BANQUE DES MÉMOIRES

Master de Droit du numérique
Dirigé par Monsieur Jérôme PASSA
2020

Le régime d'accès aux données du CLOUD ACT et son conflit avec le Règlement général sur la protection des données (RGPD)

Myriam BOUET-DIAF

Sous la direction de Madame le Professeur Nana BOTCHORICHVILI

Remerciements

Je tiens à remercier Monsieur le Professeur Jérôme PASSA pour m'avoir donné l'opportunité d'accéder à la richesse des savoirs transmis par l'équipe enseignante du Master 2 de Droit du numérique.

Je remercie tout particulièrement à Madame le Professeur Mérav GRIGUER pour ses enseignements en protection des données personnelles reçus à l'Université Panthéon-Assas et à Sciences-Po.

Mes remerciements s'adressent enfin à Madame le Professeur Nana BOTCHORICHVILI pour m'avoir fait l'honneur de diriger mon mémoire et pour ses précieux conseils.

SOMMAIRE

INTRODUCTION

1. D'après les statistiques mises à la disposition du public par la Commission européenne[1], 85 % des enquêtes pénales font intervenir des données numériques. Dans la moitié des cas, une demande transfrontière d'accès à ces données est formulée. Outre-Atlantique, le Department of Justice (DoJ)[2] dresse un constat similaire en indiquant qu'il lui est plus que jamais nécessaire *« de s'assurer un accès effectif aux preuves électroniques où qu'elles se trouvent[3] »*. La convergence de ces analyses aboutit à un même état de fait : dans un monde structuré par les systèmes d'information, les autorités répressives européennes et américaines sont amenées à procéder à une collecte des données en dehors de leurs frontières[4].

2. La notion de « preuve numérique», indifféremment appelée « preuve électronique », ne fait l'objet d'aucune définition juridique dans la législation européenne ou américaine. Néanmoins, il convient de l'appréhender via son format informatique et via les données auxquelles elle renvoie. La preuve numérique est une donnée immatérielle qui constitue le support d'indices digitaux[5] grâce auxquels la culpabilité ou l'innocence d'une personne pourront être établies au cours d'un procès. Pour être utile, la donnée en question doit véhiculer des informations rendant l'individu ciblé par l'enquête, identifiable. Cette preuve peut donc être qualifiée de donnée personnelle au sens du Règlement (UE) 2016/679 (RGPD)[6], en tant qu'elle recouvre une *« information se rapportant à une personne physique identifiée ou identifiable (…) directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale[7]»*. Conscient que l'enquête pénale entraîne la manipulation de données susceptibles de singulariser des individus, le législateur européen ne s'est pas contenté d'abroger la directive 95/46/CE[8] par l'adoption du RGPD. Il a aussi prévu une Directive (UE) 2016/680 dédiée à la protection des données personnelles dans le cadre

1 https://www.consilium.europa.eu/fr/policies/e-evidence/
2 28 U.S.C § 501
3 U.S Department of Justice, *Promoting Public Safety, Privacy and the Rule of Law Around the World : the Purpose and Impact of the Cloud Act*, White Paper, April 2019, p. 2
4 V. Franssen, A. Berrendorf, M. Corhay, *La collecte transfrontière de preuves numériques en matière pénale. Enjeux et perspectives européennes*, eRIDP, 2019, p. 2
5 M. Quéméner, *La preuve numérique dans le cadre pénal*, Fasc Jcl 1105, 28 avril 2019, p.2
6 Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (Règlement général sur la protection des données, RGPD) entré en application le 25 mai 2018 dans les États membres de l'UE.
7 Art. 4§1, RGPD
8 Directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données

des activités de police et de justice. Ensemble, ces deux textes composent un « paquet européen» qui fait de la donnée le support de droits personnels.

3. Face aux difficultés rencontrées par les autorités judiciaires pour accéder aux preuves numériques[9], un certain nombre d'Etats membres[10] et d'Etats observateurs[11] du Conseil de l'Europe ont ratifié la Convention de Budapest sur la cybercriminalité, ouverte à la signature le 23 novembre 2001. C'est notamment le cas des Etats-Unis et des Etats-membres de l'UE à l'exception de l'Irlande et de la Suède[12]. Ce texte est le premier traité international relatif aux crimes et délits informatiques et/ou commis à l'aide des systèmes d'information. Ayant pour but d'harmoniser les techniques d'enquête et de favoriser la coopération judiciaire tout en assurant une protection adéquate des droits de l'Homme, la Convention de Budapest n'en demeure pas moins sensible à la protection des données personnelles. Elle renvoie ainsi à la Convention 108 de 1981[13], premier instrument juridique international contraignant dans ce domaine. Bien que ratifiée par l'ensemble des Etats-membres de l'UE, la Convention 108 ne l'a cependant pas été par les Etats-Unis. De son côté, la Convention de Budapest répartit les données en trois catégories : les données de trafic, les données de contenu et celles de l'utilisateur ou métadonnées. Les données de trafic[14] sont les informations générées par l'utilisation des réseaux de communication et indispensables à leur fonctionnement: adresse IP de l'ordinateur, date, heure et durée de chaque connexion. Elles doivent être conservées pendant une durée spécifique pour les besoins de l'enquête pénale. Ensuite, les données de contenu correspondent au *« contenu informatif de la communication, à savoir le sens de la communication ou le message ou l'information transmis par la communication autre que les données relatives au trafic*[15] ». Elles permettent le plus souvent d'identifier l'auteur et/ou le destinataire d'un message et constituent parfois à elles seules des éléments à charge ou à décharge[16]. Enfin, les données de l'utilisateur, de l'abonné ou encore les métadonnées permettent de reconstituer les détails de la vie d'une personne : habitudes, lieux de séjour, déplacements, activités exercées, environnement et milieux sociaux fréquentés[17]. Bien qu'elles n'aient pas toutes la même

9 Conseil de l'Europe, Convention sur la cybercriminalité - STE 185, Budapest, 23.XI.2001, *Préambule*
10 47 États membres dont les 27 États membres de l'UE
11 6 États observateurs dont les États-Unis d'Amérique depuis le 7 décembre 1995 conformément à la résolution (95)37
12 https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures
13 Conseil de l'Europe - Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel – STE 108 - Strasbourg, 28.I.1981 ;
14 Article 1 (d) , Convention sur la cybercriminalité - STE 185
15 Rapport explicatif de la Convention sur la cybercriminalité – STE 185 – Cybercriminalité (Convention), Chapitre II, Section 1, Titre 5 *Collecte en temps réel des données informatiques*, § 209, p.40
16 Th. Christakis, *Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques*, CEIS Group Chekoff, Décembre 2017, p.19
17 M.Quéméner, *Ibidem*, p.3

valeur informative, ces trois catégories de données sont utilisées, en matière pénale, pour établir un lien entre une information et un individu.

4. Avec le développement de l'informatique en nuage et des data centers, les preuves sont *« de plus en plus stockées sur des serveurs hébergés dans des juridictions étrangères, multiples, fluctuantes ou inconnues, autrement dit dans le Cloud*[18] *» ;* et ce, alors que les pouvoirs des services répressifs restent limités par les frontières territoriales. En effet, *« les lois pénales s'appliquent sur l'ensemble du territoire à toute personne s'y trouvant et (…) le juge peut les appliquer pour toute infraction commise sur le territoire*[19] *»*. Pour surmonter la difficulté suscitée par ce strict principe de compétence territoriale, la Convention de Budapest crée différents critères de rattachement entre l'Etat et les données. Par exemple, l'injonction de production des données d'un utilisateur est fondée sur le critère du lieu où sont offerts les services[20]. En revanche, les injonctions de production des données de trafic et de contenu dépendent de la présence de la personne visée par l'enquête[21] sur le territoire de l'État à l'origine de la requête. Ces critères de rattachement accroissent mécaniquement la compétence extraterritoriale des Etats qui peut être définie comme *« tout ou partie du processus d'application d'une norme (…) en dehors du territoire de l'État qui l'a émise*[22] *»* et comme « *la prétention d'un Etat à appréhender, à travers son ordre juridique, des éléments situés en dehors de son territoire*[23] *»*. Malgré le caractère novateur de la Convention de Budapest en 2001, les techniques informatiques ne cessent de se réinventer et la cybercriminalité également. En conséquence, les initiatives juridiques se multiplient. A l'échelle internationale, le Conseil de l'Europe prépare un second protocole à la Convention de Budapest et l'Assemblée générale des Nations-Unies vient de voter une résolution pour l'adoption d'un Traité sur la cybercriminalité. A l'échelle des Etats, les Etats-Unis ont adopté le Clarifying Law Overseas Use of Data Act (CLOUD Act) le 23 mars 2018 ; à leur suite, la Commission européenne a présenté une proposition de Règlement relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale[24].

5. Outre-Atlantique, la question de l'accès transfrontière aux preuves numériques s'est posée avec une particulière acuité à l'occasion de l'affaire *Microsoft Corp v. United States*, autrement appelée *Microsoft Ireland case*. En 2013, en effet, le DoJ enjoint à Microsoft de lui communiquer

18 Coopération internationale renforcée sur la cybercriminalité et les preuves électroniques : vers un protocole à la Convention de Budapest, 19 mars 2017
19 E.David, Éléments *de droit pénal international et européen*, 2ème éd, Bruxelles, Bruylant, 2018, p.35
20 Article 18 § 1 (b) , Convention sur la cybercriminalité, STE 185
21 Article 18 § 1 (a), *Supra ibidem*
22 Propos de B. Stern cités in J. Salmon (éd.), *Dictionnaire de droit international public*, Bruylant, 2001, p.211
23 *Supra Ibidem*
24 Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale

les données de contenu (mails) et celles de souscription d'un utilisateur soupçonné de trafic de stupéfiants. Pour ce faire, l'autorité gouvernementale s'appuie sur un mandat de perquisition, appelé *SCA warrant* et délivré par un magistrat[25] conformément à la Section 2703 (a) du Stored Communications Act (SCA)[26]. L'entreprise considère alors que ce mandat doit respecter la disposition du Federal Rules of Criminal Procedures (FCPR), selon laquelle un tel acte doit être exécuté sur un territoire ou une possession des Etats-Unis[27]. Microsoft accepte donc de ne communiquer aux enquêteurs que les données de souscription de son client et non ses mails, stockés en Irlande. Remettant en cause la portée extraterritoriale du mandat, l'entreprise avance deux arguments d'importance. D'une part, les données de contenu de son client ne peuvent être obtenues par le Gouvernement américain qu'en vertu d'un Traité d'entraide judiciaire[28]. D'autre part, l'exécution éventuelle du *SCA warrant* dont le DoJ se prévaut, conduirait à un conflit de lois avec la directive 95/46/CE qui interdit les transferts de données vers les Etats-Unis en l'absence de décision d'adéquation[29]. Malgré ces arguments, elle est déboutée en première instance. Elle interjette donc appel devant la Cour du Second Circuit de New York[30] qui s'appuie alors sur un *Morrison test*[31] pour apprécier si le législateur a souhaité donner une portée extraterritoriale au mandat en question. En effet, selon une jurisprudence constante et ancienne, les lois américaines sont présumées être d'application territoriale[32]. Cette présomption est toutefois simple et peut être renversée si la loi comporte des dispositions explicitement contraires. Après avoir identifié l'objectif *(focus)* du SCA comme étant la protection de la vie privée[33], le juge d'appel conclut que l'exécution du mandat reviendrait à lui donner une portée extraterritoriale générant un conflit avec la loi irlandaise de transposition de la directive 95/46/CE. Bien que cette décision d'appel n'ait pas été suivie[34], le DoJ saisit la Cour Suprême qui accepte de réviser l'affaire en octobre 2017. Finalement, la Cour est interrompue dans sa démarche par le Congrès, qui vote le CLOUD Act le 23 mars 2018 et apporte donc une réponse législative au litige. Le DoJ obtient gain de cause et la Cour Suprême classe l'affaire.

25 United States District Court for the Southern District of New York
26 18 U.S.C § 2703 (a)
27 FRCP, Title VIII, Rule 41, (b) (5) (A)
28 https://www.congress.gov/treaty-document/107th-congress/9?s=1&r=16
29 Article 25 § 1 de la directive 95/46/CE
30 U.S Court of Appeal for the Second Circuit of New York
31 *Morrison v. National Australia BankLtd*, 561 U.S. 247, 130S. Ct. 2869 (2010)
32 W.S Dodge, *Morrison's Effects Tes*t, University of California, Hastings College of the Law, 2011
33 *In re* Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corp, . 829F. 3D, 56
34 I*n re* Search Warrant No. 16-960-M-01 to Google ; In re Search of Premises Located at (reddacted) @yahoo.com, Stored at Premises Owned, Maintained, Controlled or Operated by Yahoo, Inc, No. 6:17-mj-1238 (M.D.Fla.April 7, 2017)

6. Le CLOUD Act s'articule autour de deux parties. La première précise les champs d'application personnel et matériel de la loi et crée une nouvelle voie de recours. La seconde pose le cadre bilatéral de coopération proposé aux Etats tiers pour accéder aux preuves numériques relevant des juridictions américaines. Ce cadre a un double objectif : juguler les conflits de lois et contourner la lourdeur des Traités d'entraide judiciaire[35].

