Premières réflexions sur le *Cloud Act*: contexte, mécanismes et articulations avec le RGPD

Alexandre Cassart[1]

Le Cloud Act, *voté rapidement pour,* a priori, *résoudre une difficulté juridique interne aux USA, a pris les commentateurs par surprise. Un peu plus d'un an après le vote de cette loi qui ouvre largement les possibilités d'accès des forces de l'ordre américaines aux contenus électroniques stockés à l'étranger, cet article est l'occasion d'un point sur cette législation et sur son articulation avec le RGPD.*

The Cloud Act which was intended to solve an internal legal issue has surprised most scholars. A year later, this paper intends to examine the context, mechanics and (strained) relationship with the GDPR of this Act which allows US police forces to access to electronical evidences stored abroad.

I. INTRODUCTION

Comme les nuages portés par le vent, les flux de données se moquent des frontières. Le succès de l'Internet et du *Cloud Computing*[2] renforce encore cette mobilité extrême. À la différence des cumulus, les données peuvent être contraintes par le droit. Les frontières se réinvitent alors dans le débat avec une acuité particulière.

Il n'a toutefois guère été question de débats – parlementaires cette fois – lorsque le Congrès américain a voté le *Clarifying Lawful Overseas Use of Data Act*[3] (ci-après le « *Cloud Act* ») en date du 23 mars 2018. Camouflé dans une loi fiscale interminable, promulguée le lendemain par le Président Trump, ce texte vise à permettre aux forces de l'ordre de requérir des fournisseurs de services de communication électronique américains qu'ils transmettent aux instances étatiques des données stockées sur des serveurs situés aux États-Unis ou dans des pays étrangers. Ni la personne concernée par l'accès, ni le pays dans lequel l'accès est opéré, ni le pays dont la personne concernée est citoyenne ne sont tenus informés de cet accès.

Eu égard à l'hégémonie économique des géants américains de la technologie, les GAFAM[4] entre autres, le *Cloud Act* permet donc concrètement aux services de police américains d'accéder à une proportion importante des données échangées du point de vue mondial.

1 Avocat, Lexing Belgium. Chargé de cours invité UNamur, Fellow CRIDS. Les opinions exprimées sont celles de l'auteur uniquement.

2 Méthode informatique par laquelle la plupart des traitements et le stockage des données sont réalisés sur des machines distantes hébergées dans des data centers. L'utilisateur final se moquant généralement de connaître la localisation de ces data centers, l'image du « nuage » a été utilisée pour symboliser cet endroit mystérieux.

3 *Clarifying Lawful Overseas Use of Data Act*, *Pub.L.* 115-141.

4 Acronyme de Google Apple Facebook Amazon Microsoft.

Vu par beaucoup comme la réponse américaine au Règlement général sur la protection des données[5] (ci-après « RGPD ») qu'il a précédé de peu, le *Cloud Act* fait l'objet de nombreuses critiques[6-7]. Certaines, peut-être formulées « à chaud », étaient sans doute issues d'une compréhension incomplète de la portée exacte du *Cloud Act* et du texte, le *Stored Communication Act*[8] (ci-après « *Stored Communication Act* ») dans lequel il s'inscrit. L'émotion étant passée, il convient d'examiner les questions posées par le *Cloud Act* et leur impact juridique concret[9].

Après cette introduction, cet article abordera la genèse du *Cloud Act* et le contexte dans lequel celui-ci a été rédigé. La seconde section décrira les deux dispositions principales du *Cloud Act* ainsi que les procédures et protections qu'il prévoit. Enfin, la troisième section fournira quelques éléments de réflexion sur l'articulation entre le *Cloud Act* et le RGPD.

II. ÉLÉMENTS DE CONTEXTE

A. *Stored Communication Act*

Le *Cloud Act* est un ajout législatif dans le *Stored Communication Act*, lui-même introduit en 1986 dans le Titre 18 des *United States Codes*[10], dont il forme le chapitre 121. Ce Titre 18 rassemble les règles fédérales américaines en matière de droit pénal et de droit de la procédure pénale.

1. *Historique du* Stored Communication Act

a. *Absence de protection des données électroniques par le Quatrième Amendement de la Constitution américaine*

Dans les années 1980, en réponse au succès grandissant de l'informatique, les demandes d'accès par les autorités pénales américaines aux données stockées par les fournisseurs de service de communication électronique se multiplièrent. Mais, alors que le Quatrième Amendement[11] américain protégeait fortement les citoyens américains contre les perquisitions et saisies à leur domicile, ils ne bénéficiaient pas de la même protection en ce qui concernait leurs données électroniques[12].

5 Règlement (UE) 2016/679 du Parlement européen et du Conseil 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 (règlement général sur la protection des données), *J.O.*, L 119, 4 mai 2016, pp. 1-88.

6 Parmi de nombreux articles de presse et de réactions d'ONG, voy. notamment la page consacrée au sujet par l'Electronic Frontier Foundation, https://www.eff.org/document/cloud-act-one-page-summary. Pour une critique plus scientifique concernant le poids de la compliance, voy. notamment O. Dorgans, « Le *CLOUD ACT* : un nouvel instrument de guerre économique renforçant l'ingérence des autorités américaines sur les prestataires de services de communication électronique américains », *Revue internationale de la compliance et de l'éthique des affaires*, n° 26, 2018.

