated Appropriations Act* de 2018 (H.R. 1625, Pub.L. 115-141).
(4) 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 avr. 2018.
(5) 18 U.S.C. § 2703.

La cour d'appel du 2nd circuit fit droit en 2016 aux positions de Microsoft [6] et le gouvernement américain décida de porter l'affaire devant la Cour suprême. La position de la cour d'appel combinée à celles en sens contraire d'autres juridictions fédérales de première instance générait pour les autorités une incertitude susceptible d'entraver l'efficacité des procédures pénales. Le Congrès américain a ainsi adopté le *Cloud Act* afin de clarifier la portée du SCA, et ce, avant l'issue de la procédure devant la Cour suprême qui a mis fin à l'instance en avril 2018.

Promulgué par le président américain le 23 mars 2018, le *Cloud Act* donne la possibilité aux autorités américaines d'exiger des prestataires de services électroniques la divulgation de données, et ce, « *whether such communication, record, or other information is located within or outside of the United States* » [7]. Cette dimension extraterritoriale a suscité de nombreuses controverses, certains suggérant qu'elle reflétait une hégémonie américaine dans le domaine numérique. Une analyse attentive du *Cloud Act* conduit toutefois à nuancer ces critiques d'autant plus qu'il y a quelques similarités entre le *Cloud Act* et la proposition de la Commission européenne d'avril 2018 de règlement relatif à l'accès aux preuves électroniques en matière pénale (projet de règlement « *e-evidence* ») [8] qui instaurerait une procédure d'injonction européenne de production et de conservation de données pouvant viser les prestataire offrant des services dans l'Union, et ce, sans avoir à avoir recours aux procédures MLAT. Ce projet de règlement a d'ailleurs été également initié dans le contexte de l'affaire *Microsoft v. United States*.

B – Une dimension extraterritoriale à nuancer et appelant une solution globale

Le *Cloud Act* précise que les données dont la divulgation est demandée peuvent être situées aux États-Unis ou à l'étranger. Le projet *e-evidence* n'indique pas que les seules données localisées dans l'UE peuvent être sollicitées et il s'applique dès lors, à l'instar du *Cloud Act*, aux données que les prestataires stockent aussi à l'étranger. S'il y a une dimension extraterritoriale dans les deux dispositifs, celle-ci mérite d'être nuancée.

Le lieu de stockage des données sollicitées est à l'origine inconnu des autorités. Les données sont fragmentées et dispersées par les prestataires sur plusieurs serveurs localisés dans des États différents, parfois selon des 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 (comme le coût de l'électricité). Les données sont parfois dupliquées et stockées sur des serveurs différents afin de les préserver [9]. Cette répartition spatiale souvent aléatoire des données a généré des difficultés pour les 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 vidéo étaient stockés à l'étranger [10]. On a également pu constater que des prestataires stoc-

(6) *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016).
(7) 18 U.S.C. § 2713.
(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 avr. 2018.
(9) T. Christakis, Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques, CEIS, The Chertoff Group, 2017, p. 25 s.
(10) 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), p. 5-6.

kaient 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 [11]. 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.

Prenons aussi l'exemple de Google qui dispose de huit *data centers* aux États-Unis, quatre en Europe, deux en Asie et un au Chili [12]. Un utilisateur de services Google habitant sur le continent africain ne peut ainsi avoir ses données stockées dans son État de résidence. Un État souhaitant accéder à ces données dans le cadre d'une procédure pénale qui ne présenterait par ailleurs aucun autre élément d'extranéité 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 justifiable : 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 affectent l'efficacité de la justice. De la fracture numérique découlerait donc une fracture juridique. C'est en ce sens qu'une solution à terme sur cette question ne pourrait être que globale.

À cette aune, deux constats peuvent être réalisés quant à l'extraterritorialité du *Cloud Act*, lesquels permettent de montrer que le débat ne peut exclusivement s'articuler autour du critère de la localisation des données.

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 est « *irrelevant* » [13], 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. En retenant le lieu de stockage, on pourra certes gloser sur l'atteinte à la souveraineté de Singapour, 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 ?) [14], 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.