7. La principale innovation du CLOUD Act consiste à légaliser la pratique des autorités gouvernementales, jusque-là informelle[36] , consistant à accéder aux données stockées en dehors des Etats-Unis, directement auprès des fournisseurs américains[37]. L'appréciation de la portée du CLOUD Act nécessite de se pencher sur son régime (I). Etant donné que, par ailleurs, de nombreux data centers des « géants du Web » sont situés sur le territoire de l'UE et que le RGPD protège l'accès aux données qui y sont traitées, un conflit de loi entre la législation américaine et la législation européenne semble inévitable. En conséquence, il faudra se pencher sur la substance de ce conflit, son anticipation par les parties et les tentatives de résolution mises en oeuvre (II)

35 U.S Department of Justice, *Ibidem*, p.2
36 18.U.S.C § 2510 (6) (7)
37 18 U.C.S § 2713

I/ CLOUD ACT : UN NOUVEAU RÉGIME D'ACCÈS AUX DONNÉES POUR LES AUTORITÉS GOUVERNEMENTALES AMÉRICAINES

8. Le CLOUD Act fait obligation aux fournisseurs américains de services numériques, de faire droit aux demandes gouvernementales d'accès aux données, indépendamment du lieu de leur stockage (A). Même si le texte ne modifie pas le formalisme procédural de la requête, il crée une voie d'opposition spécifique au bénéfice des entreprises concernées (B).

A – Principe : le caractère indifférent du lieu de stockage des données

9. Ce principe, qui constitue la nouveauté principale du texte, découle des champs d'application personnel (1) et matériel (2) du CLOUD Act .

1 – Le champ d'application personnel du CLOUD Act et sa portée extraterritoriale

10. En vertu du CLOUD Act, *«un fournisseur de service de communication électronique ou un fournisseur de service informatique distant* [38] *», « soumis aux juridictions américaines* [39]*»,* est tenu de transmettre aux autorités les données du client ou de l'abonné qu'il a *« en sa possession, sous sa garde ou sous son contrôle, peu importe que la communication, l'enregistrement ou l'information en question soient localisés sur le territoire ou en dehors du territoire américain*[40] *»*. Trois critères cumulatifs permettent ainsi de caractériser les prestataires de services visés : d'une part, ils doivent appartenir à la catégorie des fournisseurs de service de communication électronique *(ECS*[41]*)* ou à celle des fournisseurs de services informatiques distants (*RCS*[42]*) ;* d'autre part, ils doivent disposer du contrôle, de la garde ou avoir en leur possession les données du client ou de l'abonné requises; enfin, ils doivent être soumis aux juridictions américaines. Ces trois critères font l'objet de précisions légales et jurisprudentielles qu'il convient de détailler, dans un souci de compréhension de la portée du CLOUD Act.

38 18 U.S.C § 2713
39 18 U.S.C.A SEC. 102 (2)
40 18 U.S.C § 2713
41 Electronic communication service
42 Remote computing services

11. Tout d'abord, l'Electronic Communications Privacy Act (ECPA), ensemble de trois textes législatifs adopté en 1986[43] et dont le SCA fait partie, énonce qu'un ECS couvre *« tout service qui fournit à ses utilisateurs la capacité d'envoyer ou de recevoir des communications filaires ou électroniques[44] »* tandis qu'un RCS permet « *la fourniture au public de services de stockage informatique et de traitement informatique par le biais d'un système de communication électronique[45] [46]*». Le DoJ cite plusieurs exemples d'entreprises dont les activités entrent alternativement ou cumulativement dans l'une ou l'autre de ces deux catégories : les fournisseurs de boîtes mails, les opérateurs de téléphonie mobile, les plateformes de médias sociaux, les sites de mise en réseau social ou encore les prestataires de Cloud[47]. De leur côté, les juges du fond ont été amenés à qualifier les fournisseurs de boîtes mails[48] et les sites de mise en réseau social[49], à la fois d'ECS et de RCS. Le DoJ précise à cet égard que la qualification de fournisseur de services numériques est indifférente à une quelconque *« insertion dans le réseau Internet[50] »*. Deux remarques peuvent ici être faites : d'abord, la frontière entre ECS et RCS n'est pas étanche ; en outre, tout dépend de l'appréciation du juge du fond, au cas par cas.

12. Ensuite, le prestataire de services doit exercer un contrôle sur les données demandées. A la lumière du rapport explicatif de la Convention de Budapest, cette notion de contrôle peut être comprise comme faisant référence à *« des situations dans lesquelles l'intéressé ne possède pas matériellement les données (…) mais peut contrôler librement leur production depuis le territoire de la partie en ayant ordonné la communication*[51]». Le contrôle ne requiert donc pas la détention d'un titre de propriété[52] sur les données. Il implique plutôt une capacité technique à les traiter. Néanmoins, *« la simple possibilité technique d'accéder à des données stockées à distance (…) ne constitue pas nécessairement un contrôle [53]»* au sens de l'article 18 de la Convention. La mise en place par le législateur américain de ce second critère pour caractériser les prestataires de services numériques fait écho à l'argument soulevé par le DoJ dans l'affaire Microsoft. Ce dernier soutenait,

43 The Wiretap Act, 18.U.S.C §§ 2510-2522 ; the Pen Register and Pen and Trap and Trap Statute, 18 U.S.C §§ 3121-3127 ; The Stored Communication Act (SCA), 18 U.S.C §§ 2701-2712
44 18 U.S.C § 2510 (15)
45 18 U.S.C § 2711 (2)
46 18.U.S.C § 2510 (12)
47 Department of Justice, *Ibidem*, p.16
48 *United States v. Weaver,* 636 F. Supp. 2D 769 (C.D.III, 2009)
49 *People v. Harris*, 36 Misc. 3D 613, 945 N.Y.S 2d 505 (N.Y City Crim. Ct.2012) ; *People v. Harris,* 36 Misc. 3D 868, 949, N.Y.S 2d, 590 (N.Y.City Crim. Ct. 2012)
50 Department of Justice, *Ibidem,* p.16
51 Rapport explicatif de la Convention sur la cybercriminalité – STE 185 – Cybercriminalité (Convention), Chapitre II, Section 1, Titre 3, *Injonction de produire (article 18),* §173, p.34
52 Department of Justice, *Ibidem,* p.16
53 Rapport explicatif de la Convention sur la cybercriminalité – STE 185 – Cybercriminalité (Convention), *Supra Ibidem*

en effet, que les données demandées était en la possession de l'entreprise car *« à portée de clic [54]»* de son personnel de Redmond à Washington. Par conséquent, le mandat de perquisition n'avait rien d'extraterritorial[55]. Le CLOUD Act établit ainsi un lien de causalité entre le contrôle exercé par le prestataire sur les données et son obligation de divulgation. Un parallèle peut ici être dressé avec les dispositions du RGPD relatives au responsable de traitement[56] et au sous-traitant[57]. Là où le texte européen introduit une distinction entre celui qui définit les moyens du traitement et celui qui traite les données pour le compte de ce dernier, le CLOUD Act se dispense d'une telle distinction. Seul le contrôle, la possession ou la garde des données constituent un facteur déterminant. Il en résulte donc, que des responsables de traitement et des sous-traitants au sens du RGPD pourront, indifféremment, être qualifiés d'ECS ou des RCS.

13. Enfin, pour qu'un ECS ou un RCS soit soumis aux exigences du CLOUD Act, il doit être un sujet de droit américain[58], c'est à dire soumis à la compétence du juge des Etats-Unis. L'insistance du législateur sur le lien personnel qui unit les prestataires de services numériques et l'État américain a pour but d'obliger les premiers à obtempérer aux sommations gouvernementales[59] . L'affaire Microsoft en a fourni l'illustration la plus achevée. Se pose dès lors la question, au demeurant très débattue[60], de l'étendue de la compétence des juridictions américaines. Dans un souci de clarté du propos, le raisonnement s'en tiendra ici à appréhender cette compétence au travers de la définition légale de la « personne américaine » *(US person)* d'une part et d'autre part au travers de l'interprétation qu'en donne le DoJ en tant qu'il exécute les lois.

14. Au sens du Code of Federal Regulations (CFR), une entreprise est soumise aux juridictions américaines dès lors qu'elle peut être qualifiée de « personne américaine » *(US person)*[61]. Il en va ainsi alternativement des sociétés *« localisées sur le territoire des Etats-Unis[62] »*, de celles qui sont *« enregistrées sur le territoire américain[63] »* et de celles qui sont *« détenues ou contrôlées par un citoyen ou un résident des Etats-Unis quel que soit leur lieu d'enregistrement et leur lieu*

54 E. Mignon, *Le Cloud Act ou l'impuissance européenne démasquée*, Revue des Juristes de Sciences-Po n°16, Janvier 2019, p.4

55 *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, No. 14-2985, 2016 U.S.App LEXIS 12926, at 50 (2d Circuit) (Droney, J., dissenting)

56 Art. 4 § 7 RGPD

57 Art. 4§ 8 RGPD

58 18 U.S.C.A SEC.102 (2)

59 Department of Justice, *Ibidem*, p.8

60 R. Bismuth, *Fantasmes et réalités autour de l'extraterritorialité du droit américain*, RLDA, n°157, 1er mars 2020, p.2

61 La notion de « US person » englobe les personnes morales et physiques. Pour la clarté du propos, n'est abordée dans ce paragraphe que la personne morale de l'entreprise. Les personnes physiques assujetties au droit américain seront abordées plus loin dans le développement.

62 31 CFR § 515.329 (b)

63 31 CFR § 515.329 (c)

d'activité [64]». Le CFR fait donc reposer la sujétion au droit américain sur un critère de rattachement territorial et personnel. En conséquence, les ECS, les RCS enregistrés, localisés ou détenus aux Etats-Unis ainsi que leurs filiales sont soumis au CLOUD Act.

15. Le DoJ opère néanmoins plus particulièrement une distinction entre deux types d'entreprises[65]: celles qui sont localisées sur le territoire des Etats-Unis et qui de ce fait se voient appliquer les dispositions du CFR en vertu du principe de compétence territoriale du juge pénal ; et celles qui n'entrent pas dans le champ d'application du CFR mais qui visent les Etats-Unis par leurs activités *(directing its conduct into the United States).* Dans ce dernier cas, le juge appréciera, au cas par cas *(fact-specific inquiry),* la nature, la quantité et la qualité des contacts que l'entreprise entretient avec les Etats-Unis. Ainsi, plus l'activité d'une entreprise visera le pays, plus l'entreprise en question sera susceptible d'être qualifiée de sujet de droit américain. Selon une jurisprudence constante, le juge civil apprécie le lien personnel d'un site internet (ECS) avec les Etats-Unis en fonction de ses interactions avec ses clients américains. Pour ce faire, il s'appuie sur un faisceau d'indices tels que le fonctionnement du site, son architecture, l'existence d'une publicité et d'offres promotionnelles ciblées et enfin le trafic[66]. En conséquence, sont susceptibles d'entrer dans le champ d'application personnel du CLOUD Act des entreprises étrangères, localisées et/ou enregistrées en dehors du territoire américain et/ou détenues par des individus qui ne sont ni résidents, ni citoyens des Etats-Unis, dès lors que leurs activités ciblent ce pays. Dans une logique similaire et selon la doctrine *Bank of Nova Scotia,* du nom d'une affaire dans laquelle la filiale américaine d'une banque canadienne localisée aux Iles Caimans avait été enjointe de communiquer des documents[67], les filiales américaines des sociétés étrangères entrent dans le champ d'application du CLOUD Act.

16. La prévalence du lien personnel entre le prestataire et l'État américain comme préalable à l'accès aux données a pour effet de marginaliser le critère de leur localisation[68]. En découle mécaniquement la portée extraterritoriale des requêtes gouvernementales[69]. De ce point de vue, l'approche retenue par le législateur se veut stratégique à deux égards. D'abord, le CLOUD Act fait directement écho à l'argument soulevé par le DoJ dans l'affaire Microsoft. Celui-ci arguait, en effet, que le lieu de stockage des données n'était pas un critère opérant pour mettre en échec l'exécution

64 31 CFR § 515.329 (d)
65 Department of Justice, *Ibidem*, p.8
66 *Supra Ibidem*
67 In Re Grand Jury Proceedings the Bank of Scotia v. United States of America, Plaintiff, Appellee, v. Bank of Nova Scotia, Defendant, appelant, 740 F.2d (11è Cir. 1984)
68 P. Jacob, *La compétence des États à l'égard des données numériques : du nuage au brouillard en attendant l'éclaircie ?*, Revue critique de droit international privé, Décembre 2019, p.665
69 18 U.S.C §2713

du mandat de perquisition. Il soutenait en particulier que la divulgation *(disclosure)* des informations aurait lieu aux Etats-Unis au moment où les enquêteurs en prendraient connaissance et non en Irlande. Selon lui, l'objectif du SCA était la divulgation des données aux autorités et non la protection de la vie privée[70]. Ensuite, le législateur américain entend prendre en compte les techniques de stockage des fournisseurs de services et surmonter la difficulté d'une *« répartition spatiale aléatoire des données[71] »*. Cette dernière dépend en effet de choix algorithmiques faits, en considération de certaines contraintes géographiques[72], environnementales et économiques. Ainsi, il est arrivé que les contenus texte de courriels d'utilisateurs soient stockés sur des serveurs aux Etats-Unis et leurs pièces-jointes le soient sur des serveurs situés en dehors du territoire américain[73]. Même si certains juges ont tenté de tenir compte des techniques mises en place par certains fournisseurs[74], ces derniers ont su faire preuve d'innovation pour s'adapter au risque judiciaire[75]. C'est notamment le cas de Microsoft qui, dès 2015, a conclu, en Allemagne, des ententes commerciales (*local data trusts)* avec des tiers locaux de confiance pour leur confier la gestion de l'accès aux données stockées dans ses data centers germaniques[76]. Le CLOUD Act a pour effet de neutraliser ce type de stratégie.