7 Curieusement, la législation belge connaît depuis plusieurs années la possibilité d'étendre une recherche au sein d'un système informatique au-delà des frontières belges, sans que cela ne semble chagriner grand monde. Cette possibilité est prévue à l'article 39*bis*, § 3, du Code d'instruction criminelle.

8 *Stored Communications Act*, *Pub.L.* 99-508.

9 Pour répondre à ces critiques et clarifier le propos du *Cloud Act*, le Département américain de la justice a publié un livre blanc : USA DoJ, White Paper, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, April 2019, www.justice.gov/CLOUDAct.

10 https://www.govinfo.gov/content/pkg/USCODE-2017-title18/html/USCODE-2017-title18.htm.

11 Quatrième amendement de la Constitution américaine : « *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized* », https://www.archives.gov/founding-docs/bill-of-rights-transcript.

12 O. Kerr, « A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It », *Geo. Wash. L. Rev.*, 72, 2004.

Pour organiser une perquisition ou une saisie, conformément à ce Quatrième Amendement, les forces de police américaines doivent obtenir d'un juge qu'il accorde un mandat de perquisition (« *Search Warrant* »). Le juge délivre ce mandat s'il est convaincu qu'une cause probable (« *probable cause* ») ressort de l'affidavit qui lui est présenté par les policiers[13].

b. La difficulté posée par la Third Party Doctrine

Avant l'entrée en vigueur du *Stored Communication Act*[14], sous l'influence de la « *Third Party Doctrine* »[15], les données confiées à des prestataires de service tiers ne bénéficiaient pas de cette protection.

Selon la théorie de la *Third Party Doctrine*, le fait de confier volontairement des données à des tiers ne passe pas le test de l'attente raisonnable de vie privée (« *Reasonable expectation of privacy* »), test développé par la Cour Suprême américaine dans l'arrêt *Katz v. United States*[16]. Un mandat n'était donc pas nécessaire pour obtenir une donnée d'un prestataire de service, par exemple une compagnie de téléphone. Une *subpoena* suffisait, soit une procédure beaucoup plus légère.

Cette position de la Cour Suprême, répétée dans différents arrêts[17], devenait difficilement tenable du fait de l'importance croissante des technologies de l'information dans la vie quotidienne. En conséquence, le Congrès américain adopta, en 1986, le *Electronic Communications Privacy Act*[18-19], lequel contient le *Stored Communication Act*.

2. *Mécanismes originaux contenus dans le* Stored Communication Act

Le *Stored Communication Act* contient plusieurs dispositions visant à améliorer la protection des citoyens et de leurs données.

La section 2701 du *Stored Communication Act* pose le principe de l'illégalité de l'accès non autorisé à ces communications. La section 2702 encadre quant à elle la divulgation volontaire des données par les fournisseurs de services.

Enfin, la section 2703 a pour objet de permettre aux forces de l'ordre de requérir l'accès aux données, tout en étendant sur ces données la protection conférée par le Quatrième Amendement. Cette section différencie le contenu des communications électroniques des métadonnées afférentes à ces communications. Et distingue si le contenu est stocké électroniquement ou s'il se trouve chez un service informatique à distance (« *remote computing services* »). Les conditions d'accès ainsi que les recours sont différents selon les cas.

Sans rentrer dans les détails du texte, notons qu'une entité gouvernementale doit disposer d'un mandat pour exiger d'un fournisseur de services de communication électronique qu'il

13 La cause probable est reconnue lorsqu'il existe une probabilité raisonnable qu'une perquisition aboutisse à la preuve de la découverte d'un crime. Voy. *Illinois v. Gates et ux.*, 462 U.S. 213, https://caselaw.findlaw.com/us-supreme-court/462/213.html.

14 Pour être tout à fait précis, une certaine protection était déjà prévue contre les écoutes téléphoniques par le Wiretap Act contenu dans l'Omnibus Crime Control and Safe Streets Act de 1968 (*Pub.L.* 90-351), sous l'influence de la « Third Party Doctrine ».

15 O. Kerr, « The Case for the Third-Party Doctrine », *Mich. L. Rev.*, No. 107, 2009.

16 *Katz v. United States*, 389 U.S. 347 (1967), https://supreme.justia.com/cases/federal/us/389/347/.

17 *United States v. Miller*, 425 U.S. 435 (1976), https://supreme.justia.com/cases/federal/us/425/435/, et *Smith v. Maryland*, 442 U.S. 735 (1979), https://supreme.justia.com/cases/federal/us/442/735/.

18 *Electronic Communications Privacy Act*, *Pub.L.* 99-508.

19 Voy. notamment, sur l'historique du *Electronic Communications Privacy Act*, D. Mulligan, « Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act », *Geo. Wash. L. Rev.*, 72, 2004 ; ou encore R. Ward, « Discovering Facebook: Social Network Subpoenas And The Stored Communications Act », *Harvard Journal of Law & Technology*, Vol. 24, No. 2, 2011, 563 et s.

transmette le contenu d'une communication électronique stockée pendant 180 jours ou moins[20].

Par contre, au-delà d'une durée de conservation de 180 jours de stockage, il suffit d'une *subpoena*[21] et d'une notification préalable pour obtenir la divulgation, ce qui représente un formalisme bien plus léger et donc moins protecteur du citoyen.

3. *Inadéquation progressive entre le* Stored Communication Act *et les usages*

L'objectif premier du *Stored Communication Act* était donc de protéger les citoyens contre les dérives policières et les accès trop aisés à leurs données.