En second lieu, on peut constater que la configuration actuelle du stockage des données par des prestataires opérant

(11) *Ibid.*, p. 4.
(12) Liste consultable au lien suivant : https://www.google.com/about/datacenters/inside/locations.
(13) P. S. Berman, Legal Jurisdiction and the Derritorialization of Data, Vanderbilt Law Review, vol. 71, 2018, p. 23.
(14) Critère pouvant être pris en compte lorsqu'il existe un accord avec un État étranger. 18 U.S.C. §2713(h)(2)(i).

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, à charge pour les 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[15]. Ce modèle implique une responsabilisation des prestataires qui deviendraient des sortes de *gatekeepers*, et c'est pourquoi le *Cloud Act* a suscité certaines craintes. Le *Cloud Act* donne la possibilité au gouvernement américain 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[16]. Il devrait être traité au moment de la négociation des accords intergouvernementaux et le *Cloud Act* prévoit d'ailleurs que de tels accords 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* »[17]. Un problème similaire se pose d'ailleurs pour le 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[18], affectant ainsi l'utilité et l'effectivité d'un tel recours.

II – La gestion des conflits entre le *Cloud Act* et le droit de l'UE

A – La possible prise en compte par le juge américain des conflits normatifs résultant du *Cloud Act*

Les prestataires de services 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*[19].

(15) V. art. 4 à 12 de la proposition de règlement e-evidence (*op. cit.* note 8).
(16) P. Sterne et C. Fassett, The Cloud Act: A Danger to Journalists Worldwide, Freedom of the Press Foundation, 22 mars 2018, https://freedom.press.
(17) 18 U.S.C. § 2523(b)(1).
(18) Art. 11(2) de la proposition de règlement e-evidence (*op. cit.* note 8).
(19) T. Christakis, art. préc., note 9, p. 32 s.

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 États-Unis et (ii) que cette communication « *would create a material risk that the provider would violate the laws of a qualifying government* » [20] – 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* [21]. 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* ») exige 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 [22].

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 [23], lesquels traduisent une « *comity analysis* » existant déjà en droit américain. Ces critères 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 [24] et, d'ailleurs, le *Cloud Act* indique que les « *common law standards governing the availability or application of comity analysis* » restent applicables [25]. 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 commerciale [26]. 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* » [27]. Dans le sillage de la jurisprudence *Aérospatiale*,

(20) 18 U.S.C. § 2703(h)(2)(ii).
(21) 18 U.S.C. § 2703(h)(1)(A)(i).
(22) 18 U.S.C. § 2703(h)(2)(B).
(23) 18 U.S.C. § 2703(h)(3).
(24) 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, CDE 2018, n° 4.
(25) *Cloud Act,* sec. 6.
(26) *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa*, 482 U.S. 522 (1987).
(27) *Ibid.*, 482 US 522, 543-544.

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 [28].

B – Les règles de droit de l'UE susceptibles de faire obstacle aux demandes de divulgation

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

Outre la directive 2016/943 dite « secrets d'affaires », transposée en France par loi n° 2018-670 du 30 juillet 2018 [29], le nouveau Règlement général sur la protection des données (RGPD) [30] 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 [31], étant entendu que les « données à caractère personnel » intègrent aussi bien les données de contenu que les métadonnées se rapportant à des personnes physiques [32].

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 [33]. 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 dispositions 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 (art. 45) ; lorsque des garanties appropriées ont été prévues et que les personnes concernées disposent de droits opposables et de voies de droit effectives (art. 46) ; lorsque l'autorité nationale de contrôle approuve des règles d'entreprise contraignantes (art. 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 (art. 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 » [art. 49(1)(d)].

(28) V. par ex., *Wultz v. Bank of China Ltd*, 910 F.Supp.2d 548 (S.D.N.Y. 2012).
(29) Sur ces aspects, v. 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. 28.
(30) Règl. (UE) 2016/679 du 27 avr. 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 dir. 95/46/CE, JOUE L 119/14, mai 2016.
(31) RGPD, art. 44 s.
(32) RGPD, art. 4(1).
(33) RGPD, art. 3(1) et 3(2).