17. Enfin, en faisant des prestataires de services numériques des courroies légales de transmission des preuves numériques, le CLOUD Act institutionnalise leur rôle d' *« intermédiaires[77] »* . Cela emporte trois conséquences juridiques. La première est la remise en cause de la disposition de la Convention de Budapest relative à l'exigence d'un consentement préalable du fournisseur, quand il est directement saisi d'une requête gouvernementale d'accès transfrontière[78]. La seconde conséquence c'est la légalisation du caractère extraterritorial des demandes d'accès aux données stockées à l'étranger[79]. En découle la création d'un cadre procédural d'exception, remettant en cause la disposition du FRCP[80] en vertu de laquelle le SCA était d'application strictement territoriale. La troisième conséquence est l'invisibilisation de la personne

70 *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, No. 14-2985, 2016 U.S. App LEXIS 12926, at 50 (2d Circuit) (Droney, J., dissenting)
71 R. Bismuth, *Every Cloud has a silver lining – Une analyse contextualisée de l'extraterritorialité du CLOUD Act*, La semaine juridique Entreprise et Affaires n°40, 4 octobre 2018, p.4 (14)
72 https://www.google.com/about/datacenters/inside/locations/
73 Department of Justice, Statement of Brad Wiegmann before the Subcommittee on crime and terrorism, Committee on the Judiciairy, United States Senate, *Law enforcement access to data stored across borders : facilitating cooperation and protecting rights*, May 2017
74 In re Search of Content That is Stored at Premises Controlled by Google, No 16 mc 80263-LB, 2017 WL 1398279, at (*4) (ND, California.April 25, 2017)
75 https://www.zdnet.com/article/microsoft-conflicting-data-laws-could-cost-tech-companies-billions/
76 Th Christakis, Ibidem, p.34
77 A.Z Rozenshstein, *Surveillance intermediaries*, Stanford law Review, vol 70, 2018
78 Article 32 (b), STE185 – Cybercriminalité (Convention), 23. XI. 2001
79 18 U.S.C §2713
80 FRCP, Title VIII, Rule 41, (b) (5) (A)

dont les données sont requises. En effet, si le champ d'application personnel du texte vise explicitement les entreprises de droit américain, il passe sous silence le critère de la nationalité des personnes visées par l'enquête pénale américaine. A ce titre, dans l'affaire Microsoft, la personne inquiétée pour trafic de stupéfiants n'était a priori ni citoyenne, ni résidente des Etats-Unis[81]. Elle ne pouvait donc pas être qualifiée de *« personne américaine[82] »*. Toutefois, cette circonstance n'a jamais été évoquée lors litige. Interrogé sur ce point, le DoJ précise que les autorités américaines peuvent être amenées à requérir des informations concernant une personne qui n'est ni citoyenne, ni résidente américaine[83]. En conséquence, la nationalité étrangère n'est pas un critère absolu de neutralisation de la requête gouvernementale américaine.

2 – Le champ d'application matériel du CLOUD Act

18. Le CLOUD Act introduit un amendement 103 § 2713 au SCA qui oblige les prestataires de services à divulguer, conserver ou préserver les *« contenus d'une communication filaire ou électronique et tout enregistrement ou toute autre information se rapportant à un client ou à un abonné[84] »*. Pour comprendre le champ matériel du CLOUD Act, le DoJ[85] invite à se référer aux catégories de données auxquelles s'applique l'ECPA. Ce texte distingue en effet les informations de contenu *(content information),* des informations non-relatives au contenu *(non-content information).* Si les premières couvrent *« toute information afférente à la substance, à la signification et au sens de la communication [86]»*, les secondes renvoient aux *« informations de connexion, routage, adressage et de signal [87]»*, qui, selon le juge, comprennent *: « les données générées automatiquement sans action volontaire de la part de l'utilisateur ou celles ayant trait à l'enveloppe de la communication[88] »*. Cette catégorisation binaire relativement imprécise englobe celle de la Convention de Budapest plus précise. Au-delà de cette distinction et en tout état de cause, les données visées par le CLOUD Act doivent pouvoir être rattachées à l'utilisateur. Bien que la notion de « donnée personnelle » ne soit pas mentionnée, le texte induit un lien entre l'information recueillie et l'identification d'une personne. De ce point de vue, le champ matériel du

81 E. Mignon, *Ibidem*, p.1
82 18 U.S.C § 2523 (a) (2)
83 Department of Justice, *Ibidem*, p.15
84 18 U.S.C § 2713
85 Department of Justice, *Ibidem*, p.18
86 18 U.S.C § 2510 (8)
87 18 U.S.C §3121
88 *ACLU v. Clapper*, 785 F.3d 787, 822 (2d Cir. 2015)

CLOUD Act coincide avec celui du RGPD[89]. Ce constat renvoie à l'analyse menée en introduction de ce mémoire au sujet de la preuve numérique.

19. Ensuite, le texte américain pose une obligation de préservation, de sauvegarde, et de divulgation *« des données stockées ou des données traitées[90] »* . Concernant la notion de « traitement des données » *(processing data)*, elle est certes utilisée dans le SCA pour décrire l'activité des services informatiques à distance *(computing remote services)*[91], mais elle n'y fait l'objet d'aucune définition. Il est donc utile de se reporter au RGPD qui considère que *« toute opération (…) effectuée ou non à l'aide de procédés automatisés et appliqués à des données ou à des ensembles de données à caractère personnelles[92] »* est un traitement. Y sont incluses la conservation, l'extraction ou toute forme de mise à disposition des données. Selon cette approche extensive, les actions de stockage, de préservation, de sauvegarde peuvent être qualifiées de traitement si bien que le champ matériel du CLOUD Act recouvre de nouveau celui du Règlement européen. Concernant la notion de « stockage électronique » *(electronic storage)* cependant, elle est explicitée dans le SCA comme étant *« (A) tout stockage temporaire, intermédiaire d'une communication filaire[93] ou électronique lié à la transmission électronique de celle-ci ; et (B) tout stockage d'une telle communication par un service de communication électronique[94] à des fins de protection des sauvegarde d'une telle communication. [95]».* Sont ainsi visées les données des mémoires vive, tampon ou cache mais aussi leur sauvegarde. A cet égard, le CLOUD Act ne restreint pas les délais de conservation. En ce sens, il ne modifie pas l'état du droit antérieur si bien que chaque fournisseur est libre de définir sa propre politique en la matière. Sur ce point, le texte américain s'oppose au RGPD qui impose une durée de conservation des données proportionnelle à la finalité de leur traitement[96].

20. Enfin, conformément à la Convention de Budapest[97], le CLOUD Act a pour objectif de *« protéger la sécurité publique et combattre les crimes sérieux y compris le terrorisme [98]»*. Seul l'exposé des motifs fait référence[99] aux types d'infractions pouvant déclencher une demande d'accès. Selon le DoJ, entrent dans la catégorie des crimes sérieux *(serious crime) « le*

89 Art. 4§1, RGPD
90 Department of Justice, *Ibidem*, p.13
91 18 U.S.C §2711 (2)
92 Art. 4 § 2 , RGPD
93 18 U.S.C §2510 (1)
94 18 U.S.C § 2510 (15)
95 18 U.S.C § 2510 (17) (A) (B)
96 Art. 5 §1 (e)
97 DoJ, *Ibidem*, p.2
98 18 U.S.C.A SEC.102 (1)
99 18 U.S.C.A SEC.102 § 3

terrorisme[100]*, les crimes violents, la cybercriminalité et l'exploitation sexuelle des enfants*[101] *»*. La notion est plus précisément définie dans le CFR comme incluant *« toutes les infractions classées dans la catégorie des crimes en vertu des lois des Etats-Unis, des lois d'un Etat fédéré ou des lois de l'État étranger où le crime s'est produit*[102] *»*. La Cour Suprême a ainsi considéré qu'une infraction punie de 6 mois d'emprisonnement pouvait être qualifiée de crime sérieux, permettant ainsi à l'accusé de bénéficier d'un Jury *(Jury trial)*, en vertu du 6ème Amendement de la Constitution[103]. En sus de cette première catégorie d'infractions, le texte vise également les infractions portant atteinte à la sûreté publique *(public safety)*. Cette dernière n'est pas définie en tant que telle en droit américain mais les attributions des agents de sûreté *(public safety officer)* permettent d'appréhender les domaines qu'elle concerne. Semblent ainsi relever du domaine de la sûreté : les catastrophes, urgences et sauvetages majeurs ainsi que les urgences et catastrophes sanitaires avérées ou potentielles[104]. Par conséquent, un très grand nombre d'infractions peuvent permettre aux autorités américaines de déclencher le mécanisme d'accès aux données du CLOUD Act.

B – Formalisme de la requête gouvernementale et nouvelle voie d'opposition

21. Le CLOUD Act ne modifie pas la procédure qui s'impose aux autorités répressives pour formuler une requête (1). Cependant, il crée une nouvelle voie d'opposition au bénéfice des ECS et RCS (2).

1 – Le formalisme de la requête

22. En vertu du SCA, deux procédures existent pour former une demande d'accès aux preuves numériques: celle permettant l'accès aux données de contenu[105] d'une part, et celle encadrant l'accès aux données de connexion et aux métadonnées[106] d'autre part. Là où le champ d'application matériel du SCA englobe les données non-relatives au contenu de manière large, les procédures

100 18 U.S.C § 2331 (1)
101 Department of Justice, *Ibidem*, p.10
102 37 CFR §11.1
103 *Duncan v. Louisiana*, 391 U.S. 145 (1968)
104 34 U.S.C §10284 (9)
105 18 U.S.C §2703 (a) (b)
106 18 U.S.C § 2703 (c)

envisagées par le texte restreignent ce champ aux données des utilisateurs. Le sort réservé aux données de trafic (adresses MAC, IP...) est donc passée sous silence[107].

23. En ce qui concerne les données de contenu, le SCA distingue selon qu'elles sont détenues par un ECS ou un RCS . Pour les ECS, la demande d'accès aux informations varie en fonction de leur délai de conservation. Si elles sont détenues depuis 180 jours ou moins, la requête doit obligatoirement prendre la forme d'un mandat de perquisition délivré conformément aux dispositions du FRCP ou conformément aux procédures de délivrance de l'État fédéré qui l'émet[108]. Si, en revanche, elles sont détenues depuis plus de 180 jours , les autorités disposeront des mêmes options que pour l'accès aux données de contenu détenues par les RCS. Pour ces dernières en effet, aucun délai de conservation n'est pris en compte et les enquêteurs peuvent s'appuyer alternativement sur trois formes d'actes: le mandat de perquisition délivré par le juge conformément aux exigences du FRCP *(warrant)*[109], l'injonction de production administrative ou celle délivrée par un Grand jury *(administrative subpoena duces tecum subpoena)*[110] et enfin l'ordonnance judiciaire *(court order)*[111]. En ce qui concerne l'accès aux données de connexion, le SCA ne fait aucune différence de traitement entre les ECS et les RCS si bien que les autorités répressives disposent de plusieurs possibilités : le mandat[112], l'ordonnance[113], le consentement de la personne concernée par l'enquête[114], une requête écrite pour les cas de fraude par télémarketing[115] ou encore une injonction de production[116].

24. A chacune de ces catégories de requêtes, sont associées des garanties procédurales plus ou moins fortes, en matière de contrôle juridictionnel a priori d'une part et de notification à la personne concernée d'autre part.

25. De la forme de la demande dépend l'intensité de l'intervention a priori du juge américain. L'injonction de production ne fait l'objet d'aucun contrôle juridictionnel préalable. A cet égard, le juge du fond a censuré son utilisation pour un accès aux données de contenu en soutenant que, dans le cas d'espèce, les enquêteurs avaient mené une perquisition au sens du 4ème Amendement de la Constitution qui aurait du être fondée sur un mandat[117]. Si cette décision n'a été ni confirmée, ni

107 Ces données sont explicitement visées dans le Wiretap Act. Néanmoins, leur stockage demeure à ce stade un impensé.
108 18 U.S.C § 2703 (a)
109 18 U.S.C § 2703 (b) (1) (A)
110 18 U.S.C § 2703 (b) (1) (B) (i)
111 18 U.S.C § 2703 (b) (1) (B) (ii)
112 18 U.S.C § 2703 (c) (1) (A)
113 18 U.S.C § 2703 (c) (1) (B)
114 18 U.S.C § 2703 (c) (1) (C)
115 18 U.S.C § 2703 (c) (1) (D)
116 18 U.S.C § 2703 (c) (2)
117 *United States v. Warshak* – 631 F.3d 266 (6th Cir. 2010)

infirmée par la Cour Suprême, cette dernière a jugé en 2018 que la demande d'accès aux métadonnées de géolocalisation d'un téléphone portable devait être fondée sur un mandat alors qu'elle l'était initialement sur une injonction[118]. Bien que ces jurisprudences discréditent le recours à l'injonction pour accéder aux données de contenu et aux métadonnées, les dispositions autorisant son utilisation dans ces deux cas n'ont pas disparu sous l'effet du CLOUD Act. Par opposition, le contrôle juridictionnel effectué en amont de la délivrance d'une ordonnance judiciaire est fondé sur *« une cohérence de faits permettant de laisser raisonnablement croire que l'accès aux données (…) est pertinent et crucial pour l'enquête pénale en cours[119] »*. Enfin, c'est le mandat qui fait l'objet du contrôle juridictionnel a priori le plus strict. Dans ce cas, le juge apprécie en effet la cause probable *(probable cause)* dont les enquêteurs se prévalent dans leur déclaration sous serment *(affidavit)[120]*. *A* l'aune du 4ème Amendement de la Constitution, la cause probable doit être fondée sur *« des circonstances de faits laissant raisonnablement croire que la perquisition aboutira à la découverte d'une infraction[121] »* c'est à dire sur *« une probabilité légèrement inférieure à la réalité de la preuve aboutissant à la condamnation[122] »*. De même, elle doit exister au moment de la délivrance du mandat[123]. La validité de ce dernier[124] est par ailleurs soumise à un formalisme strict précisant, entre autres : *« l'infraction alléguée, l'information dont il est demandé la divulgation et la preuve recherchée[125] »*. Enfin, la présence physique des agents gouvernementaux n'est pas requise pendant l'exécution du mandat[126], qui devra avoir lieu dans un délai de 14 jours à compter de la décision judiciaire[127]. Le standard de la cause probable est donc considéré par le DoJ comme l'un des plus exigeants au monde pour la protection de la vie privée des individus.

