Le US Cloud Act
vu de France : craintes légitimes ou peurs inutiles ?

Par Emmanuelle Legrand

Sans prétention d'exhaustivité, le présent article a pour ambition de proposer au lecteur quelques clés de lecture du US Cloud Act et de la recommandation de la Commission européenne en vue de négociations UE-US, à partir de l'analyse des textes, afin de mieux comprendre le cadre dans lequel pourrait s'inscrire l'action de l'Union européenne.

(1) Le texte est disponible en anglais à : https://www.govtrack.us/congress/bills/115/s2383/tex

(2) https://www.lesechos.fr/tech-medias/hightech/bruno-le-maire-vent-debout-contre-le-cloud-act-americain-991515

EMMANUELLE LEGRAND

Magistrate de liaison française en Europe du Sud Est

Signé par le président Trump, le 23 mars 2018, le US Cloud Act[1] a suscité de nombreuses réactions aux États-Unis comme en Europe. En France, des craintes ont notamment été exprimées quant aux risques encourus par les entreprises nationales[2].

En octobre 2019, le département de justice américain annonçait la signature du premier « Executive agreement » (accord gouvernemental) avec le Royaume-Uni[3]. Quelques jours plus tard, l'ouverture de négociations avec l'Australie était officialisée[4].

De son côté, la Commission européenne présentait, en avril 2018, au Conseil ses propositions « E-evidence »[5] visant à faciliter l'accès transfrontière à la preuve

(3) Cet accord a été signé en octobre 2019 : https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists ; en décembre et janvier 2020, le Département de justice américain a adressé sa certification au Congrès américain, avec une prise d'effet prévue en juillet 2020 : https://www.justice.gov/dag/page/file/1236281/download.

(4) https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us ; l'Australie a préparé une loi à cette fin : https://www.lexology.com/library/detail.aspx?g=2cf0f5f7-4a6b-4523-b04c-4674296f9f74.

(5) https://www.consilium.europa.eu/fr/policies/e-evidence/

numérique et recevait mandat, le 6 juin 2019, pour ouvrir des négociations avec les États-Unis sur le même sujet. Les deux initiatives européennes partent du constat largement partagé par les magistrats et enquêteurs européens de la lenteur des outils traditionnels de l'entraide pénale, peu adaptés aux spécificités de la preuve électronique. Ce constat a déjà conduit les services d'enquête de nombreux pays à s'adresser directement aux fournisseurs de services américains pour obtenir des données techniques, et ce sans cadre juridique international clair, laissant ainsi le droit national et la jurisprudence fixer les limites d'une pratique développée pragmatiquement au fil du temps.

Les échanges directs des enquêteurs avec les fournisseurs de services américains reposent en l'état sur deux principes : d'une part, en général, seules les données de trafic[6], souvent utiles pour orienter l'enquête, peuvent être communiquées aux enquêteurs étrangers, conformément au droit américain. D'autre part, cette communication aux services d'enquête étrangers intervient sur une base volontaire, après analyse au cas par cas par les fournisseurs de service américains, selon les règles fixées par eux et par le droit américain[7]. C'est donc aujourd'hui dans un cadre juridique incertain, reposant pour beaucoup sur la bonne volonté des acteurs privés, que les enquêtes pénales en France, comme en Europe, peuvent avancer, ou pas.

De nombreuses publications ont fait état des craintes suscitées par la promulgation de l'US Cloud Act. Toutefois, peu ont tenté de déchiffrer les termes employés, pourtant riches d'enseignements[8].

Les craintes exprimées sur le US Cloud Act apparaissent-elles véritablement fondées, à la lumière des termes choisis par ses rédacteurs et par l'Union européenne ?

Le US Cloud Act (1ère partie) : la clarification d'une pratique en matière d'obtention de données stockées à l'étranger

L'US Cloud Act s'organise en deux parties.
La première constitue le « Microsoft fix »

(6) On opposera ici par souci de simplicité les données de trafic, qui ne révèlent pas le contenu des échanges entre les personnes mais apportent des informations techniques sur ces échanges, aux données de contenu, qui contiennent le contenu d'une communication écrite ou verbale.