Toutefois, plusieurs critiques[22] se sont élevées contre le *Stored Communication Act*, notamment du fait de l'inadéquation à l'évolution des pratiques et partant, du manque de protection de la vie privée des citoyens.

Par exemple, si dans les années 1980 le stockage électronique était limité et les courriels effacés après quelques jours, les courriels sont maintenant stockés pendant des années sans difficulté. Le seuil de 180 jours de conservation a donc totalement perdu de sa pertinence.

Il revenait aux juges d'adapter, avec des fortunes diverses, le *Stored Communication Act* aux nouveaux usages[23].

4. *Débat au sujet de la portée territoriale du* Stored Communication Act

La question de l'extraterritorialité du *Stored Communication Act* s'est également posée de plus en plus fréquemment, notamment du fait des caractéristiques particulières des données[24], dont la mobilité a entraîné la multiplication des *data centers* localisés à l'étranger.

Le *Stored Communication Act* s'appliquait-il aux données stockées dans des serveurs localisés en dehors du territoire américain, mais gérés par des sociétés américaines ?

Deux écoles s'affrontaient principalement sur ce sujet, la doctrine de l'arrêt *Bank of Nova Scotia* et les tenants de la conclusion de traités internationaux.

a. Bank of Nova Scotia *Doctrine*

Les tenants de l'extraterritorialité se basaient sur la doctrine dégagée par l'arrêt *Bank of Nova Scotia*.

Dans cette affaire soumise à la Cour d'appel du 11e Circuit, la filiale américaine d'une banque canadienne avait refusé de communiquer des documents visés dans un « *grand jury subpoena duces tecum* ». Les dossiers étaient conservés au sein d'autres filiales situées aux Bahamas ou

20 Sur la justification supposée de ce délai de 180 jours à l'époque, voy. O. Kerr, « The Next Generation Communications Privacy Act », *University of Pennsylvania Law Review*, No. 162, 2004.

21 La possibilité de recours à la *subpoena* est toutefois battue en brèche par différents arrêts de jurisprudence, dont United States v. Warshak (http://www.opn.ca6.uscourts.gov/opinions.pdf/08a0252p-06.pdf), ainsi que le récent arrêt de la Cour Suprême *Carpenter v. United States* (No. 16-402, 585 U.S.), https://www.aclu.org/legal-document/united-states-v-carpenter-supreme-court-decision.

22 Par exemple, D. Solove, « Reconstructing Electronic Surveillance Law », *Geo. Wash. L. Rev.*, 72, 2004 ; J. Kesan *et al.*, « Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency », *Wash. and Lee L. Rev.*, 70, 2013 ; C. Borchert, F. Pinguelo et D. Thaw, « Reasonable expectations of privacy settings: social media and The Stored Communications Act », *Duke Law And Technology Review*, Vol. 13, No. 1, 2015 ou encore I. Kattan, « Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud », *Vand. J. Ent. and Tech. L.*, No. 13, 2011.

23 W. Robinson, « Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act », *Geo. L.J.*, No. 98, 2010.

24 J. Daskal, « The Un-Territoriality of Data », *Yale Law Journal*, No. 135, 2015-2016.

dans les îles Caïmans, et la requête américaine serait, selon la banque, entrée en contradiction avec les droits nationaux de ces pays.

La banque n'a pas été suivie par la Cour et a été sanctionnée à défaut d'avoir exécuté de bonne foi la *subpoena*[25].

b. Mutual legal assistance treaty

Les partisans du respect des souverainetés nationales avançaient plutôt la nécessité d'utiliser les *Mutual legal assistance treaty* (ci-après MLAT), soit les traités internationaux réglant les coopérations policières et pénales renforcées entre les États[26].

B. *Microsoft vs the United States*

Un cas de jurisprudence allait toutefois défrayer la chronique et précipiter une solution.

1. Contexte de l'affaire

En 2013, dans le cadre d'une enquête relative à un trafic de stupéfiants, un juge new-yorkais a lancé un mandat sur la base du *Stored Communication Act*, obligeant Microsoft à produire tous les courriels et informations associés à un compte utilisateur. Si ces dernières étaient stockées sur des serveurs américains de Microsoft, les courriels se trouvaient sur un serveur situé à Dublin, en Irlande.

Microsoft a accepté de fournir les renseignements concernant le compte, mais a refusé de remettre les courriers électroniques, arguant qu'un juge américain n'avait pas de compétence pour lancer un mandat visant des données situées à l'étranger.

Microsoft s'appuyait sur le conflit de lois pour renvoyer vers le MLAT conclu entre les USA et l'Irlande[27].

2. Première décision de confirmation

Un premier juge a donné tort à Microsoft. Il a conclu que le *Stored Communication Act* produisait des effets en fonction du contrôle effectif du fournisseur de service sur les données, et non en fonction du lieu où les données se trouvent. Selon le juge, la communication des données ne constituait pas une atteinte à la souveraineté étrangère et ne constituait pas une application extraterritoriale du *Stored Communication Act*[28].

25 In Re Grand Jury Proceedings the Bank of Nova Scotia.united States of America, Plaintiff, appellee, v. the Bank of Nova Scotia, Defendant, appellant, 740 F.2d 817 (11th Cir. 1984), https://law.justia.com/cases/federal/appellate-courts/F2/740/817/233788/. Voy. notamment B. Stern, « Une tentative d'élucidation du concept d'application extraterritoriale », *Revue québécoise de droit international*, n° 3, 1986.