26. Ensuite, la forme de la requête fait peser sur les autorités gouvernementales une obligation plus ou moins lourde de notification à la personne concernée. Cette procédure varie en fonction des données visées par la demande. Pour l'accès aux métadonnées, aux données de connexion et à celles de l'utilisateur, le SCA ne prévoit aucune obligation de notification[128]. Pour l'accès aux données de contenu, cette obligation dépend de la forme de la requête. Ainsi, le mandat n'est jamais notifié à la personne visée par l'enquête[129]. En revanche, une injonction de production et

118 *Carpenter v. United States* No 16-402, 585 U.S 2018
119 18 U.S.C § 2703 (b) (1) (B) (i)
120 FRCP, Title II, Rule 4 (a)
121 *Nathanson v. United States*, 290 U.S ; 41, 54S, Ct.11, 78 L.Ed. 159 (1933)
122 *Dumbra V. United States*, 268 U.S. 435 (1925)
123 *United States v. Grubbs*, 126 S. Ct, 1494, 1498-1501, 164 L. Ed. 2D 195 (2006)
124 FRCP, Title VIII, Rule 41 (e) (2) (A) (B)
125 Department of Justice, Ibidem, p.15
126 18 U.S.C § 2703 (g)
127 FRCP, Title VIII, Rule 41 (e) (2) (A) (i)
128 18 U.S.C § 2703 (c) (3)
129 18 U.S.C § 2703 (b) (1) (A)

l'ordonnance doivent l'être[130]. Une exception et deux tempéraments à ce dernier principe ont cependant été introduits par le législateur américain. L'exception concerne l'ordonnance restrictive *(protective order)*[131] qui peut être délivrée par le juge, s'il existe un risque de destruction des preuves recherchées[132] ou de mise en danger d'autrui[133], à la suite de la notification de l'ordonnance judiciaire simple *(court order).* Ainsi, les autorités gouvernementales peuvent contourner l'obligation de notification de l'ordonnance en sa forme simple grâce à l'ordonnance restrictive qui, elle, ne sera pas notifiée. Ensuite et c'est le premier tempérament à cette obligation, les autorités gouvernementales disposent d'un délai de 90 jours[134] pour notifier la demande d'accès s'il existe un risque de mise en danger d'autrui, de fuite du suspect, de destruction ou d'altération des preuves, de subordination de témoins ou de mise en péril de l'enquête et du jugement[135]. Passé ce délai, elles pourront, soit notifier en respectant un formalisme spécifique[136], soit demander une ordonnance restrictive[137] au juge. Le second tempérament concerne enfin les copies de sauvegarde. Quand ces dernières sont requises par le juge, elles doivent être produites dans un délai de 2 jours ouvrables par le fournisseur de service sans notification préalable à son client[138]. Elles sont ensuite communiquées dans un délai n'excédant pas 14 jours aux autorités gouvernementales[139] qui, à leur tour, ont 3 jours, à compter de la confirmation de la prise en compte de leur demande par le fournisseur de services électroniques[140], pour informer la personne concernée.

27. Cette analyse du cadre formel de la demande met en relief toutes les possibilités qui s'offrent aux autorités américaines pour accéder à des données personnelles dans le cadre d'une enquête pénale. Les individus dont les données sont recherchées disposent d'un droit à l'information résiduel, l'obligation de notification étant restreinte. En conséquence, la divergence de fond avec la directive 2016/680 qui constitue le cadre européen de protection des données dans le cadre de la détection des infractions, est d'abord de principe. Là où le CLOUD Act semble faire de l'information à la personne l'exception et du secret de l'enquête le principe, la directive 2016/680 fait de l'information à la personne concernée le principe[141], lui ouvrant ainsi un droit inconditionnel

130 18 U.S.C § 2703 (b) (1) (B)
131 18 FRCP, Title IV, Rule 16, (d) (1)
132 18 U.S.C § 2705 (b) (3)
133 18 U.S.C § 2705 (b) (1)
134 18 U.S.C § 2705 (a) (1) (A) (B)
135 18 U.S.C § 2705 (a) (2)
136 18 U.S.C § 2705 (a) (5) (A) (B)
137 18 U.S.C § 2705 (b)
138 18 U.S.C § 2704 (a) (1)
139 18 U.S.C § 2704 (a) (4)
140 18 U.S.C § 2704 (a) (2)
141 Art 13 § 1

d'accès à ses données[142] et de contestation du traitement[143]. Cependant, la directive laisse une marge d'appréciation aux Etats membres pour prévoir des limitations au contenu de l'information délivrée à la personne[144]. Ces limitations peuvent être justifiées par des impératifs de sécurité[145], d'ordre public[146] ou encore de défense nationale[147].

28. Enfin, l'absence de droit à l'information sous l'empire du CLOUD Act pose une difficulté accrue pour les personnes considérées comme étrangères par le droit américain. En effet, depuis les années 90 et de manière constante, la Cour Suprême ne reconnaît le bénéfice des protections du 4ème Amendement qu'aux citoyens et résidents des Etats-Unis et non *« aux individus qui n'ont aucun lien[148] »* avec ce pays. En conséquence, le CLOUD Act crée une asymétrie des droits exposant les étrangers à une extrême vulnérabilité. Si leurs données peuvent faire l'objet d'une demande d'accès, au même titre que celles des citoyens et résidents permanents américains, les standards juridiques et procéduraux qui leur seront appliqués restent d'intensité incertaine[149].

2 – Nouvelle voie d'opposition, la Comity Analysis et voies de droit commun

29. Le CLOUD Act introduit une voie d'opposition dédiée aux ECS et aux RCS, appelée « Analyse de Comité » (*Comity Analysis)*[150]. Le principe reste néanmoins l'obligation de se soumettre à la requête gouvernementale[151]. De ce fait, dans le cas où les fournisseurs de services n'obtempéreraient pas, ils s'exposeraient à une sanction pour outrage au tribunal *(contempt of court),* crime passible d'une amende de 1000$ et d'une peine de prison de 6 mois[152]. La qualification de l'infraction d'outrage étant un privilège du juge, ce dernier peut prononcer une condamnation immédiate et sans jury, dès lors qu'il existe plus qu'un doute raisonnable *(beyond a reasonable doubt).* En conséquence, ignorer la demande d'accès aux données fait courir un risque non-négligeable aux ECS et RCS. A titre indicatif, la seule voie de recours préalable ouverte par le SCA aux personnes concerne la copie de sauvegarde de leurs données[153].

142 Art. 13 § 1 (e)
143 Art. 13 § 1 (d)
144 Art. 13 § 3
145 Art. 13 § 3 (a) (b)
146 Art. 13 § 3 (c)
147 Art. 13 § 3 (d)
148 *United States v. Verdugo-Urquidez*, 494, U.S. 259 (1990)
149 C. Boineau, *Extraterritorialité des lois américaines : conséquences pratiques et juridiques pour les cadres dirigeants et mandataires sociaux*, RLDA, n°157, 1er mars 2020, p.3
150 18 U.S.C § 2703 (h)
151 18 U.S.C § 2703
152 18 U.S.C § 401 (3)
153 18 U.S.C § 2704 (b) (1)

30. Pour juguler le risque de conflit de lois en même temps que celui de voir les entreprises du numérique se soustraire à leur obligation de divulgation, le CLOUD Act leur donne la possibilité de demander au juge l'annulation ou la modification *(motion to quash or modify)* de la requête gouvernementale dont ils ont été saisis, à deux conditions[154]. Premièrement, la personne dont les données sont requises ne doit pas être une « *US person*[155] », c'est à dire : « *un citoyen ou une personne disposant de la nationalité des Etats-Unis ; un étranger admis légalement sur le territoire américain à la résidence permanente ; une association*[156] *enregistrée aux Etats-Unis dont un nombre substantiel de membres sont des citoyens américains ou des étrangers admis légalement sur le territoire américain à la résidence permanente ; ou une société enregistrée aux Etats-Unis*[157] ». En somme, cette personne ne doit être ni une personne physique citoyenne, résidente ou disposant de la nationalité des Etats-Unis, ni une personne morale entretenant des liens étroits avec des citoyens ou résidents américains ou admise à exercer une activité économique aux Etats-Unis. Deuxièmement, il doit exister un risque de conflit avec la loi d'un Etat auquel les Etats-Unis sont liés par un accord exécutif *(executive agreement)*[158], c'est à dire avec la loi d'un Etat étranger considéré comme « qualifié » *(qualifying foreign government)*[159]. En vertu des dispositions du CLOUD Act, les Etats-Unis acceptent d'entrer dans un tel accord[160] s'il existe, entre autres, une réciprocité procédurale et substantielle des voies de recours offertes aux ECS et aux RCS américains[161]. Si ces deux conditions sont cumulativement remplies, la requête en annulation ou en modification devra être introduite dans un délai de 14 jours à compter de la notification de la demande d'accès gouvernementale à l'ECS ou au RCS sauf dérogation prévue dans l'accord exécutif avec l'État étranger qualifié[162]. Le juge mettra alors en balance les circonstances suivantes[163] : l'atteinte à la loi de l'État étranger qualifié[164] ; l'intérêt de la justice américaine[165] ; la qualification de « personne américaine »[166]. Les intérêts de la justice américaine sont plus particulièrement évalués à l'aune d'une analyse de Comité[167] fondée sur une série de huit critères parmi lesquels: l'intérêt de la divulgation des données pour l'enquête pénale en cours[168] ; les intérêts

154 18 U.S.C § 2703 (h) (2) (A)
155 18 U.S.C § 2703 (h) (2) (A) (i)
156 La notion d'*association* en droit américain est plus large que la catégorie des associations 1901 en France
157 18 U.S.C § 2523 (a) (2)
158 18 U.S.C § 2523 (b)
159 18 U.S.C § 2703 (h) (1) (A) (i) (ii)
160 Les détails du cadre de la conclusion des accords exécutifs est développé plus loin
161 18 U.S.C § 2703 (h) (1) (A) (ii)
162 18 U.S.C § 2703 (h) (2) (A) (ii)
163 18 U.S.C § 2703 (h) (2) (B)
164 18 U.S.C § 2703 (h) (2) (B) (i)
165 18 U.S.C § 2703 (h) (2) (B) (ii)
166 18 U.S.C § 2703 (h) (2) (B) (iii)
167 18 U.S.C § 2703 (h) (3)
168 18 U.S.C § 2703 (h) (3) (A) (E)

de l'État étranger qualifié[169], la probabilité et l'ampleur des sanctions encourues par l'entreprise américaine en cas de violation de la loi de l'État étranger[170], le lieu de résidence et la nationalité de la personne concernée, appréciés à la lumière des liens qu'elle entretient avec les Etats-Unis[171], la nature et l'étendue des liens du fournisseur de services électroniques avec les Etats-Unis[172] ou encore l'existence d'un accès rapide et efficace aux données ayant des conséquences moins graves que celles d'un conflit de lois[173]. En conséquence, cette voie d'opposition n'est ouverte que si la demande d'accès concerne le ressortissant étranger d'un Etat lié aux Etats-Unis par un accord exécutif bilatéral. Dans le cas, cependant, où la demande gouvernementale américaine concerne le ressortissant d'un Etat n'ayant pas conclu un tel accord, le fournisseur de services pourra contester la demande devant le juge américain qui examinera sa requête en vertu du principe de courtoisie internationale[174]. Ce dernier repose sur des standards de common law[175] selon lesquels l'exécution du droit des Etats-Unis doit être nuancée pour tenir compte des intérêts des Etats étrangers. Néanmoins, à la différence des critères de l'analyse de Comité qui sont explicitement énoncés dans le CLOUD Act, ceux du principe de courtoisie internationale sont jurisprudentiels. Ils sont donc plus délicats à appréhender[176]. En outre, les ECS et les RCS ne pourront s'en prévaloir que par la voie de l'exception dans le cadre d'une procédure pour outrage au tribunal[177]. Enfin, dans le cas où la demande d'accès concerne un ressortissant américain, les fournisseurs d'accès disposeront de la voie de recours de droit commun leur permettant d'introduire une requête en annulation *(motion to quash)* de la demande devant le juge compétent.