(7) Voir notamment la recommandation de la Commission européenne en faveur de l'ouverture de négociations avec les États-Unis en vue d'un accord sur l'obtention transfrontière de la preuve électronique en matière pénale, page 5 : « As regards non-content data, due to the growing number of Mutual Legal Assistance requests addressed to the United States of America, the U.S. authorities have encouraged EU law enforcement and judicial authorities to request non-content data from U.S. service providers directly, and U.S. law allows but does not require U.S.-based service providers to respond to such requests. An EU-U.S. Agreement would provide more certainty, clear procedural safeguards and reduce fragmentation for EU authorities to access non-content data held by U.S. service providers. It would also allow for reciprocal access by U.S. authorities to data held by EU service providers."

(8) On pourra citer notamment Christakis, Theodore, 21 Thoughts and Questions about the UK/US CLOUD Act Agreement: (and an Explanation of How it Works – With Charts) (October 13, 2019). European Law Blog, October, 2019, Available at SSRN: https://ssrn.com/abstract=3469704

en amendant la loi de procédure américaine et en entérinant la possibilité pour les autorités américaines d'accéder à des données quel que soit leur lieu de stockage.

Le Cloud Act modifie ainsi le titre 18 du US Code[9]. Il clarifie une pratique qui avait été remise en cause par la société Microsoft, dans le cadre du bras de fer juridique engagé en 2014 contre le gouvernement américain, en refusant de communiquer à ce dernier des données stockées en Irlande[10]. La promulgation du Cloud Act, sans attendre la décision de la Cour suprême, est ainsi venue clore le débat juridique.

Désormais, une autorité américaine peut légalement requérir la production de données auprès de sociétés, quel que soit le lieu de stockage de ces données[11].

Le US Cloud Act et le juge américain : à quelles entreprises ne s'appliquera-t-il pas ?

Le Cloud Act ne précise toutefois pas à quelles entités cette obligation de communication des données aux autorités américaines est limitée. Ainsi, par défaut, on peut penser que toute entreprise tombant sous le coup de la compétence des juridictions américaines (US jurisdiction) est susceptible d'être concernée[12].

La section §2713 de l'*US Code*[13] définit néanmoins le fournisseur de service concerné comme étant celui qui *a la possession, la garde ou le contrôle* des données, où que se situe la communication[14]. Cette obligation s'applique aux fournisseurs de service de communication électronique comme aux services informatiques à distance[15].

Les sociétés américaines ne semblent donc pas être les seules concernées. Le droit américain, rappelons-le, est un droit de *Common law*, qui évolue essentiellement par les décisions des tribunaux[16]. Or, nul ne sait en l'état comment le juge américain interprétera la notion de « US jurisdiction » dans l'application spécifique du *Cloud Act*.

Comparaison n'est pas raison. Néanmoins, il n'est pas inutile de rappeler que les

(9) Les modifications touchent le titre 18 du US Code, intitulé « Crimes and criminal procedure », et concernant donc a priori les enquêtes pénales. Plus précisément, ce sont les chapitres 119 (« Wire and electronic communications interception and interception of oral communications ») et 121 (« Stored wire and electronic communications and transactional records access ») qui sont modifiés par le Cloud Act.

(10) https://www.nextinpact.com/article/27715/105782-une-etude-dresse-lesenjeux

(11) Voir 18 U.S. Code §2713 : https://www.law.cornell.edu/uscode/text/18/2713

(12) Aucun élément en sens contraire ne semblant en l'état amener à une autre conclusion. Dans le même sens que l'auteure: https://www.justice.gov/opa/press-release/file/1153446/download

(13) 18 U.S. Code § 2713 « Required preservation and disclosure of communications and records »

(14) https://www.law.cornell.edu/uscode/text/18/2713

(15) Cette dernière formulation suscite un intérêt particulier lorsque l'on s'interroge par exemple sur la situation d'une société française qui n'aurait de lien avec les Etats-Unis que son service de stockage de données en ligne.

(16) https://ppp.worldbank.org/public-private-partnership/legislation-regulation/framework-assessment/legal-systems/common-vs-civil-law

juridictions américaines peuvent parfois retenir, notamment en matière civile[17], leur compétence 'élargie'[18], parfois même en tenant volontairement en échec les lois de blocage étrangères[19].

Reste à savoir si, dans l'hypothèse d'une interprétation large du juge américain sur l'application du Cloud Act aux sociétés étrangères, ces dernières estimeront devoir répondre aux demandes des autorités américaines ou si les initiatives nationales ou européennes leur apporteront des réponses.