26 Les MLTAS font l'objet de critiques récurrentes mettant en avant leur lourdeur et leur inefficacité par rapport à la volatilité des données électroniques. Voy. notamment à ce sujet : S. Vergnolle, P. Swire, J. Hemmings, « A Mutual Legal Assistance Case Study: the United States and France », *Wisconsin International Law Journal*, 2017, vol. 34, pp. 119 et s., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2921289.

27 *Treaty Between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters, signed at Washington on January 18, 2001*, https://www.congress.gov/107/cdoc/tdoc9/CDOC-107tdoc9.pdf. Ce traité doit être lu à la lumière de l'Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire, *J.O.*, L 181, 19 juillet 2003, pp. 0034-0042 et de « l'instrument » juridique pris en application de l'article 3.2. de cet accord visant à appliquer les provisions de l'accord EU-US aux traités bilatéraux négociés antérieurement par les États membres. En l'occurrence, pour l'Irlande : *Instrument as contemplated by Article 3(2) of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003, as to the application of the Treaty between the Government of Ireland and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters signed 18 January 2001, done at Dublin on 14 July 2005*, https://www.dfa.ie/media/dfa/alldfawebsitemedia/treatyseries/uploads/documents/legaldivisiondocuments/treatyseries2011/no.-4-of-2011.pdf.

28 In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

Le mandat a donc été confirmé[29].

3. *Décision de réformation en appel*

La Cour d'appel du Second Circuit a été saisie en appel par Microsoft.

Par un arrêt du 24 janvier 2017 très attendu, la Cour a infirmé la décision d'instance et a invalidé le mandat[30]. La Cour a suivi l'argumentation de Microsoft et a conclu ne pas trouver, dans le corps du *Stored Communication Act*, d'indices démontrant une volonté du législateur américain de lui conférer une portée extraterritoriale.

Malgré les *Amicus Briefs* introduits par la République d'Irlande et Monsieur Jan Philipp Albrecht pour le Parlement européen, le texte de l'arrêt ne mentionne pas la réglementation européenne en la matière.

Face à ce dangereux précédent[31], le ministère américain de la Justice a soumis l'affaire à la Cour Suprême.

Toutefois, avant qu'une décision ne soit rendue, le *Cloud Act* a été adopté par le Congrès. La loi clarifiant la situation, la Cour Suprême n'a pas continué l'instruction et le dossier a été classé[32].

III. LE *CLOUD ACT*

A. L'extension de l'accès aux données stockées à l'étranger

L'objet principal du *Cloud Act* est d'ajouter le paragraphe suivant au *Stored Communication Act*:

> *§ 2713. Required preservation and disclosure of communications and records.*
> *"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."*

Ce paragraphe étend la possibilité prévue à l'article 2703 du *Stored Communication Act* d'obtenir d'un fournisseur de service de communication électronique qu'il conserve ou transmette à l'autorité certaines données, et ce même si les données se trouvent sur un territoire étranger.

La conception assez large des sociétés américaines au sens du droit américain, soit une société constituée aux États-Unis ainsi que les sociétés contrôlées par elle, renforce encore le caractère extraterritorial de la législation.

Il ne suffit pas que les données soient stockées à l'étranger sur des serveurs gérés par une filiale pour échapper au *Stored Communication Act* tel qu'étendu par le *Cloud Act*.

29 Pour une analyse historique du cas et des conséquences éventuelles de celui-ci sur l'économie américaine des fournisseurs de services cloud, voy. N. Schultheis, «Warrants in the Clouds: How Extra-territorial Application of the Stored Communications Act Threatens the United States Cloud Storage Industry», *Brooklyn Journal of Corporate, Financial and Commercial Law*, Vol. 9, No. 2, 2015.

30 United States Court of Appeals, Second Circuit, IN RE: a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation Microsoft Corporation, appellant, v. United States of America, appellee, 14-2985, Decided: January 24, 2017, https://caselaw.findlaw.com/us-2nd-circuit/1768498.html.

31 Le ministère disposait toutefois au moins d'une décision favorable rendue par un juge fédéral dans un cas proche concernant Google, In re Search Warrant No. 16 – 960 – M – 01 to Google, No. 16-1061-M, 2017 WL 471564 (E.D. Pa. Feb. 3, 2017), https://case-text.com/case/in-re-search-warrant-no-16-1061-m-to-google.

32 Voy. notamment la réaction de Microsoft accueillant l'entrée en vigueur du *Cloud Act*: https://blogs.microsoft.com/datalaw/initiative/reforming-laws/clarifying-lawful-overseas-use-of-data-cloud-act/.

B. Les mécanismes formels de demande d'accès aux données restent identiques

Notons que le *Cloud Act* n'a pas d'impact sur le formalisme procédural nécessaire pour mettre la main sur ces données. Les forces de l'ordre devront encore obtenir un mandat ou une *subpoena* selon les cas prévus par le *Stored Communication Act*[33].

La protection du Quatrième Amendement garantie par le *Stored Communication Act* est toujours d'application et les sociétés recevant un mandat ou une *subpoena* disposeront des mêmes droits et bases juridiques qu'auparavant pour contester la licéité de ces documents.