31. En tout état de cause, les modalités selon lesquelles les entreprises activeront effectivement cette voie d'opposition restent inconnues. Par ailleurs, l'analyse de Comité reposera sur l'appréciation par le juge américain des risques auxquels l'entreprise est exposée en vertu du droit étranger[178]. A ce titre, il n'est pas exclu que cela donne lieu à des erreurs d'interprétation[179] ou encore à une survalorisation des intérêts des Etats-Unis au détriment des exigences légales de l'État

169 18 U.S.C § 2703 (h) (3) (B)
170 18 U.S.C § 2703 (h) (3) (C)
171 18 U.S.C § 2703 (h) (3) (D)
172 18 U.S.C § 2703 (h) (3) (E)
173 18 U.S.C § 2703 (h) (3) (G)
174 W.S Dodge, *International Comity in American Law,* Columbia Law Review, Vol.115, n°8
175 18 U.S.C § 2703 (c)
176 Congressional Research Service, *Cross-border data sharing under the Cloud Ac*t, Legislative Attorney, April 23, 2018, p.9
177 E. Mignon, *Faut-il avoir peur du CLOUD Act ?* Auguste Debouzy, 25/06/2018
178 18 U.S.C (h) (3) (C)
179 P. Jacob, *Ibidem*

tiers. Certains auteurs craignent donc que cette nouvelle voie d'opposition ne se transforme en *« doctrine de diplomatie judiciaire fondée sur la souveraineté »*[180].

32. Enfin, pour inciter les fournisseurs de services à coopérer avec les autorités, le CLOUD Act leur octroie une exception de bonne foi *(good faith exception)*[181] à la règle de l'exclusion *(exclusionary rule)*[182] des preuves obtenues en violation du 4ème Amendement de la Constitution. En vertu de cette exception, le fournisseur de services qui aura divulgué les informations conformément à l'injonction de production, à l'ordonnance judiciaire ou au mandat de perquisition, ne pourra voir sa responsabilité recherchée si cette demande s'avère invalide[183] et/ou si elle s'avère porter une atteinte arbitraire à l'attente raisonnable de vie privée *(reasonable expectation of privacy)*[184]. Le fournisseur de services bénéficiera en effet d'une présomption irréfragable de bonne foi qui le préservera de toute poursuite sur ce fondement.

33. L'examen approfondi du régime mis en place par le CLOUD Act met en lumière l'aspiration des Etats-Unis à étendre leur compétence pour accéder aux données personnelles indispensables à la conduite de leurs enquêtes pénales. L'objectif du législateur américain est de s'adapter aux processus algorithmiques qui fragmentent et dispersent les preuves numériques sur des serveurs situés dans différents Etats. Il est aussi de s'extraire de la lenteur des Traités d'entraide judiciaire, jugée incompatible avec la volatilité des données. Conscient que cette aspiration interfère avec la mise en œuvre du RGPD, le législateur américain propose deux mécanismes pour anticiper et résoudre un éventuel risque de conflit de lois. La première partie de ce mémoire a permis d'aborder le mécanisme interne de prévention de ce conflit opérée par la doctrine de Comity Analysis. Il reste cependant à envisager le mécanisme bilatéral de résolution ainsi que la réponse qu'y apporte l'Europe à ce stade.

180 L.M Augagneur, *Héberger ses données chez les GAFAM : quel discours croire sur le CLOUD Act*, RLDI, n°162, Août-septembre 2019, p. 54
181 18 U.S.C § 2703 (e)
182 *Mapp v. Ohio*, 367 U.S. 643 (1961)
183 *Arizona v. Evans*, 514, U.S. 1 (1995)
184 *Katz v. United States*, 389 U.S 347 (1967)

II – CONFLIT DE LOIS ENTRE LE CLOUD ACT ET LE RGPD: ENTRE VOLONTÉ ASYMÉTRIQUE DE RÉSOLUTION DES ÉTATS-UNIS ET RÉACTION DE L'EUROPE

34. Le RGPD pose un principe d'interdiction des transferts de données personnelles à des fins d'enquête pénale en dehors de tout Traité d'entraide judiciaire. Ce principe est néanmoins assorti d'exceptions qui ont nourri des difficultés d'interprétation (A). Anticipant cet obstacle, le CLOUD Act met en place un mécanisme bilatéral d'échange de données auquel l'Europe a réagi (B).

A – Le conflit sur les transferts internationaux de données

35. Par principe, le RGPD restreint les transferts de preuves numériques vers les Etats tiers au cadre de la coopération judiciaire(1). Ce principe est cependant assorti d'exceptions dont l'interprétation a dû être précisée (2).

1 – Le principe du recours aux Traités d'entraide judiciaire posé par le RGPD

36. En premier lieu, le transfert de données personnelles stockées sur le territoire de l'UE, vers les Etats-Unis, entre dans le champ d'application matérielle et territoriale du RGPD. En effet, tout traitement automatisé ou non-automatisé de données personnelles *« contenues ou appelées à figurer dans un fichier*[185] *»* est soumis à ses dispositions. Bien que les notions de « stockage » et de « transfert » n'y soient pas expressément définies, *« la collecte, l'enregistrement, la conservation*[186] *(…), la communication par transmission»* qu'ils impliquent, sont qualifiés de traitement de données. En outre, l'autorité de contrôle française (CNIL[187]) a précisé que le transfert recouvre *« toute communication, copie ou déplacement de données par l'intermédiaire d'un réseau (…) ou d'un support à un autre quel que soit le type de support (...)* [188]». Il en va ainsi du simple accès y compris sans conservation ou extraction, de même que du simple hébergement. Par ailleurs, le RGPD concerne les *« traitements de données à caractère personnel effectués dans le cadre des activités d'un établissement d'un responsable de traitement ou d'un sous-traitant sur le territoire de*

185 Art. 2§1, RGPD
186 Art. 4§2, RGPD
187 Commission Nationale de l'Informatique et des Libertés
188 CNIL, *Les transferts de données à caractère personnel hors de l'Union européenne*, nov. 2012, p.5

l'Union, que le traitement ait lieu ou non dans l'Union[189] *»*. Il protège également les personnes *« qui se trouvent sur le territoire de l'Union*[190] *»* et auxquelles sont offerts des biens, des services[191] ou faisant l'objet d'un suivi comportemental[192]. Sur ce point, peu importe le lieu d'établissement du fournisseur. Deux critères alternatifs permettent donc de déclencher l'application territoriale du RGPD : l'établissement du prestataire sur le territoire de l'UE d'une part et la résidence sur ce même territoire de la personne visée par les biens ou les services fournis. A ce titre, la nationalité de la personne est indifférente[193]. Aussi, les ECS et les RCS qui ont des data centers *« participant directement à des activités impliquant le traitement de données personnelles*[194] *»* dans l'UE, sont pleinement soumis aux dispositions du RGPD. De même, les données des citoyens et résidents américains stockées sur le territoire de l'UE sont protégées par le RGPD. En outre, les ECS et les RCS qui n'ont aucun ancrage territorial sur le territoire européen mais qui traitent les données des personnes y résidant à des fins commerciales doivent aussi se conformer au texte européen dont on mesure ici la portée extraterritoriale.

37. En second lieu, l' exécution d'une demande juridictionnelle ou administrative américaine délivrée en vertu du CLOUD Act, revient à déclencher un transfert de données vers les Etats-Unis, c'est à dire un pays tiers n'appartenant pas à l'Espace économique européen (EEE)[195]. Considérant que *« cela peut accroître le risque que les personnes physiques ne puissent exercer leurs droits liés à la protection des données, notamment pour se protéger de l'utilisation ou de la divulgation illicite de ces informations*[196] *»*, le législateur européen restreint ce genre d'opération par une extension de la protection accordée aux données de la personne en dehors de l'UE[197]. En tout état de cause, le RGPD dispose 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 fondées sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un Etat membre, sans préjudice d'autres motifs de transfert (...)*[198] *»*. Par principe donc, un transfert international de données servant les intérêts d'une autorité administrative ou judiciaire dans le cadre d'une enquête pénale a vocation à être opéré sur le fondement d'un Traité d'entraide judiciaire et d'une convention internationale

189 Art. 3§1, RGPD
190 Art. 3§2, RGPD
191 Art. 3§2 (a), RGPD
192 Art. 3§2 (b), RGPD
193 Considérant 14, RGPD
194 G29, avis n°8/2010 du 16 décembre 2010, WP 179
195 Cet espace inclut les 27 Etats membres de l'UE ainsi que la Norvège, l'Islande et le Lichtenstein
196 Considérant 116, RGPD
197 Art. 44, RGPD
198 Art. 48, RGPD

prévue à cet effet[199]. C'est notamment au soutien de cet argument que Microsoft s'était opposé à la demande du DoJ [200]. Selon une approche similaire, l'Amicus Curiae de la Commission européenne devant la Cour Suprême soulignait que *« les accords internationaux incarnent un équilibre négocié entre les intérêts des Etats, destiné à juguler les risques de conflits[201] »*. L'article 48 du RGPD entre donc en conflit frontal avec la disposition du CLOUD Act qui offre aux autorités gouvernementales un accès direct aux données détenues par les entreprises américaines. A l'aune du RGPD en effet, les données stockées dans un data center de l'UE par ces entreprises, sont protégées et ne pourront être divulguées qu'en vertu des mécanismes européens d'entraide.

38. En Europe, l'entraide judiciaire en Europe est élaborée à un double niveau. Au niveau du Conseil de l'Europe d'abord, la Convention européenne d'entraide judiciaire en matière pénale de 1959 dont les Etats membres de l'EEE et les Etats-Unis sont parties, crée un mécanisme de commissions rogatoires[202]. Dans ce cadre, une autorité requérante donne mandat à une autorité requise pour qu'elle procède à un ou plusieurs actes d'enquête[203]. La Convention de Budapest de 2001 sur la cybercriminalité est le second instrument de coopération judiciaire et contient à la fois des dispositions de droit matériel[204], procédural[205] et de coopération internationale[206]. Au niveau de l'UE, ensuite, un accord d'entraide judiciaire avec les Etats-Unis a été conclu le 19 juillet 2003 et est entré en vigueur le 1er février 2010. Il s'impose à l'ensemble des accords bilatéraux des Etats membres. Plusieurs de ses dispositions prévoient une protection spécifique des données échangées dans le cadre de l'accès à la preuve numérique[207] . Ainsi, l'État requis peut imposer des limitations à l'utilisation des données et des informations demandées[208]. Il peut également demander au pays requérant de fournir des informations sur leur utilisation [209]. Le 10 décembre 2016, cet accord a été complété par un accord-cadre appelé *Umbrella Agreement[210]* dont le but est de protéger les informations à caractère personnel lors de leur transfert *« entre les Etats-Unis et l'UE à l'occasion d'une décision d'assistance mutuelle prise en vertu d'un Traité d'entraide judiciaire[211] »*. L'accord

199 Considérant 115, RGPD
200 Le RGPD n'est pas encore appliqué quand la Cour Suprême accepte d'examiner l'affaire Microsoft
201 Brief of the European Commission in United States of America v. Microsoft Corporation, Supreme Court of the United States, n°17-2, p. 15-16
202 Art. 3, Convention européenne de 1959
203 Rapport explicatif de la Convention de 1959, p.5
204 Art. 2 à 10, Convention STE 185 sur la cybercriminalité, 2001
205 Art. 14 à 21, Supra ibidem
206 Art. 23 à 35, Supra ibidem
207 Art. 9, Accord entre l'Union européenne et les Etats-Unis d'Amérique en matière d'entraide judiciaire
208 Art. 9§2 (a), Supra ibidem
209 Art. 9§3, Supra ibidem
210 Accord entre les Etats-Unis d'Amérique et l'Union européenne 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, 10 décembre 2016
211 Art. 1§2, *Ibidem*

« Parapluie » ne constitue cependant en aucun cas la *« base juridique d'éventuels transferts d'informations à caractère personnel[212] »*. Prohibant expressément toute divulgation de données à caractère personnel fondée sur la décision juridictionnelle ou administrative d'un pays tiers en dehors de ces mécanismes d'entraide, le RGPD indique cependant que *« les transfert ne devraient être autorisés que lorsque les conditions fixées par le présent règlement pour les transferts vers les pays tiers sont remplies[213] »*. Le principe d'interdiction de l'article 48 étant *« sans préjudice des autres motifs de transfert »*, il doit être lu à l'aune des conditions *« en cascade[214] »* visées aux articles 45 et 46 du RGPD.