La réponse de l'Union européenne (2e partie) : négocier un accord complet au niveau européen en matière pénale

Dans sa seconde partie, l'*US Cloud Act* autorise également le gouvernement américain à conclure des accords gouvernementaux (*Executive agreements*), avec des gouvernements étrangers[20].

L'objectif affiché est de faciliter l'obtention des données électroniques, y compris de contenu et en temps réel (non stockées), notamment des interceptions de communications[21], sous réserve pour l'État partenaire de répondre aux exigences fixées par le *Cloud Act*, et le cas échéant après avoir modifié sa loi interne. C'est à cette seconde partie de l'*US Cloud Act* que semble répondre la recommandation de la Commission européenne[22], présentée au Conseil en février 2019, en vue de l'ouverture de négociations avec les États-Unis. Cette recommandation eut pu paraître inutile si, comme cela a pu être évoqué de manière erronée, les propositions *E-Evidence* d'avril 2018, toujours en cours de discussion, avaient constitué une réponse au *Cloud Act*. Tel ne semble pas être le cas[23].

S'agissant de négociations UE-US, la lecture attentive des termes

(17) https://www.kirkland.com/publications/article/2019/03/can-your-overseas-company-be-taken-to-us-court

(18) En matière civile notamment, il est question de « long-arm jurisdiction » ou « long-arm statute » : https://www.law.cornell.edu/wex/long-arm_statute. Littéralement, les autorités judiciaires américaines peuvent donc, selon les domaines juridiques et les textes et jurisprudences, recourir à la théorie du « bras long » pour retenir leur compétence, parfois qualifiée d'extraterritorialité par certains observateurs. Voir à ce propos le rapport d'information sur l'extraterritorialité de la législation américaine déposée en octobre 2016 par la Commission des affaires étrangères et la Commission des finances de l'Assemblée nationale : http://www.assemblee-nationale.fr/14/pdf/rap-info/i4082.pdf

(19) Voir notamment sur la loi dite de blocage française du 26 juillet 1968 : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JOR

(20) En se dispensant ainsi du processus législatif habituellement applicable en matière de traités internationaux. Voir notamment C. Bradley, J. Landman Goldsmith, O.A. Hathaway, The failed transparency regime for executive agreements: an empirical and normative analysis: https://www.ssrn.com/abstract=3589900

(21) A noter sur ce point que le US Cloud Act modifie également les dispositions du US Code relatives aux outils de pen register et de trap and trace (voir notamment 18 U.S.Code §3121, qui crée une exception au principe de délivrance d'un mandat du juge notamment dans le cas d'une demande d'un gouvernement étranger dans le cadre d'un « executive agreement »). https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000532.pdf.

(22) https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

(23) Contrairement à ce que certains observateurs ont pu percevoir, les propositions E-Evidence de la Commission européenne d'avril 2018 ne pouvaient pas constituer une « réponse » au US Cloud Act, promulgué en mars 2018, car elles résultent directement des engagements pris par la Commission européenne dès 2015 dans le cadre de l'agenda sur la politique européenne de sécurité (https://ec.europa.eu/commission/presscorner/detail/en/IP_15_4865), de la déclaration commune des ministres de la justice et de l'intérieur des Etats-Membres et des représentants des institutions européennes sur le sujet de l'accès à

© EisenhansL - Fotolia

Le CLOUD Act est une alternative aux réglementations découlant du droit de l'UE. Son approche pose la question de la construction d'un modèle cohérent d'échange et de protection des données personnelles et d'échange d'informations probatoires dans le cadre de procédures pénales.

choisis par la Commission européenne, adoptés par le Conseil, suggère ainsi qu'elle n'entend pas inscrire ces négociations dans le cadre d'un accord gouvernemental, ni dans les conditions fixées par le Cloud Act. La possibilité d'un simple accord-cadre ne semble pas non plus être la piste privilégiée par la Commission[24].

En effet, tandis que le Cloud Act favorise la conclusion d'accords bilatéraux avec des Etats remplissant les conditions fixées par les États-Unis en matière d'État de droit[25], la Commission, gardienne des traités, semble adopter l'approche consistant à refuser qu'un État tiers s'octroie unilatéralement le rôle d'évaluateur de la situation de l'État de droit dans l'Union européenne, au profit d'une application harmonisée[26] du droit et des valeurs de l'Union au sein des États-Membres,

la preuve électronique au lendemain des attentats de Bruxelles en 2016 (https://www.consilium.europa.eu/fr/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/), des consultations réalisées par la Commission européenne, des conclusions du Conseil de l'Union européenne demandant à la Commission en novembre 2017 de faire des propositions d'amélioration de l'accès transfrontière à la preuve électronique (https://www.consilium.europa.eu/media/31666/st14435en17.pdf), et à une étude d'impact détaillée, le tout bien avant la promulgation du US Cloud Act. La véritable question est donc de savoir si le Cloud Act ne constitue pas, lui, une réponse aux efforts annoncés de la Commission de faciliter l'accès aux données au sein de l'Union européenne.