Elles pourront invoquer les principes traditionnels d'application territoriale du droit et en contester les effets extraterritoriaux en se basant sur d'autres règles de droit, comme les règles de courtoisie internationale et de respect mutuel (« *doctrine of international comity* »)[34].

Notons encore que, pour être invoquée avec succès, cette doctrine exige une application concrète de la loi conflictuelle dans l'État tiers et un risque concret de condamnation pour les entreprises se trouvant en situation de conflit de lois. Le poids de l'argument variera en fonction de l'effectivité réelle du RGPD dans l'État membre éventuellement concerné.

C. Nouveau recours ouvert aux fournisseurs de service

Le *Cloud Act* introduit une procédure complémentaire ouverte aux fournisseurs de services afin de contester la légalité de la demande portée devant eux :

> *"A provider of electronic communication service to the public or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes:*
>
> *'(i) that the customer or subscriber is not a United States person and does not reside in the United States; and*
> *'(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government."*

1. Les conditions

La première condition est relative à la qualité du client ou de l'utilisateur du service. Celui-ci ne doit pas être un ressortissant américain (« *US person* »)[35] et ne doit pas résider sur le territoire américain.

La seconde condition est relative à l'existence d'un risque de conflit avec les lois d'un gouvernement étranger éligible. Ce concept de gouvernement étranger éligible est défini par le *Cloud Act* comme étant un gouvernement étranger avec lequel les États-Unis ont conclu un accord exécutif, soit un type particulier d'accord international.

Si ces deux conditions cumulatives sont remplies, le fournisseur de services peut alors introduire une requête en modification ou en annulation du mandat ou de la *subpoena*. Ce mécanisme de recours vise à éviter que le fournisseur de service

33 Ce qui est confirmé par le livre blanc du département de la Justice, USA DoJ, White Paper, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the Cloud Act*, April 2019, www.justice.gov/CLOUDAct.

34 Voy. à ce sujet, W. Dodge, « International Comity in American Law », *Columbia Law Review*, vol. 115, n° 8.

35 Au sens de : un citoyen ou ressortissant des États-Unis, un étranger légalement admis pour résidence permanente, une association non constituée en société dont un nombre important de membres sont des citoyens des États-Unis ou des étrangers légalement admis pour la résidence permanente, ou une société qui est incorporée aux États-Unis.

ne se retrouve dans une inconfortable situation de conflit de lois.

À l'heure actuelle, les possibilités d'un tel recours sont toutefois limitées dès lors qu'il n'existe pas encore d'accord exécutif de ce type entre l'Union européenne et les États-Unis.

2. La procédure d'introduction et d'examen du recours

Le *Cloud Act* décrit le formalisme d'introduction et d'examen de ces requêtes en modification ou en annulation.

Le recours doit être introduit dans les 14 jours de la signification du mandat ou de la *subpoena*, sauf dérogation contenue dans l'accord exécutif pertinent. L'autorité publique qui a fait signifier le mandat ou la *subpoena*, dispose d'un droit de réponse.

Le tribunal ne peut modifier ou annuler la procédure, selon le cas, que s'il constate que :

- la divulgation requise obligerait le fournisseur à enfreindre les lois d'un gouvernement étranger éligible ;
- le client ou l'abonné n'est pas ressortissant des États-Unis et ne réside pas aux États-Unis ;
- compte tenu de l'ensemble des circonstances, l'intérêt de la justice impose que la procédure judiciaire soit modifiée ou annulée.

Ces conditions sont cumulatives. Le pouvoir d'appréciation du magistrat siège dans la troisième condition.

3. Critères d'appréciation – Comity Analysis

Le *Cloud Act* prévoit que le tribunal, dans son appréciation de cette troisième condition (l'analyse de courtoisie ou « *Comity Analysis* »), doit prendre en compte les critères suivants :

- les intérêts des États-Unis, y compris les intérêts en matière d'enquête de l'entité gouvernementale cherchant à exiger la divulgation ;
- l'intérêt du gouvernement étranger éligible à empêcher toute divulgation interdite ;
- la probabilité, l'ampleur et la nature des sanctions imposées au fournisseur ou à l'un de ses employés en raison de l'incohérence des exigences légales imposées au fournisseur ;
- le lieu et la nationalité de l'abonné ou du client dont l'accès aux communications est recherché, si elles sont connues, ainsi que la nature et l'étendue du lien de l'abonné ou du client avec les États-Unis, ou si la procédure judiciaire a été demandée pour le compte d'une autorité étrangère en vertu d'un accord exécutif, la nature et l'étendue du lien de l'abonné ou du client avec le pays de l'autorité étrangère ;
- la nature et l'étendue des liens et de la présence du fournisseur de services aux États-Unis ;
- l'importance pour l'enquête des informations devant être divulguées ;
- la probabilité d'un accès rapide et efficace aux informations devant être divulguées par des moyens qui auraient des conséquences négatives moins graves ; et
- si la procédure judiciaire a été demandée au nom d'une autorité étrangère en vertu d'un accord exécutif, l'intérêt de l'enquête de l'autorité étrangère à l'origine de la demande d'assistance.

D. La possibilité de conclure des accords exécutifs avec des gouvernements étrangers

La notion de gouvernement étranger éligible – cruciale pour la détermination de la possibilité de recours exposée ci-dessus – s'applique aux gouvernements étrangers avec lesquels un accord exécutif est conclu selon les modalités prévues au chapitre 119 du *Stored Communication Act*. Un tel accord n'existe pas encore entre l'Union européenne et les USA, ni entre un des États membres et les USA.