39. Le transfert de données vers un Etat tiers est possible si la Commission européenne rend une décision[215] attestant que l'État en question assure *« un niveau de protection adéquat[216] »* de la vie privée, des libertés et des droits fondamentaux des personnes concernées. Ce niveau de protection s'apprécie notamment en fonction des dispositions en vigueur au sein du pays tiers[217] et des mesures de sécurité appliquées aux traitements. Dans la lignée des orientations du G29[218], est également prise en compte *« l'existence et le fonctionnement effectif d'une ou plusieurs autorités de contrôle indépendantes[219] »*. Enfin, entrent en considération l'adhésion à des engagements internationaux tels que la Convention 108[220] et la mise en place de mécanismes de coopération[221] avec les autorités de contrôle des Etats membres. Sous le régime de la directive 95/46/CE du 24 octobre 1995, la Commission a rendu une décision d'adéquation pour quinze Etats dont les Etats-Unis ne font pas partie. Cela s'explique par un lourd précédent jurisprudentiel. En 2013, en effet, la mise en lumière par le lanceur d'alerte E. Snowden des programmes de surveillance de la National Security Agency (NSA)[222] a entraîné l'action en justice d'un jeune étudiant autrichien, Max Schrems, devant la High Court irlandaise. Alléguant que *« le droit et les pratiques des Etats-Unis n'offrent aucune protection réelle contre la surveillance d'Etat[223] »*, celui-ci exigeait la suspension des transferts vers les Etats-Unis sur le fondement de l'accord du *Safe Harbor* ou « Sphère de sécurité ». Ledit accord résultait d'une décision de la Commission européenne[224] et reposait sur

212 Art. 1§3, Ibidem
213 Considérant 115, RGPD
214 R. Perray, *Quelle stratégie pour les transferts de données personnelles hors de l'Union européenne à l'aune du RGPD*, CCE, n°4, avril 2018
215 Art. 45§1, Ibidem
216 Art. 45§2 Ibidem
217 Art 45§2 (a), RGPD
218 G29, 26 juin 1997, WP4 ; G29, 24 juillet 1998, WP12 ; G29, 3 juin 2003, WP74
219 Art. 45§2 (b), RGPD
220 Considérant 105, Règlement UE 2016/679
221 Considérant 104, Règlement UE 2016/679
222 https://www.nextinpact.com/news/86591-la-nsa-confirme-que-geants-web-savaient-pour-programme-prism.htm
223 Ibidem, considérants 72 et 73
224 Décision 2000/520/CE du 26 juillet 2000

l'auto-certification d' entreprises américaines contrôlées dans le cadre du Federal Trade Commission Act (FTCA). Avant de se prononcer, la juridiction suprême irlandaise saisit la CJUE d'une question préjudicielle pour savoir si le Safe Harbor respectait les exigences de la Directive de 1995 et les articles 7 et 8 de la Charte des droits fondamentaux de l'UE. A cet égard, la Commission européenne avait eu l'occasion, dès 2013, de constater que *« toutes les entreprises participant au programme PRISM (programme de collecte de renseignements à grande échelle) qui permettent aux autorités américaines d'avoir accès à des données stockées et traitées aux Etats-Unis, semblent être certifiées dans le cadre de la « Sphère de sécurité », qui est devenue l'une des voies par lesquelles les autorités américaines du renseignement ont accès à la collecte des données à caractère personnel initialement traitées dans l'Union*[225] *».* Elle concluait alors que *« l'accès à grande échelle des agences de renseignement aux données, que des entreprises certifiées au titre de la « Sphère de sécurité » transfèrent aux Etats-Unis, soulève de graves questions sur la continuité de la sauvegarde des droits des citoyens européens (…) lorsque les données les concernant sont transférées aux Etats-Unis*[226] *».* Dans sa décision du 6 octobre 2015, la CJUE constate à son tour que le Safe Harbor consacre la primauté du principe de sécurité nationale des Etats-Unis sur celui de protection des données et que de ce fait, les entreprises américaines écartent cette dernière chaque fois qu'elle entre en conflit avec les objectifs de sécurité nationale[227]. Considérant qu'un tel accord ouvre la voie à une surveillance massive et indiscriminée[228] de la part du renseignement américain, la CJUE l'invalide[229]. Cependant, un nouvel accord, sectoriel et partiel, le Privacy Shield, voit le jour le 1er août 2016[230]. Il autorise uniquement les transferts de données personnelles vers les entreprises américaines certifiées respectant ses exigences[231]. En conséquence, il n'existe à ce stade, aucune décision d'adéquation permettant aux ECS et les RCS de faire droit aux requêtes gouvernementales américaines émises en application du CLOUD Act. L'analyse de la jurisprudence *Schrems* et de ses effets juridiques permet toutefois de dresser deux constats. D'abord, l'Union européenne considère comme insuffisante la protection des données personnelles garantie par le droit américain. On peut ici y voir la conséquence du refus des Etats-Unis d'adhérer à la Convention 108[232] ainsi que celle de l'absence d'une législation dédiée[233]. Ensuite, le risque que

225 Communication relative au fonctionnement de la « Sphère de sécurité » du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, COM(2013) 847 final
226 Supra Ibidem
227 CJUE, 6 oct 2015, aff. C-362/14, considérant n°86
228 CJUE, 6 oct 2015, aff. C-362/14, considérant n°94
229 CJUE, 6 oct 2015, aff. C-362/14, considérant n°106
230 Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis du 1er août 2016
231 Y. Padova, *Le Safe Harbor est mort, vive le Privcay Shield ?*, RLDI, n°127, 1er juin 2016
232 Art. 45§2 (c), RGPD
233 Art. 45§2 (b), RGPD

constituent les transferts de données personnelles vers les Etats-Unis pour les droits fondamentaux provient de la collaboration entre les « Géants du Web » et le Gouvernement américain[234]. Or, le champ d'application personnel du CLOUD Act recouvre précisément cette zone de risque.

40. En l'absence de décision d'adéquation peuvent être adoptées des garanties appropriées *« à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives*[235] *»*. Ces conditions sont de deux ordres : celles ne nécessitant pas une autorisation particulière de la part de l'autorité de contrôle[236] et celles en nécessitant une[237]. Les premières renvoient à un instrument juridique contraignant et exécutoire entre autorités ou organismes publics[238], à des règles d'entreprises contraignantes[239], aux clauses types adoptées par la Commission[240] ou par une autorité de contrôle nationale approuvée par la Commission, aux codes de conduite[241] ou aux mécanismes de certification approuvés[242]. Les secondes renvoient aux clauses contractuelles ad hoc qui doivent être revues par une autorité de contrôle[243] ainsi qu'aux dispositions intégrées dans les arrangements administratifs des autorités publiques ou des organismes publics qui prévoient des droits opposables pour les personnes concernées[244]. En tout état de cause, les demandes d'accès aux données personnelles formulées en vertu du CLOUD Act ne font l'objet d'aucune garantie appropriée au sens de l'article 46 et suivants du RGPD.

41. Si le transfert de données vers un Etat tiers ne peut être effectué ni sur le fondement d'une décision d'adéquation ni sur celui de garanties appropriées, l'ultime hypothèse envisageable demeure celle de l'article 49§2 (d) quand le transfert est *« nécessaire pour des motifs importants d'intérêt public »*.

2 – Les difficultés d'interprétation de l'exception de transfert pour motif d'intérêt public

42. Quand l'affaire Microsoft est portée devant la Cour Suprême américaine, le RGPD n'est pas encore appliqué dans les Etats membres de l'UE. De même, le CLOUD Act n'a pas encore été adopté. Cependant, les mémoires des deux parties et des *Amici curiae* fournissent des indications

234 CJUE, 6 oct 2015, aff. C-362/14, considérant n°96
235 Art. 46§1, RGPD
236 Art. 46§2, RGPD
237 Art. 46§3, RGPD
238 Art. 46§2 (a), RGPD
239 Art. 46 §2 (b), RGPD
240 Art. 26§2, Directive 95/46/CE du 24 octobre 1995
241 Art. 40, RGPD
242 Art 42, RGPD
243 Art. 46§3 (a) RGPD
244 Art. 46§3 (b), RGPD

quant à la possibilité pour les ECS et les RCS de communiquer les données au DoJ sur le fondement de l'exception d'intérêt public visée à l'article 49§2 (d) du RGPD.

43. Tout d'abord, les arguments des parties sont marqués par une évaluation opposée du risque de conflit de lois. Pour le DoJ, ce risque est hypothétique dans la mesure où Microsoft et d'autres se sont jusque là conformé à ses demandes d'accès à portée extraterritoriale. Dans son premier mémoire, il indique ainsi que l'application de l'article 48 du RGPD est *« sans préjudice »* des exceptions visées aux articles 49§1 (d) et (e) selon lesquelles il est possible de transférer des données personnelles depuis l'UE *« pour des raisons importantes d'intérêt public »* et *« nécessaires à la constatation, à l'exercice ou à la défense de droits en justice »*[245]. Dans son contre-mémoire[246] de réponse à la Commission européen, le DoJ retient une interprétation extensive de l'article 49§1 du RGPD, qui, selon lui, permet de tenir compte des impératifs de l'enquête pénale américaine, en l'occurrence, un motif d'intérêt public. De son côté, Microsoft conteste cette thèse et retient dans son mémoire, une approche restrictive de ce même article en indiquant qu'il n'existe aucune portée générale permettant les transferts exigés par le DoJ, et qu'en tout état de cause, les dérogations de l'article 49 requièrent une évaluation de la demande au regard du droit de l'UE et non au regard de celui des Etats-Unis[247].

44. Le mémoire d'Amicus Curiae de la Commission européenne livre une première interprétation de l'article 49§1 (d) émanant d'une institution de l'UE. Selon elle, les « motifs importants d'intérêt public » doivent être reconnus par le droit de l'UE ou par le droit d'un Etat membre de l'UE soumis aux dispositions du RGPD. Par conséquent, le recours à cette base légale doit rester limitée à des situations particulières faisant l'objet de définitions spécifiques telles que *« les domaines de criminalité particulièrement graves »* de l'article 83§1 du Traité sur le Fonctionnement de l'UE (TFUE)[248], à savoir : *« le terrorisme, la traite d'êtres humains et l'exploitation sexuelle des femmes et des enfants, le trafic illicite de drogues, le trafic illicite d'armes, le blanchiment d'argent, la corruption, la contrefaçon de moyens de paiement, la criminalité informatique et la criminalité organisée »*. Cette interprétation laisse donc ouverte la possibilité pour un ECS ou un RCS de faire droit à la requête des autorités américaines, dans le cadre de la lutte contre la criminalité.

45. En novembre 2017 et alors que l'affaire *United States v. Microsoft Corp* est pendante devant la Cour Suprême, le Comité européen de la Protection des Données (CEPD)[249] qui vient de

245 Brief for the United States, United States of America v. Microsoft Corporation. No. 17-2. December 6, 2017
246 Reply Brief for the United States, No17-2, February 12, 2018
247 Brief for Respondent, United States of America v. Microsoft Corporation, No. 17-2., January 11, 2018
248 Traité sur le fonctionnement de l'Union européenne (version consolidée)
249 Art. 68, RGPD

remplacer le G29, rend l'avis suivant : *« Le droit de l'Union européenne en matière de protection des données prévoit que les accords internationaux existants tels que les traités d'entraide judiciaire doivent (…) être respectés lorsque des autorités administratives ou judiciaires de pays tiers demandent à accéder à des données personnelles ou à se les faire communiquer auprès de responsables de traitement de l'Union européenne. Le fait de contrevenir aux Traités d'entraide judiciaire existants, ou tout autre fondement juridique applicable au regard du droit de l'Union européenne, par les autorités d'un pays tiers constitue une intrusion dans la souveraineté territoriale des Etats membres de l'Union européenne*[250] *».* Après l'adoption du CLOUD Act, le CEPD publie les directives d'interprétation relatives aux dérogations de l'article 49 du RGPD[251] et précise que *« dans les situations où il existe un accord international, tel un accord d'entraide judiciaire, les entreprises de l'Union européenne devraient généralement refuser de faire droit à des demandes directes et renvoyer l'autorité du pays tiers vers l'accord de coopération applicable*[252] *».* Concernant l'interprétation de l'article 49§1 (d), le CEPD indique que cette dérogation pour motif d'intérêt public ne s'applique que *« lorsqu'il peut être démontré précisément au regard du droit de l'Union ou de celui de l'État membre auquel le responsable du traitement des données est soumis que de tels transferts servent des raisons importantes d'intérêt public – y compris dans un esprit de réciprocité. L'existence d'un accord international qui consacre un certain objectif et prévoit une assistance mutuelle afin d'y parvenir, peut être un critère d'appréciation de l'existence d'un intérêt public au regard de l'article 49§1 (d) dès lors que l'Union ou l'État membre concerné est partie à cet accord*[253] *».* Cette interprétation emporte donc deux conséquences. D'une part, le motif d'intérêt public ne pourra être invoqué par les Etats-Unis que si le transfert des données correspond aux intérêts de l'Union européenne. A ce titre, l'existence d'un Traité international auquel les Etats membres de l'UE et les Etats-Unis sont parties constitue un facteur clé pour l'appréciation d'un tel motif. D'autre part, cette interprétation de l'exception est plus restrictive que celle de la Commission qui ne s'opposait pas aux transferts justifiés par la détection de crimes transfrontières en vertu du TFUE. Cependant, le CEPD a pour mission d'assurer la cohérence de l'interprétation du RGPD et de promouvoir une compréhension commune de son contenu[254]. En ce sens, son interprétation fait autorité.

46. Le 10 juillet 2019, le CEPD et le Contrôleur européen de la protection des données (EDPS), ont rendu une évaluation de l'impact du CLOUD Act sur le cadre juridique européen de la

250 CEPD, Avis du 29 novembre 2017, D*ata protection and privacy aspects of cross-border access to electronic evidence*, p.9
251 Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du Règlement UE 2016/679, 25 mai 2018
252 CEPD, *Supra ibidem*, p.5
253 CEPD, *Supra ibidem*, p.10
254 Art. 70, RGPD

protection des données[255]. Selon une approche fondée sur un *« double test [256]»*, les deux organes affirment que le flux transfrontière de données en vertu du CLOUD Act est possible si sont cumulativement respectés les articles 6 et 49 du RGPD. Le transfert étant une forme spécifique de traitement de données[257], il devra tout d'abord être licite[258], nécessaire[259], proportionnel à la finalité recherchée[260] et répondre à l'exigence de minimisation de la collecte[261]. A cet égard, le DoJ a précisé que le CLOUD Act ne visait pas les jeux de données brutes et indiscriminées[262]. Une fois considéré comme licite, le traitement devra ensuite correspondre à l'une des exceptions de l'article 49, étant entendu que l'exception « pour motif d'intérêt public » doit renvoyer à un intérêt reconnu par le droit de l'Union et non par le droit américain[263].