(24) Extrait de la recommendation de la Commission européenne, du 5 février 2019 page 4: « The European Union has an interest in a comprehensive agreement with the United States of America, both from the perspective of protecting European rights and values such as privacy and personal data protection and from the perspective of our own security interests."

(25) https://www.justice.gov/dag/page/file/1153466/download

(26) La recommandation de la Commission européenne adoptée en juin 2019 par le Conseil mentionne clairement l'intérêt d'un accord au niveau européen : « An agreement between the European Union and the United States would offer a number of practical advantages: (…)It would reduce the risk of fragmentation of rules, procedures, and harmonise the rights and safeguards through a single negotiation mandate for all European Union Member States with the United States ensuring non-discrimination between European Union Member States and their nationals (…)"

(27) On pourra citer à titre d'exemple le mandat d'arrêt européen, la décision d'enquête européenne, le renforcement des droits des victimes, ou celui des droits des suspects et accusés.

(28) Extrait du US Cloud Act : "the term `qualifying foreign government' means a foreign government".

(29) https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

(30) Du point de vue de l'auteure, le terme anglais original « order » ne saurait, du point de vue du droit français, recouvrir la notion de l'injonction, bien qu'utilisée par les juristes-linguistes de la Commission européenne dans la version française de la recommandation de la Commission européenne. Cette notion d'injonction, utilisée en matière civile, a en effet des conséquences juridiques totalement différentes de celle évoquée ici en matière pénale. Le terme « order » se rapproche donc davantage en droit français de la notion de réquisition judiciaire, en ce que cela oblige le destinataire à y répondre.

et du maintien d'un espace commun de liberté, de sécurité et de justice.[27]

Ainsi, si le fait de savoir si l'Union européenne pouvait ou non être qualifiée de gouvernement étranger pour conclure un accord gouvernemental selon les termes du US Cloud Act[28] a pu susciter des réflexions intéressantes, ce débat est en réalité sans grand intérêt, l'Union européenne ne s'étant pas engagée dans cette voie, tout en en prenant acte. Dès le titre de la recommandation de la Commission, le ton semble donné[29] : il s'agit en l'état de négocier un accord sur l'accès transfrontière à la preuve électronique, au niveau européen et non national, et uniquement à des fins de coopération judiciaire en matière pénale.

Cet intitulé n'a pas suscité beaucoup de réactions mais est pourtant riche de sens, puisque l'Union européenne fixe un cadre clair pour les négociations, et a fortiori quant à l'utilisation des données qui seraient éventuellement recueillies en vertu d'un tel accord. Or, le texte américain précise, quant à lui, en modifiant la section §2523 du titre 18 du US Code, que les « réquisitions »[30] aux entreprises doivent avoir pour objectif d'obtenir de l'information relative à la prévention, la détection, l'investigation ou la poursuite des infractions graves, incluant le terrorisme. Le *US Cloud Act* ne définit pas la notion d'infraction grave. Le droit français non plus.

La première difficulté soulevée par le texte du Cloud Act est de savoir de quel type de procédure on parle, puisque le rôle premier du système pénal n'est pas, en principe, de prévenir et de détecter mais de réprimer les infractions commises. Or, le Cloud Act ne précise pas qu'il s'appliquerait aux seules procédures pénales. Il ne précise pas non plus quelles seraient les autorités américaines qui s'adresseraient aux fournisseurs de services de l'État contractant[31].