Ces traités viseraient à mettre en place une certaine forme de réciprocité entre les parties. Un État pourrait donc, sur cette base, obtenir des informations ou des contenus de communication électronique de la part d'un fournisseur de services américain. Le *Cloud Act* exclut toutefois immédiatement que la réciprocité puisse porter sur des données de ressortissants américains. Cela n'est pas précisé, mais cette logique devrait également s'appliquer aux données des ressortissants du pays cocontractant de l'accord exécutif.

Le *Cloud Act* se réfère à la notion juridique d'accords exécutifs («*executive agreements*»), c'est-à-dire d'accords conclus par l'exécutif américain, sans que le consentement du Sénat ou des chambres du Congrès ne soit nécessaire. Ils peuvent toutefois s'y opposer *a posteriori*. Le *Cloud Act* comprend plusieurs exigences de qualité et de respect des droits fondamentaux par les gouvernements souhaitant négocier. Il est notamment requis que l'État soit partie à la Convention de Budapest sur la cybercriminalité ou que son droit national contienne des garanties et dispositions équivalentes.

E. L'impossibilité de conclure un accord exécutif avec l'Union européenne, le symptôme d'une relation compliquée en matière de données

De nombreux commentateurs ont souligné que le texte ne visait que les gouvernements étrangers, à l'exclusion des unions de pays. Bon nombre y voient une exclusion *de facto* de l'Union européenne, les USA préférant peut-être négocier bilatéralement avec chacun des États membres.

L'Union européenne, en tant que puissance économique et «cliente» importante des solutions technologiques américaines, devrait être un partenaire incontournable. En matière de flux de données, la relation entre les deux économies est pourtant compliquée.

Si les États-Unis avaient obtenu une refonte superficielle du *Safe Harbor* avec le *Privacy Shield*[36], le RGPD semblait idéal pour arracher des engagements plus stricts de respect des droits des citoyens européens par les GAFAM et autres entreprises américaines.

Le *Cloud Act* serait-il donc une mesure de rétorsion au RGPD ? Ou simplement une solution législative bricolée pour éviter une décision contraire de la Cour Suprême dans le dossier Microsoft ?

IV. L'ARTICULATION ENTRE LE RGPD ET LE *CLOUD ACT*[37]

A. Le champ d'application du RGPD

1. Champ d'application territorial[38]

Rappelons qu'au terme de l'article 3, 1., le RGPD s'applique au traitement des données à caractère personnel effectué dans le cadre

36 A. Cassart, «Les données personnelles expédiées aux U.S.A. arriveront-elles un jour à bon port ?», *J.L.M.B.*, 2017/26.

37 L'article n'aborde pas les questions relatives à la conformité du *Cloud Act* avec les autres garanties prévues dans les textes fondamentaux de l'Union européenne, ou dans les textes fondamentaux nationaux. Sur ces garanties, voy. notamment : E. Cape, R.-S. Namoradze, T. Sponken, *Effective Criminal Defence in Europe*, Maastricht, Intersentia, 2010. Sur l'implication du *Cloud Act* par rapport aux mécanismes européens transfrontaliers aux données électroniques et la coopération judiciaire en matière pénale, voy. notamment : M. Stefan, G. Gonzalez Fuster, «Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters – State of the art and latest developments in the EU and the US», *CEPS*, 3 décembre 2018, https://www.ceps.eu/ceps-publications/cross-border-access-electronic-data-through-judicial-cooperation-criminal-matters/.

38 De manière plus large, sur le champ d'application territorial du RGPD, voy. C. de Terwangne, «Définitions clés et champ d'application du RGPD», in C. de Terwangne, K. Rosier (dir.), *Le Règlement Général sur la Protection des Données (RGPD/GDPR). Analyse approfondie*, Bruxelles, Larcier, 2018, pp. 75 et s.

des activités d'un établissement[39] d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union.

L'article 3, 2., rend applicable le RGPD au traitement des données à caractère personnel relatif à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

Le champ d'application territorial[40] du RGPD est défini largement de manière à envisager le maximum de couverture et de protection. En conséquence, le RGPD va très rapidement trouver à s'appliquer aux sociétés américaines développant une activité vers l'UE, singulièrement les fameux GAFAM.

2. Champ d'application matériel[41]

L'article 2.1. du RGPD définit son champ d'application matériel en précisant qu'il s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. Le contenu des communications électroniques transmises via un prestataire de services soumis au *Cloud Act* tombe dans cette définition.

Par la conjonction de la largesse des critères retenus pour définir les champs d'application territorial et matériel, une société américaine, ou une de ses filiales européennes, se verra très aisément appliquer le RGPD.

L'article 2.2., qui contient quelques exceptions, ne lui sera guère d'une grande aide.

Certains pourraient toutefois noter que le RGPD ne s'applique pas aux traitements opérés par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces. Et de tirer argument de cette exception prévue par l'article 2.2., d), pour tenter d'en déduire qu'une demande des autorités américaines agissant aux fins décrites ci-dessus ne rentrerait pas dans le champ d'application matériel du règlement.

Cette exception n'est toutefois ouverte qu'aux autorités compétentes concernées par le RGPD et, plus largement, concernées par le droit de l'Union. Les autorités américaines ne sont pas tenues des règles du droit de l'Union. Elles ne peuvent donc pas bénéficier non plus des exceptions prévues par ces règles.