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"* »[34]. 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[35]. 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 »[36], ce qui inclut néanmoins la coopération en matière de lutte contre le terrorisme ainsi que la criminalité grave[37] et transnationale[38]. 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 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*[39].

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[40]. 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.

À 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

(34) *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.
(35) T. Christakis, art. préc., note 9, p. 33.
(36) RGPD, art. 49(4).
(37) CJUE 8 avr. 2014, aff. C-293/12 et C-594/12, *Digital Rights Ireland Ltd* et *Kärntner Landesregierung*, § 42, AJDA 2014. 773 ; *ibid.* 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D. 2014. 1355, note C. Castets-Renard ; *ibid.* 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; Légipresse 2014. 265 ; RTD eur. 2015. 117, étude S. Peyrou ; *ibid.* 168, obs. F. Benoît-Rohmer ; *ibid.* 786, obs. M. Benlolo-Carabot.
(38) CJUE 26 juill. 2017, avis 1/15, § 148, D. 2017. 1655, obs. E. Autier ; JT 2017, n° 201, p. 12, obs. X. Delpech.
(39) European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 mai 2018, p. 10.
(40) RGPD, art. 83(5).

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 nationale ». 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 »[41]. 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*.

III – Les jalons d'un droit global de l'accès aux preuves électroniques

A – De l'unilatéral au bilatéral : l'éventualité d'un cadre coopératif États-Unis/UE

Une mise en œuvre unilatérale du *Cloud Act* et du projet de règlement *e-evidence* placera les prestataires dans un conflit d'obligations. C'est 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[42] 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[43].

Dans l'hypothèse 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 services 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, le législateur américain entendait 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 simplifiée qui permettront aux autorités étrangères de solliciter directement des informations auprès des prestataires américains avec, en contrepartie, la possibilité donnée aux autorités américaines de solliciter la communication de données détenues par des prestataires étrangers. Nous ne sommes toutefois pas dans une authentique logique de réciprocité. Les prestataires américains bénéficient d'une position dominante. Ces *executive agreements* visent en réalité moins à

(41) Art. 15(3) de la proposition de règlement *e-evidence*.
(42) Convention de Budapest sur la cybercriminalité, STE n° 185, 23 nov. 2001.
(43) Comité de la Convention sur la cybercriminalité (T-CY), T-CY(2018)16, 21 mai 2018, p. 6.

permettre le transfert de données par des prestataires étrangers aux autorités américaines qu'à sécuriser juridiquement leurs demandes. La mise en place d'une démarche coopérative permettrait aux principaux prestataires d'éviter des conflits d'obligations. Relevons aussi que le projet *e-evidence* de l'UE a été proposé afin de faire « d'un danger une opportunité » [44]. 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*, laquelle 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 [45]. 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 [46]. 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 dans l'ordre juridique américain.

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 [47]. Ces IGAs ont toutefois été conclus directement par l'exécutif, 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 [48]. En bénéficiant de la délégation conférée par le Congrès, les *executives agreements* conclus sous les auspices du *Cloud Act* pourraient donc éventuellement intégrer des 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 sur le fond. 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* [49]. Le *Cloud Act* précise que le droit de l'État étranger souhaitant conclure un tel accord doit « *affor[d] robust substantive and procedural protections for privacy and civil liberties in light of the data collection* » [50] et établit une liste de facteurs pris en compte à cette fin par les autorités [51], parmi lesquels : cadre

(44) S. Peyrou, *Le projet de règlement « E-evidence » (preuves électroniques) présenté par la Commission européenne : Un « Cloud Act » européen*, 24 avr. 2018, http://www.gdr-elsj.eu.
(45) Constitution des États-Unis, art. II, sect. 2(2).
(46) 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.
(47) R. Bismuth, L'extraterritorialité du FATCA et le problème des « Américains accidentels », JDI 2017. 1203 s.
(48) *Ibid.*, p. 1221 s.
(49) 18 U.S.C. §2523(b).
(50) 18 U.S.C. §2523(b)(1).
(51) 18 U.S.C. §2523(b)(1)(B).