(31) Le US Cloud Act fait seulement référence au « US gouvernement » et ne précise pas que son champ d'application se limite aux procédures judiciaires. Il semble préciser, certes, l'intervention d'un juge dans certains cas. Toutefois, pour ne citer l'exemple que du FBI, ce dernier ne dispose pas seulement des pouvoirs que l'on assimilerait en France à de la police judiciaire (https://www.wsj.com/articles/fbi-wants-audit-firm-to-review-how-it-makes-fisa-wiretap. Par ailleurs, la notion de « law enforcement » reste très large, et la mention de l'intervention d'un juge dans le texte du Cloud Act ne préjuge pas forcément, en l'absence de toute précision complémentaire, du cadre juridique dans lequel s'exercerait la communication de données. Le Cloud Act, s'agissant des exigences applicables aux États contractants en matière de minimisation des procédures, fait d'ailleurs une référence explicite aux procédures en vigueur selon le Foreign Intelligence Surveillance Act de 1978 (50 U.S.C. 1801).

En réalité, on relèvera que le premier accord gouvernemental conclu par les États-Unis l'a été avec le Royaume-Uni[32], avant de se tourner vers l'Australie[33]. Autrement dit, des accords entre trois pays du club dit des « Five Eyes »[34]. La question qu'on ne formule jamais clairement est donc celle-ci : l'objectif principal du Cloud Act et des accords gouvernementaux est-il vraiment de faciliter l'obtention de la preuve numérique dans le cadre pénal, dans le respect des principes généraux de la procédure pénale des État[35], ou plutôt de faciliter le transfert de données collectées dans le cadre des activités de renseignement[36]? Cette question demeure entière mais d'importance, lorsqu'on analyse les termes choisis par la Commission européenne dans sa recommandation au Conseil.

Ainsi, sans préjuger de l'issue des négociations, la Commission, en rappelant sa compétence, semble avoir proposé d'atteindre non un accord gouvernemental ou un accord-cadre, mais un accord complet au niveau européen assurant la protection adéquate et non discriminatoire des droits des citoyens de l'UE, dans le respect des principes et valeurs de l'Union, uniquement dans le cadre des procédures pénales et assorti de conditions claires et de garanties permettant aux autorités judiciaires européennes, dans le prolongement des propositions E-Evidence, d'user d'une nouvelle possibilité procédurale adaptée aux spécificités de la preuve numérique.

Le texte européen semble ainsi partir d'un présupposé différent du Cloud Act : la recherche d'un accord complet en matière pénale, aux conditions négociées, équilibrées, et fondées sur la réciprocité.

A titre d'exemple, l'objectif de réciprocité

(32) A cette époque, le Royaume-Uni était pourtant toujours soumis, a priori, au principe de loyauté envers l'Union européenne.

(33) Voir l'article de Paul Greaves et Peter Swire « New developments for the UK and Australian executive agreements with the US under the Cloud Act" : https://www.crossborderdataforum.org/new-developments-for-the-u-k-and-australian-executive-agreements-with-the-u-s-under-the-cloud-act-2/
Dans cet article les auteurs notent notamment que la proposition de loi visant à adapter la procédure australienne mentionne la possibilité pour les autorités de solliciter les fournisseurs de service dans le cadre du renseignement. Ce choix n'est donc pas anodin.

(34) Alliance des services de renseignements américains, australiens, britanniques, canadiens et néo-zélandais : https://fr.wikipedia.org/wiki/Five_Eyes

(35) Citons entre autres le principe du contradictoire, de la proportionnalité, du respect des droits de la défense ou encore le droit au recours effectif.

(36) Aux État-Unis, l'autorisation nécessaire pour certaines activités de renseignement relèvent de la compétence de la United States Foreign Intelligence Surveillance Court. Les activités de renseignement ne sont donc pas totalement dépourvues d'un contrôle par un juge, sans que cela ne soit régi par les règles du procès pénal à proprement parler. La notion de juge ou de tribunal ne permet dès lors pas à elle seule de déterminer le cadre d'utilisation du US Cloud Act.
loi FISA (Foreign Intelligence Surveillance Act) s'applique aux activités.

(37) Le mot « reciprocal » apparaît à 7 reprises dans la recommandation de la Commission européenne.

(38) La définition de la « US person » est donnée à l'article 18 U.S. Code §2523 et inclut tout citoyen ou national des État-Unis, tout étranger résident permanent légal, toute association de fait (« unincorporated ») dont un nombre substantiel de membres sont citoyens des Etats Unis ou étrangers résidents permanents légaux, ou toute société créée aux État-Unis.

recherché par la Commission européenne[37] est intéressant, alors même que le Cloud Act exclut toute demande de données visant directement ou indirectement les « US persons », dont la définition apparaît bien large[38].