De plus, la difficulté liée au conflit de lois s'applique en amont du traitement réalisé par les autorités américaines sur les données qui lui seraient transférées. Le conflit de lois surgit lorsque les autorités américaines requièrent de l'entreprise sous juridiction américaine qu'elle transmette des données à caractère personnel, ce traitement étant soumis au RGPD. L'excep-

39 F. Coton, « L'établissement du responsable de traitement de données, une notion clé », *J.L.M.B.*, 2017/26.

40 F. Coton, J.-H. Henrotte, « Application territoriale de la législation européenne en matière de protection des données et transfert de données vers des pays tiers : vaincre la peur de l'autre », in *Les enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015.

41 De manière plus large, sur le champ d'application matériel du RGPD, voy. C. de Terwangne, « Définitions clés et champ d'application du RGPD », in C. de Terwangne, K. Rosier (dir.), *Le Règlement Général sur la Protection des Données (RGPD/GDPR). Analyse approfondie*, Bruxelles, Larcier, 2018, pp. 69 et s.

tion ouverte aux traitements réalisés par les autorités compétentes ne trouvera pas à s'appliquer. Car l'exception doit être examinée du point de vue de l'acteur privé qui reçoit l'injonction d'une autorité.

Enfin, l'article 48 du RGPD est particulièrement clair et contredit cette position.

B. Le conflit de lois paraît inévitable

RGPD et *Cloud Act* entrent de plein fouet en collision.

Une enquête américaine relative à des intérêts américains pourrait, sur la base du *Cloud Act*, donner lieu à un mandat exigeant un transfert de données concernant, par exemple, un citoyen européen, données hébergées et traitées sur le territoire de l'UE. Et ce en dehors de tout cadre légal européen ou national, sans aucun contrôle d'une autorité européenne et fort peu de recours effectifs[42] ouverts à la personne concernée.

Un tel transfert contreviendrait tant à l'article 44 qu'à l'article 48 du RGPD.

L'article 44 pose le principe général d'interdiction des transferts de données, sous réserve des exceptions prévues dans le Chapitre V du RGPD.

L'article 48 du RGPD vise quant à lui explicitement l'hypothèse créée par l'application du *Cloud Act*. Cet article précise que toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert reconnus par le RGPD.

En l'occurrence, il n'existe pas d'accord exécutif au sens du *Cloud Act* ni de motifs justifiant un tel transfert sur une base autre que les éventuels traités d'entraide judiciaire existants.

1. Défaut d'accord exécutif

À l'heure de rédiger les présentes lignes, il n'existe, entre l'Union européenne et les États-Unis, aucun accord exécutif au sens du *Cloud Act*, ni plus largement aucun traité qui pourrait justifier, conformément à l'article 48, une demande d'une autorité d'un pays tiers adressée directement à un responsable de traitement devant respecter le RGPD. S'il existe un Traité d'entraide judiciaire entre UE et USA signé en 2003, celui-ci n'est toujours pas entré en vigueur[43]. Il ne prévoit par ailleurs pas de possibilité pour une autorité de s'adresser directement à un responsable de traitement, chaque demande doit passer par le truchement de la partie contractante au Traité[44].

42 En janvier 2017, l'Union européenne et la Belgique ont été approuvées en tant que « *Covered countries* » au sens du *Judicial Redress Act*, en application de l'accord *Umbrella*. Cette loi ouvre aux citoyens européens et belges certains droits et moyens de recours à l'encontre de certains traitements de données réalisés par l'administration américaine, dont le département de la Justice et de la Sécurité intérieure. L'activation de ces droits est toutefois complexe du fait du caractère international et du champ restreint de ces législations. Par ailleurs, il faut encore être informé du traitement de données.

43 Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire, signé le 25 juin 2003 à Washington, *J.O.*, L 181, 19 juillet 2003, pp. 34-42.

44 Il en est de même pour le traité conclu entre la Belgique et les USA, lui en vigueur depuis le 1er février 2010. Convention entre le Royaume de Belgique et les États-Unis d'Amérique concernant l'entraide judiciaire en matière pénale, signée à Washington le 28 janvier 1988, *M.B.*, 8 décembre 1999, nº 1999A15125 (version originale), *M.B.*, 8 mars 2010, nº 2009C15102 (version conforme à l'Accord entre l'Union européenne et les États-Unis d'Amérique en matière d'entraide judiciaire, signé le 25 juin 2003).

Outre le caractère récent et précipité du *Cloud Act* qui n'a pas permis une négociation en amont, les possibilités de conclure un tel accord sont limitées aux États et non à l'UE en tant que telle.

Par contre, les transferts de données basés sur un MLAT négocié entre les USA et un État membre ne contreviendraient pas à cet article 48.