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 doute que le droit de l'UE et ses États membres offre des garanties suffisantes au regard des exigences formulées par le *Cloud Act* [52]. 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* [53] et, plus récemment avec l'UE. La Commission européenne a d'ailleurs recommandé en février 2019 l'ouverture de négociations à ce propos en demandant que le mandat comporte trois axes majeurs : obtention accélérée des preuves électroniques, gestion des conflits normatifs et respect des droits fondamentaux [54].

Le projet *e-evidence* constitue une opportunité intéressante pour envisager un cadre harmonisé avec les procédures prévues par un futur *executive agreement* [55]. 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 [56]. 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 » [57]. Il mériterait toutefois d'être amendé en certains points afin d'assurer sa conformité au droit primaire de l'UE [58].

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* » [59]. 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

(52) Au-delà des garanties découlant du droit de l'UE, tous les États membres sont parties à la Conv. EDH 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 (conv. 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).

(53) 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).

(54) *Commission recommends negotiating international rules for obtaining electronic evidence,* Press realease, 5 févr. 2019.

(55) Sur ces aspects, v. J. Daskal et 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.

(56) JOUE L 336/13, 10 déc. 2016.

(57) *Umbrella Agreement*, art. 3(1).

(58) 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 (art. 4). Aussi, les droits au recours consacrés par l'accord ne sont réservés qu'aux seuls citoyens des parties (art. 19). Cela pourrait être contraire avec la Charte des Droits fondamentaux de l'UE qui consacre le droit à la vie privée (art. 7), le droit à la protection des données (art. 8) et le droit à un recours juridictionnel effectif (art. 47) à toute personne indépendamment de sa nationalité.

(59) 18 U.S.C. §2523(b)(4)(D)(i).

doit identifier précisément la personne concernée, son compte, l'équipement ou l'identifiant [60], doit être fondée « *on requirements for a reasonable justification based on articulable and credible facts* » [61] et doit pouvoir être soumise à un contrôle juridictionnel [62].

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 [63]. 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 [64], ou une personne non américaine dans le but d'obtenir des informations sur une personne américaine [65]. 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, 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.

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 du Congrès (*congressional review*), qui a la possibilité de désapprouver l'accord par une résolution conjointe des deux chambres [66]. 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.

B – Du bilatéral au global ?

Alors qu'il a été vilipendé pour une extraterritorialité qui ne peut avoir le même sens dans l'environnement numérique [67], le *Cloud Act* pourrait constituer la rampe de lancement d'un cadre coopératif bilatéral États-Unis/UE. Associé à la proposition de règlement *e-evidence* à qui l'on pour-

(60) 18 U.S.C. §2523(b)(4)(D)(ii).
(61) 18 U.S.C. §2523(b)(4)(D)(iv).
(62) 18 U.S.C. §2523(b)(4)(D)(v).
(63) 18 U.S.C. § 2703(h)(2)(ii).
(64) 18 U.S.C. §2523(b)(4)(B).
(65) 18 U.S.C. §2523(b)(4)(C).
(66) 18 U.S.C. §2523(d)(4).
(67) J. Daskal, Borders and Bits, Vanderbilt Law Review, vol. 71, 2018. 179 s.

rait 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.

Un dispositif à l'origine unilatéral et extraterritorial a déjà pu constituer l'élément déclencheur de réflexions et de négociations conduisant à l'établissement de disciplines globales. 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 [68]. 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 d'un *executive agreement* conclu dans le cadre 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 » [69].

Les péripéties entourant le FATCA montrent 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 également 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

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

(69) 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 juill. 2018, § 10.

citoyens. Cela avait été le cas dans le cadre du FATCA avec le résultat que l'on connaît dorénavant. 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 « services territorialisés et étanches, au risque d'une balkanisation d'internet »[70]. On peut aussi manifester une méfiance constructive, voire un optimisme lucide, en envisageant le *Cloud Act* et son quasi équivalent européen comme une opportunité pour les États-Unis et l'UE de façonner un futur droit global de l'accès aux preuves numériques.

(70) P. Jacob, art. préc., note 24. V. aussi T. Christakis, art. préc., note 9, p. 33 s.