Si les négociations étaient intervenues dans le cadre de l'US Cloud Act, l'Union européenne, en affirmant son objectif de réciprocité, ne pourrait pas ignorer que l'application du principe de non-discrimination des citoyens de l'Union conduirait à un accord qui deviendrait presque sans intérêt pour les deux Parties.

Ces éléments conduisent à penser que la Commission européenne n'a pas entendu se situer au niveau du Cloud Act, mais à celui de la protection des principes, règles et valeurs communes des Etats-Membres et de la défense de l'espace européen de liberté, de sécurité et de justice[39].

(39) Le Conseil, dans sa directive de négociation, a repris l'essentiel des termes proposés par la Commission européenne, ne négligeant pas le fait d'inclure une clause relative à l'exclusion des faits pour lesquels la peine de mort ou la perpétuité réelle est encourue aux Etats-Unis. https://data.consilium.europa.eu/doc/document/ST-9666-2019-INIT/fr/pdf.

La proposition européenne : vers un accord équilibré, protecteur des droits et des données ?

Le constat de l'Union européenne est celui des praticiens, demandeurs d'outils juridiques plus adaptés en matière d'obtention de preuve numérique. Toutefois, pris entre l'approche unilatérale du Cloud Act d'un côté, et le RGPD et les propositions E-Evidence de l'autre, certains fournisseurs de services pourraient se retrouver confrontés à des conflits de loi[40]. Ainsi, l'un des objectifs affichés par la Commission semble de prévenir, et le cas échéant, de résoudre ces éventuels conflits de loi, tout en clarifiant le cadre juridique d'obtention des preuves numériques auprès des fournisseurs de services américains.

Toutefois, le *Cloud Act* s'inscrit dans une philosophie juridique propre au droit américain. Ainsi, ce texte n'impose pas, en lui-même, d'obligation aux fournisseurs de services d'un Etat contractant. Il vise uniquement à lever les obstacles juridiques leur interdisant de répondre à une autorité étrangère, comme les lois de blocage, sur la base d'une coopération volontaire. Il ne semble toutefois résoudre ni le problème de l'absence de réponse ni les conséquences juridiques qui en découleraient, sauf à modifier son droit interne pour s'octroyer une compétence extraterritoriale.[41]

(40) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

(41) Autrement dit, le US Cloud Act ne pose en lui-même aucune obligation expresse pour les fournisseurs de service, ni aucune sanction. C'est ainsi qu'il appartient au pays partenaire, s'il souhaite conclure un accord gouvernemental, d'amender sa législation interne pour lui donner le cas échéant une portée extraterritoriale et pouvoir sanctionner les manquements, à l'instar de ce qu'ont fait les Etats-Unis avec la première partie du US Cloud Act.

La recommandation de la Commission semble en revanche adopter une autre approche, plus proche de ce que nous connaissons en droit français notamment, visant à fixer des règles communes, à définir les conditions dans lesquelles l'on pourrait s'opposer aux décisions des autorités judiciaires, tout en assurant un droit au recours effectif.

Par ailleurs, la nécessité d'un accord entre l'Union européenne et les Etats-Unis assurant l'équilibre entre l'efficacité d'un outil disponible pour les autorités judiciaires et la protection adéquate des droits des personnes et de leurs données apparaît encore plus trouver son sens au regard de l'arrêt *Schrems* II du 16 juillet 2020[42], par lequel la Cour de justice de l'Union européenne a invalidé le bouclier de protection des données[43] (*Privacy Shield*) conclu entre l'Union européenne et les État-Unis.

Ainsi, si le Privacy Shield est un accord visant les transferts de donnée à des fins commerciales, la Cour, se référant à la Charte des droits fondamentaux de l'Union européenne, pointe les lacunes de la loi américaine en matière de sécurité nationale, qui, en l'état, ne permet pas d'assurer une protection adéquate, notamment en termes de proportionnalité et de recours effectif.

La lecture de cette décision soulève nécessairement des questions concernant d'autres accords transatlantiques existants[44] s'agissant des transferts de données en matière de sécurité et de justice.

Or, dans sa recommandation au Conseil en vue de l'ouverture de négociations, la Commission européenne rappelait justement la nécessité de garantir la protection des principes et droits fondamentaux reconnus par la Charte européenne des droits fondamentaux.