47. L'analyse des interprétations de l'article 49 démontre qu'il n'existe aucune voie de droit permettant aux fournisseurs de services de transférer directement aux autorités américaines les données stockées dans l'UE. Souhaitant contourner la coopération judiciaire, le législateur américain a donc crée son propre cadre bilatéral d'échanges de preuves numériques.

B – Mécanisme de résolution du conflit de loi et tentative de résolution européenne

48. Le cadre bilatéral imaginé par le législateur américain est fondé sur la conclusion d'accords exécutifs (e*xecutive agreements)* qui répondent à certaines conditions et ouvrent des droits spécifiques aux Etats tiers (1). Réagissant à l'initiative américaine, la Commission a fait une proposition de règlement E-evidence et le Conseil de l'Europe prépare un second Protocole à la Convention de Budapest sur la cybercriminalité (2).

255 EDPB and EDPS, *Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negociations of an EU-US Agreement on cross-border access tto electronic evidence,* 10 juillet 2019
256 Ibidem, p.3
257 Art. 44, RGPD
258 Art. 6§1, RGPD
259 Art. 6§1 (c)
260 Art. 6§4 (a)
261 Art. 5§1 (c)
262 Department of Justice, Ibidem, p. 5
263 CEPD and EDPS, Ibidem, p.7

1 – Les accords exécutifs bilatéraux du CLOUD Act: mécanisme asymétrique de résolution du conflit de lois

49. La mise en place par le législateur américain d'un mécanisme bilatéral d'échanges de données part du constat suivant : les demandes d'accès aux preuves numériques adressées aux Etats-Unis sont bien plus nombreuses que celles qu'ils adressent aux Etats tiers[264]. L'exemple de l'entraide pénale franco-américaine illustre ce déséquilibre. En 2018, la France a émis 61 requêtes là où les Etats-Unis en ont formulé 40[265]. En 2019, Facebook, Twitter et Google[266] ont reçu plus de 418 000 demandes officielles d'accès aux données et aux comptes de leurs utilisateurs émanantt de plus de 80 Etats. Ces trois plateformes attestent d'une augmentation significative des demandes entre 2018 et 2019. En moyenne, les Etats parties à la Convention de Budapest autres que les Etats-Unis envoient 150 000 demandes annuelles aux principaux prestataires de services américains[267]. En marge des Traités d'entraide judiciaire, le CLOUD Act dessine donc les contours d'un régime spécifique applicable aux Etats tiers.

50. Pour accéder aux données des plateformes selon la voie simplifiée ouverte par le CLOUD Act, l'État tiers doit conclure un accord exécutif avec les Etats-Unis[268] . En vertu de la Constitution, les Etats-Unis peuvent s'engager dans un accord international selon deux procédures. Soit l'exécutif obtient une autorisation à la majorité des deux-tiers du Sénat pour signer un Traité[269]; soit il obtient une délégation législative pour conclure un accord exécutif du Congrès *(Congressional executive agreements).* C'est cette dernière procédure qui est retenue par le CLOUD Act. L'Attorney General et le Secrétaire d'État devront d'abord certifier au Congrès que l'État tiers remplit un ensemble de conditions[270]. Ensuite, l'accord exécutif fera l'objet d'un examen approfondi par les deux Chambres *(congressional review)*[271] qui, in fine, pourront le désapprouver par une résolution conjointe *(joint resolution)*[272], votée à la majorité[273].

264 Department of Justice, Ibidem, p.5
265 Source Direction des affaires criminelles et des grâces, citée dans *Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale*, Rapport établi par Raphael Gauvain, 26 juin 2019, p.34
266 https://transparency.twitter.com/fr.html; https://transparencyreport.google.com/?hl=fr; https://transparency.facebook.com/;
267 R. Bismuth, *Ibidem*, p.12 (49)
268 18 U.S.C § 2723
269 U.S Constitution, Article II § 2
270 18 U.S.C § 2523 (d) (1) (A) (B)
271 18 U.S.C §2523 (d) (4)
272 18 U.S.C §2523 (d) (4) (A)
273 18 U.S.C § 2523 (d) (4) (C)

51. Pour conclure un accord exécutif en vertu du CLOUD Act, l'État tiers doit assurer *« une protection substantielle et procédurale robuste de la vie privée et des libertés civiles*[274] *»*. Il s'agit là d'un préalable. Cette exigence est appréciée au regard d'une série de critères tels que l'adhésion à la Convention de Budapest ou la mise en place d'un arsenal législatif contre le cybercrime[275] ; le respect des principes de l'Etat de droit *(Rule of law)* fondé sur la non-discrimination[276] . De même, l'État tiers doit respecter les droits fondamentaux de l'Homme[277] et tout particulièrement : le droit à la vie privée[278], le droit à un procès équitable[279], la liberté d'expression et d'association[280], l'interdiction des arrestations et des détentions arbitraires[281], l'interdiction de la torture et des traitements inhumains et dégradants[282]. On retrouve ici une partie des droits processuels et matériels garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales (CESDH) à laquelle les Etats-Unis ont adhéré. Néanmoins, le CLOUD Act n'y fait pas explicitement référence. Ensuite, l'existence d'un contrôle des procédures d'accès aux données, de leur utilisation[283], de la transparence de leur traitement[284] et du respect du principe de neutralité du Net[285] est aussi prise en considération. L'imposition de ces conditions semble a priori exclure une vaste majorité d'États à travers le monde. Le texte ne précise cependant pas si une structure politique institutionnalisée tel que l'UE est éligible à cette procédure.

52. En cas de conclusion d'un accord exécutif, l'État tiers pourra formuler des requêtes d'accès aux données directement auprès des fournisseurs de services assujettis droit américain, sans passer par les Traités d'entraide mutuelle. Cependant, cette requête sera soumise à des impératifs de fond et de forme. Tout d'abord, elle ne pourra en aucun cas viser une « personne américaine » directement[286] ou indirectement[287]. En cas de collecte incidente, toutes les mesures appropriées de minimisation[288]visées au Foreign Intelligence Surveillance Act (FISA)[289], devront être prises. Cette interdiction introduit une absence de réciprocité entre les droits d'accès des Etats-Unis qui peuvent viser des personnes non-américaines[290] et ceux des Etats tiers qui ne peuvent pas viser les personnes

274 18.U.S.C § 2523 (b) (1)
275 18 U.S.C § 2523 (b) (1) (B) (i)
276 18 U.S.C § 2523 (b) (1) (B) (ii)
277 18 U.S.C § 2523 (b) (1) (B) (iii)
278 18 U.S.C § 2523 (b) (1) (B) (iii) (I)
279 18 U.S.C § 2523 (b) (1) (B) (iii) (II)
280 18 U.S.C § 2523 (b) (1) (B) (iii) (III)
281 18 U.S.C § 2523 (b) (1) (B) (iii) (IV)
282 18 U.S.C § 2523 (b) (1) (B) (iii) (V)
283 18 U.S.C § 2523 (b) (1) (B) (iv)
284 18 U.S.C § 2523 (b) (1) (B) (v)
285 18 U.S.C § 2523 (b) (1) (B) (vi)
286 18 U.S.C § 2523 (b) (4) (A)
287 18 U.S.C § 2523 (b) (4) (B)
288 18 U.S.C § 2523 (b) (2)
289 50 U.S.C § 1801
290 18 U.S.C § 2713

américaines. Ensuite, la demande d'accès de l'autorité étrangère devra s'inscrire dans le cadre d'une enquête pénale visant à prévenir, détecter ou poursuivre un crime sérieux, un acte de terrorisme[291], les menaces de mort *(death threats)* ou la mise en danger physique d'autrui[292]. Au-delà de l'imprécision du champ de ces infractions, on relève ici une seconde asymétrie. En effet, alors que les infractions de sûreté publique constituent une base légale pour les requêtes américaines, ce n'est pas le cas pour celles des Etats tiers. Surtout, les infractions sont ici listées dans le corps du texte législatif et non dans l'exposé des motifs comme c'était le cas pour les requêtes gouvernementales américaines. Par ailleurs, l'État tiers ne pourra exiger du prestataire américain de se voir communiquer les données en clair *(encryption neutral).* Comme l'ont démontré les négociations récentes avec l'Australie[293], les Etats qui disposent de lois obligeant les plateformes à déchiffrer les données avant leur divulgation aux services d'enquêtes, devront y renoncer. En outre, rien n'est dit de la communication de la clé de chiffrement. Enfin, le CLOUD Act impose un formalisme additionnel à la requête qui devra : comporter certaines mentions relatives à l'identité de la personne[294], mentionner les obligations auxquelles les entreprises américaines sont soumises sur le territoire de l'État tiers[295] et faire l'objet d'un contrôle juridictionnel[296]. En conséquence, il existe plusieurs prérequis à la conclusion d'un accord exécutif avec les Etats-Unis et l'État tiers devra respecter certaines restrictions. Néanmoins, une marge de négociation est envisageable comme l'a démontré le Royaume-Uni en signant le premier accord exécutif conforme au CLOUD Act.

53. L'accord exécutif du 7 octobre 2019[297] permet d'identifier les points ouverts à la discussion. Ainsi, les parties ont crée un *« contrôle administratif de qualité[298] »* de la requête gouvernementale dans le cadre duquel le fournisseur de services pourra la contester[299]. A ce titre, le fournisseur pourra s'opposer à la demande de la partie requérante devant la partie requise qui pourra alors refuser d'y faire droit[300]. En outre, le Royaume Uni dispose d'un veto pour s'opposer à toute requête américaine visant à prononcer une peine de mort aux États-Unis[301]. De leur côté, les États-Unis peuvent utiliser

291 18 U.S.C § 2523 (b) (4) (D) (i)
292 18 U.S.C § 2523 (b) (4) (G)
293 https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption
294 18 U.S.C § 2325 (b) (4) (D) (ii)
295 18 U.S.C § 2325 (b) (4) (D) (iii)
296 18 U.S.C § 2325 (b) (4) (D) (v)
297 Office of Attorney General, *Explanation of Each Consideration in Determining that the Agreement Satisfies the Requirements of 18 U.S.C § 2523 (b),* November 27 2019
298 Art. 5§7 Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime
299 Art. 5 § 11, Ibidem
300 Art. 5 § 12, Ibidem
301 Art. 8 § 4 (a), Ibidem

un mécanisme similaire concernant la liberté d'expression[302]. Par ailleurs, la notion de « crime sérieux » est définie comme renvoyant à tous les crimes punis d'une peine de prison de 3 ans ou plus[303]. Bien que cet accord entre le Royaume-Unis et les États-Unis apporte des précisions d'importance concernant les éléments devant figurer dans la requête ainsi que les procédures administratives au soutien desquelles de telles requêtes pourront être contestées, il maintient une asymétrie entre les droits des deux pays. Notamment, le DoJ pourra continuer d'accéder aux données des citoyens britanniques.

54. En l'absence d'accord, les États devront recourir aux mécanismes des Traités d'entraide judiciaire. Cette ultime solution fait dire au DoJ que le CLOUD Act intervient en complément de tels Traités plus qu'il ne les supprime. Dans ce cas, le pays tiers sollicitera directement les autorités américaines qui solliciteront à leur tour le fournisseur de services. Si les données ne sont pas stockées sur le territoire des Etats-Unis, l'État requérant devra solliciter une assistance mutuelle du pays où réside le serveur pertinent, après s'être enquis du lieu de localisation des données auprès de l'État américain.

55. En tout état de cause, la conclusion de l'accord avec le Royaume-Uni et les négociations en cours avec l'Australie ne semblent pas avoir entièrement lever les difficultés posées par l'asymétrie du texte américain. Face aux risques d'un déséquilibre juridique entre les Etats-Unis et les États membres de l'UE, la Commission européenne a présenté, dès le 17 avril 2018, une proposition de Règlement E-evidence[304] et soumis, en urgence, un mandat de négociation aux États-Unis à la demande du Conseil[305], le 5 mai 2018.

2 – Face au CLOUD Act, les réactions de l'UE et du Conseil de l'Europe

56. A la suite d'un processus initié en 2015, le Conseil de l'UE s'est prononcé, en 2017, sur la nécessité de refondre le cadre européen d'accès transfrontière aux preuves numériques pour au moins trois raisons[306]. D'abord, les instruments formels de la coopération judiciaire, à savoir les Traités d'entraide judiciaires entre les États membres de l'UE et la directive 2014/41/0E du 3 avril

302 Art. 8 § 4 (b), Ibidem
303 Art. 1, Ibidem
304 Proposition de Règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, Strasbourg, 17/04/2018
305 Conseil « Justice et affaires intérieures », 4-5 juin 2018
306 *Non-paper : Progress Report following the Conclusions of the Council of European Union on Improving Criminal Justice in Cyberspace*, Dec 2, 2016

2014[307], apparaissent lents, complexes et souffrent aussi d'un manque de volonté politique[308]. S'agissant ensuite de la coopération informelle fondée sur la demande d'accès directe auprès du prestataire numérique, la difficulté résulte de l'identification des interlocuteurs, de la lisibilité et de la prédictibilité du processus. En la matière, il existe de nombreuses disparités entre les États membres. A cela, s'ajoute une absence de consensus sur la notion de « situation transfrontalière » et sur les catégories de données considérées comme étant des preuves numériques et ce, malgré les définitions retenues par la Convention de Budapest[309].