2. *Inadéquation des autres motifs de transfert*

Les autres motifs de transfert prévus par le chapitre V du RGPD ne sont pas d'une grande aide non plus.

a. Pas de décision d'adéquation

Il n'existe pas de décision d'adéquation reconnaissant que les États-Unis assurent un niveau de protection adéquat au sens de l'article 45. Le mécanisme du *Privacy Shield* ne vise que les sociétés commerciales s'étant auto-certifiées, non les entités gouvernementales américaines.

b. Pas de garantie appropriée ni de BCR

Il ne peut pas non plus être question de transfert moyennant des garanties appropriées (notamment à défaut de pouvoir octroyer les droits et voies de droit effectives aux personnes concernées) ni de règles d'entreprise contraignantes (BCR).

c. Aucune des exceptions de l'article 49

Enfin, aucune des exceptions contenues à l'article 49 ne peut s'appliquer. Si le texte de l'article 49, d), vise des transferts pour des motifs importants d'intérêt public, il s'agit de motifs d'intérêt public propres à un État membre ou à l'UE, mais pas l'intérêt public propre à un État tiers, sauf éventuellement dans une hypothèse de réciprocité issue d'un traité international[45].

3. *En conséquence, il existe un risque non négligeable de sanctions concurrentes*

Une société américaine recevant un mandat l'obligeant à transmettre des documents stockés sur des serveurs européens ou concernant des citoyens européens se trouve donc dans une situation inconfortable.

Des deux côtés, elle est soumise à un risque de sanction : aux USA, pour défaut de collaboration à la suite du mandat qui lui a été signifié, et dans l'UE, amendes administratives pouvant s'élever jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent.

V. CONCLUSION

Contrairement à ce qui a pu être dit dans les jours ayant suivi l'irruption du *Cloud Act*, celui-ci n'est pas un blanc-seing permettant au gouvernement américain d'accéder à n'importe quelle donnée, quelle que soit sa localisation. Il ne concerne que les sociétés sous juridiction américaine, notion très large il est vrai, et ne diminue pas les garanties prévues par le *Stored Communication Act*, d'autres textes ou la jurisprudence américaine.

Il n'en reste pas moins que le *Cloud Act* et le RGPD se trouvent dans une situation d'incompatibilité critique[46].

Les parties prenantes en sont bien conscientes. Très rapidement, la Commissaire européenne, Madame Jourova, a annoncé qu'elle souhaitait conclure un accord avec l'*Attorney General* américain afin que l'Union européenne soit considérée comme un gouvernement étranger

[45] EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 mai 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf.

[46] A. Gidari, *What will Microsoft and Ireland do with the new Cloud Act warrant?*, The Center for Internet and Society at Stanford Law School Blog, 9 avril 2018, http://cyberlaw.stanford.edu/blog/2018/04/what-will-microsoft-and-ireland-do-new-cloud-act-warrant.

éligible au sens du *Cloud Act*[47]. Le communiqué de presse de la réunion EU – US qui s'en est suivi ne le mentionne toutefois pas explicitement[48].

La Commission a également proposé deux projets, de règlement[49] et de directive[50] *eEvidence*, qui pourraient servir de réponse et de cadre pour la négociation d'un texte avec les USA[51].

En février 2019, en se basant sur les conclusions de la réunion du Conseil européen d'octobre 2018, la Commission européenne a publié une recommandation au Conseil suggérant de dégager un mandat en vue de dialoguer avec les États-Unis sur ces questions[52].

En juillet 2019, l'European Data Protection Board et l'European Data Protection Supervisor ont publié une lettre commune adressée au Comité LIBE sur l'impact du *Cloud Act*[53]. Cette lettre encourage l'Union européenne à dégager un terrain d'entente avec les USA et à rendre à tout le moins réciproque les obligations des uns et des autres.

Il semble en effet que la seule solution raisonnable est de discuter directement entre l'UE et les USA afin de trouver un terrain d'entente respectueux des droits de chacun, et particulièrement des citoyens. La rigueur dans l'application du RGPD doit toutefois être de mise dans le chef des Européens.

D'une part, il est essentiel que l'UE ne perde pas sa crédibilité en n'appliquant pas les sanctions prévues aux entreprises enfreignant l'article 48 du RGPD. Selon un auteur réputé sur ce point, les meilleurs accords sont négociés après des manifestations de force[54].

D'autre part, sans ce signal clair, il sera plus difficile pour les fournisseurs de service d'invoquer devant les juridictions américaines la doctrine de courtoisie internationale qui implique de prouver l'effectivité de la loi étrangère qui entrerait en conflit avec la loi nationale[55].

En conclusion, il convient d'aller jusqu'au bout de la logique et du *momentum* initiés par le RGPD sans tarder et de dégager une solution cohérente. À défaut, non seulement les entreprises risquent de se trouver dans d'inconfortables incertitudes, mais le RGPD est susceptible d'être décrédibilisé et, avec lui, tous les principes de protection des données dont il se veut le champion.

47 https://www.euractiv.com/section/data-protection/news/jourova-to-press-for-eu-us-data-sharing-deal-next-week/.

48 http://europa.eu/rapid/press-release_STATEMENT-18-3906_en.htm.

49 Proposal for a Regulation of the European Parliament and ff the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM/2018/225 final – 2018/0108(COD) https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:225:FIN.

50 Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings COM/2018/226 final – 2018/0107 (COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1524129181403&uri=COM:2018:226:FIN.

51 R. Bismuth, « Le *Cloud Act* à la lumière du projet européen e-evidence », *Expertises*, 439, 2018.

52 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 février 2019, https://ec.europa.eu/info/sites/info/files/recommendation_council_decision_eu_us_e-evidence.pdf.

53 EPDB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 12 juillet 2019, https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

54 D. Trump, T. Schwartz, *The art of the deal*, New York, Random House, 1987.

55 M. Lemperiere, « Le *Cloud Act* : origines et conséquences », *Expertises*, 437, 2018.