57. Pour faciliter et accélérer l'accès transfrontalier intra-UE aux données, la proposition E-evidence envisage deux mesures. La première consiste à doter les États membres de l'UE d'un pouvoir extraterritorial de réquisition des données à l'encontre du fournisseur de service quel que soit le territoire de l'UE sur lequel il est établi[310]. Contrairement au cadre actuel, une autorité d'enquête pourrait ainsi adresser directement une demande *(production request)*[311] ou une injonction *(production order)*[312] à un fournisseur de services installé dans un autre État membre sans passer par l'État requis. Cette mesure repose sur un principe de reconnaissance mutuelle et supprime le contrôle juridictionnel ou administratif de la demande de l'État tiers. Concernant ce premier mécanisme, le Conseil estime que les catégories de données visées par les injonctions, les catégories de fournisseurs pouvant être saisis d'une demande, les personnes concernées et leur information, le degré d'implication de l'État requis ou encore le coût de la mise en œuvre de la mesure, restent à définir[313]. La seconde mesure a pour but d'harmoniser la possibilité pour les autorités d'accéder directement aux données en s'affranchissant de l'intermédiaire des fournisseurs notamment quand la localisation des données est inconnue[314]. A ce stade, la proposition E-evidence pose uniquement un cadre procédural si bien que chaque État serait libre d'autoriser ou non, l'accès direct à des systèmes informatiques en dehors de son territoire. En outre, la procédure de notification à l'État membre affecté ainsi que le droit à un recours effectif de la personne concernée par l'enquête restent encore à déterminer.

---

307 Directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale

308 En 2016, seuls 9 Etats membres avaient transposé la directive de 2014

309 Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques »

310 Technical document : measures to improve cross-border access to electronic evidence for criminal investigation following the adoption of the Council Conclusions on Improving Criminal Justice in Cyberspace

311 Elles ne sont ni contraignantes, ni exécutoires

312 Elles sont contraignantes et exécutoires

313 *Non Paper From the Commission services, Improving cross-border access to electronic evidence : Findings from the expert process and suggested way forward,* 22 mai 2017

314 J.S Mariez, *Une nouvelle étape vers un accès transfrontalier aux preuves numériques : l'initiative européenne « e-evidence » ou la recherche d'un équilibre entre efficacité des enquêtes pénales, droit des personnes concernées et sécurité juridique pour ls fournisseurs de services internet,* RLDI, n°146, 1er mars 2018, p.5

58. Dans sa déclaration du 29 novembre 2017 consacrée à l'analyse de la proposition E-evidence, le Groupe de travail de l'article 29 (G29) rappelle que l'accès des autorités aux données d'utilisateur, de contenu ou aux métadonnées est susceptible de constituer une atteinte au droit à la vie privée garanti par l'article 7 de la Charte des droits fondamentaux de l'UE. Par conséquent, la proposition E-evidence devra respecter *« l'essence des libertés et droit fondamentaux*[315] *»*. En outre, toute limitation apportée aux garanties du RGPD doit *« constituer une mesure nécessaire et proportionnée dans une société démocratique pour garantir (…) la prévention et la détection d'infractions pénales ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* [316]*»*. Devront ainsi être précisés l'étendue des limitations, les risques pour les droits et libertés des personnes concernées et, entre autres, les garanties destinées à prévenir les abus ou l'accès ou le transfert illicite des données[317]. Cette exigence fait écho au contrôle de la CJUE quant à l'existence *« de règles claires et précises régissant la portée et l'application de la mesure en cause*[318] *»*. A cet égard le G29 insiste sur la nécessité de prendre en compte les exigences du juge européen et de la CEDH[319].

59. En février 2019, la Commission européenne a finalement recommandé l'ouverture de négociations avec les États-Unis à partir d'un mandat comportant trois axes : l'obtention accélérée des preuves numériques, la gestion des conflits normatifs et le respect des droits fondamentaux[320]. La proposition E-evidence sous-tend la volonté du législateur européen d'éviter toute asymétrie des droits entre les États membres et les États-Unis qui pourrait résulter du bilatéralisme des accords exécutifs du CLOUD Act. L'enjeu est donc d'encadrer les transferts de preuves numériques intra-européens conformément aux garanties offertes par le RGPD et par la Charte des droits fondamentaux. Cet enjeu est d'autant plus grand que les accords exécutifs ne peuvent a priori être conclus qu'avec des États. En conséquence, l'harmonisation de la coopération judiciaire en matière d'accès aux données apparaît comme un préalable à tout engagement avec les États-Unis.

60. Enfin, la proposition E-évidence s'inscrit pleinement dans les objectifs du Comité de la Convention sur la cybercriminalité (T-CY). Ce dernier prépare en effet l'adoption d'un second

315 Art 23§1, RGPD
316 Art. 23§1 (d), RGPD
317 Art. 23§2, RGPD
318 CJUE, Aff.jointes C-203/15 et C-698/15, §§ 109-117, 21 décembre 2016
319 CJUE, aff.jointes C-2013/15 et C698/15, Tele2 Sverige AB et Secretary of State of the Home Department, 21 décembre 2016
320 *Commission recommends negociating international rules for obtaining electronic evidence*, Press release, 5 février 2019

protocole à la Convention de Budapest sur la cybercriminalité[321], à partir des axes de travail dégagés par le Groupe sur les preuves dans le Cloud[322], à savoir: la nécessité de poser des exigences et des seuils différents pour l'accès aux données en fonction des catégories de données, la protection des données et la sauvegarde de l'État de droit, la perte de la connaissance de la localisation des données et le fait que les États recourent à un accès transfrontalier unilatéral de données, le critère de rattachement qui permet de déclencher la compétence de l'État à l'égard du fournisseur de services, le régime de la publication volontaire des données ou encore la divulgation accélérée des données en cas d'urgence. Un mandat a été émis portant sur l'amélioration de l'efficience de l'entraide judiciaire, l'encadrement de la coopération directe avec les fournisseurs de services et des pratiques en matière d'accès transfrontalier aux données ainsi que sur la sauvegarde des droits fondamentaux et de la protection des données.[323] Les séances de travail plénières qui se sont déroulées entre 2017 et 2019 ont abouti à l'organisation d'une conférence Octopus en novembre 2019 ainsi qu'à la volonté d'associer la société civile à la rédaction de ce Second Protocole.

61. En conséquence, le CLOUD Act et ses effets sur les États tiers constituent l'élément déclencheur de réflexions et de négociations visant à mieux encadrer l'accès aux preuves numériques. L'Union européenne très concernée par le texte étant donné le grand nombre de data centers américains qu'elle accueille, a cependant été critiquée pour son indécision et sa réaction tardive[324]. Le Conseil de l'Europe, quant à lui, s'est également vu imposer un agenda juridique, voire politique par le législateur américain. En tout état de cause donc, le CLOUD Act apparaît comme un instrument de l'influence des États-Unis sur les ordres juridiques des autres États dans le monde.

321 Council of Europe, Coopération internationale renforcée sur la cybercriminalité et les preuves électroniques:vers un protocole à la Convention de Budapest, 5 septembre 2019

322 https://www.coe.int/en/web/cybercrime/ceg

323 T-CY, Comité de la Convention sur la cybercriminalité, *Accès de la justice pénale aux preuves électroniques dans le Cloud : recommandations pour examen par le T-CY*, 16 septembre 2016

324 E. Mignon, *Le Cloud Act ou l'impuissance démasquée*, Revue des juristes de Sciences Po, n°16, Janvier 2019, p.12

CONCLUSION

62. Comme démontré ci-avant, le CLOUD Act vient amender différentes dispositions du SCA pour résoudre la problématique de la localisation des données. Cette dernière avait été soulevée à l'occasion de l'affaire Microsoft et survient généralement dans le cadre de l'enquête pénale. En ce sens, la clarification apportée par le texte, consiste plus à mettre en cohérence le droit américain et les pratiques informelles des services gouvernementaux, qu'à rénover le cadre procédural de l'accès aux preuves numériques posé par le SCA et le 4ème Amendement de la Constitution. Avec le CLOUD Act, les autorités américaines peuvent exiger que leur soient directement communiquées les informations requises, quel que soit le territoire de leur stockage. Eu égard à la mainmise des entreprises du numérique américaines sur la quasi-totalité des données mondiales, le Gouvernement des Etats-Unis peut désormais se prévaloir d'un accès potentiel à une quantité conséquente d'informations. Au-delà de cette clarification, de nombreuses ambiguités demeurent. Notamment, les imprécisions qui entourent les notions de « crime sérieux » ou de « personne américaine » ne permettent pas de saisir entièrement son champ d'application. Enfin, le CLOUD Act ne crée aucun droit pour la personne ciblée par la requête gouvernementale. Au contraire, il introduit une asymétrie des garanties entre les « personnes américaines » et celles qui ne le sont pas. La Comity Analysis a certes pour objet de limiter ce déséquilibre mais son efficacité n'est pas prouvée à ce stade.

63. Conscient que les dispositions du CLOUD Act heurtent la compétence territoriale des Etats tiers mais aussi que le RGDP est susceptible de bloquer son exécution, le législateur américain a mis en place un cadre d'échange bilatéral de données. Cependant, comme nous l'avons montré, le bilatéralisme envisagé par les Etats-Unis n'est pas réciproque. On peut dès lors se demander si le texte américain ne risque pas de produire l'effet inverse à celui escompté, c'est à dire provoquer l'adoption de lois de territorialisation des données visant à mettre en échec son exécution. Par ailleurs, en marge des Etats qualifiés, il y a ceux qui continueront de recourir aux Traités d'entraide judiciaire. Semble donc apparaitre donc un accès transfrontière à la preuve numérique à trois vitesses.

63. Aux Etats-Unis, l'adoption du CLOUD Act a suscité diverses réactions. Les plateformes numériques qui ont largement participé à son élaboration[325], s'en sont fortement réjouit. De fait, le texte leur offre une voie d'opposition dédiée et ne crée aucune sanction particulière. En outre, en consacrant le lien personnel qui les unit aux Etats-Unis pour les protéger d'un éventuel conflit de

325 J. Daskal, *Unpacking the Cloud Act*, Eucrim 4/2018

lois aux lourdes conséquences financières potentielles, le texte reconnaît explicitement leur rôle d'intermédiaire et de ressource dans la conduite de l'enquête pénale[326]. En ce sens, le CLOUD Act contribue à l' *« institutionnalisation des rapports[327]»* entre l'État fédéral et les entreprises de la Silicon Valley. Au contraire, les associations de protection des libertés civiles ont fait part de leur indignation. Elles ont notamment indiqué que cette loi menace la vie privée des Américains, des lanceurs d'alerte, des activistes et des réfugiés politiques car trop peu de garde-fous sont prévus pour éviter une collecte indiscriminée des données. De même, le pouvoir discrétionnaire de l'Attorney General et la qualité du contrôle juridictionnel exercé lors de la conclusion d'un accord exécutif ont été vivement critiqués. En mai dernier, l'adoption au Sénat d'un amendement au Patriot Act permettant au Federal Bureau of Investigation (FBI) de collecter l'historique de navigation des Américains sans mandat, semble légitimer leurs inquiétudes.

64. En Europe, c'est la capacité du RGPD à bloquer l'exécution du CLOUD Act qui a été au centre des préoccupations. Les diverses interprétations que les institutions et les organes de l'UE ont pu donner de l'article 49, ont dénoté une absence de consensus en son sein. *In fine*, celle retenue par le CEPD, au demeurant très restrictive, fait écho à une défiance ancienne de l'UE à l'égard du Gouvernement américain, régulièrement soupçonné de se livrer à des activités de renseignement. A ce stade donc, les géants du Net sont pris en étau entre les exigences du RGPD dont le non-respect peut entrainer une sanction financière extrêmement lourde[328] et celles du CLOUD Act. Cette insécurité juridique concernant à la fois les prestataires et les droits des personnes, explique que la réponse de l'Europe se déploie à deux niveaux. Au sein de l'UE d'abord, l'enjeu est de protéger les Etats membres du bilatéralisme non-réciproque des Etats-Unis, tout en maintenant les garanties relatives à la protection des données personnelles. Le but de la proposition E-evidence est de créer un cadre harmonisé de la collecte transfrontière des preuves numériques à l'intérieur des frontières de l'UE et dans le respect du RGPD. Au sein du Conseil de l'Europe ensuite, l'enjeu est d'éviter des inégalités entre les Etats en proposant un nouveau cadre de coopération judiciaire. C'est l'objet du second Protocole de la Convention sur la cybercriminalité. A ce stade, il reste à savoir suivant quelle temporalité ces démarches aboutiront et si elles pourront faire émerger un cadre d'accès transfrontière aux données respectueux des droits des personnes.

326 A.Z Rozenshstein, *Surveillance intermediaries*, Stanford Law Review, vol 70, 2018

327 J. Charpenet, *Plateformes digitales et Etats : la corégulation par les données. Le cas des requêtes gouvernementales*, *Revue internationale de droit économique*, mars 2019

328 Art. 83, RGPD