Cette décision apparaît d'autant plus intéressante que le 28 juillet 2020, Google annonçait le déploiement d'un nouveau câble sous-marin transatlantique pour le transfert de données internet[45], tandis que le sujet du chiffrement des

(42) Arrêt CJUE C-311/18 du 16 juillet 2020, Data Protection Commissioner contre Facebook Ireland Ltd, Maximillian Schrems, EECLI:EU:C:2020:559 (http://curia.europa.eu/juris/document/document.jsf;jsessionid=49B

(43) Le Bouclier de Protection des Données, mieux connu sous le nom de « Privacy Shield », est un mécanisme d'auto-certification pour les entreprises établies aux États-Unis qui a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données à caractère personnel transférées par une entité européenne vers des entreprises établies aux États-Unis. Ce mécanisme est par conséquent considéré comme offrant des garanties juridiques pour de tels transferts de données. (Source CNIL).

(44) Voir notamment Theodore Christakis, After Schrems II : Uncertainties on the Legal Basis for Data Transfers and Constitutional Implications for Europe, juillet 2020, https://europeanlawblog.eu/2020/07/21/after-schrems-ii-uncertainties-on-the-legal-basis-for-data-transfers-and-constitutional-implications-for-europe/#para_2

(45) Voir notamment https://cloud.google.com/blog/products/infrastructure/announcing-googles-grace-hopper-subsea-cable-system et https://www.lemonde.fr/pixels/article/2020/07/30/google-a-commence-a-deployer-un-nouveau-cable-internet-transatlan

données continue de diviser les autorités en quête d'éléments probants et les citoyens en recherche légitime de protection de leurs données.

Conclusion

Les débats sur les initiatives de la Commission européenne en matière d'obtention transfrontière de la preuve numérique sont légitimes et souhaitables dans une société démocratique. Le défi de l'Union européenne est d'aboutir à une solution qui facilite le travail des enquêteurs et des magistrats européens dans les enquêtes pénales où l'obtention de la preuve numérique est souvent déterminante, tout en assurant aux citoyens le nécessaire respect de leurs droits et la protection de leurs données.

En l'état du droit, les praticiens français et européens se heurtent souvent au bon vouloir des fournisseurs de service qui se réfugient derrière la législation étrangère, tout en développant leurs services sur le marché européen.

Si les enquêtes n'avancent pas faute d'éléments de preuve numérique, cela se fait nécessairement au détriment des victimes et au bénéfice, notamment, de la criminalité organisée et transnationale. Si les enquêtes avancent du fait d'une pratique pragmatique qui attend toujours d'être rattrapée par un cadre juridique international clair et efficace, cela peut se faire au détriment des droits des personnes suspectées, alors que la société civile attend une réponse de l'Union européenne qui soit à la hauteur de l'enjeu de la protection des données personnelles et des valeurs démocratiques qu'elle veut porter. C'est entre ces deux

écueils que l'Union européenne doit trouver la réponse juridique adaptée. Elle n'a pas d'autre choix, désormais, que de la trouver afin de protéger les droits et les données des citoyens de l'Union à la hauteur des valeurs qu'elle porte.

Ainsi, à ceux qui s'interrogent sur l'utilité d'un accord UE-US, tandis que les propositions E-Evidence sont toujours en discussion, une question mérite d'être posée : en l'absence d'un accord UE-US protecteur des droits et principes de l'Union, comment les entreprises françaises et européennes, dans un monde globalisé, peuvent-elles protéger efficacement leurs données contre une application extensive, unilatérale et incertaine du Cloud Act ?

AUTEURE

Emmanuelle Legrand est actuellement magistrate de liaison française en Europe du Sud Est. Elle a exercé précédemment des fonctions juridictionnelles au parquet de Nanterre où elle a notamment été référente cybercriminalité, puis en qualité de juge d'instruction au pôle financier JIRS de Paris, puis à Nanterre, spécialisée en matière économique et financière et en cybercriminalité.
Elle a également exercé au Bureau de l'entraide pénale internationale du ministère de la justice, ainsi qu'à la Commission européenne, en qualité d'experte nationale détachée, où elle a travaillé sur les questions de coopération judiciaire et de preuve numérique.
Elle a notamment fait partie de la Task Force E-evidence, et participé aux travaux de la Commission européenne en vue de l'ouverture de négociations avec les Etats-Unis sur la preuve numérique.

Elle intervient régulièrement à l'École nationale de la magistrature en formation initiale et continue, comme expert en cybercriminalité pour le Conseil de l'Europe, ou encore dans le cadre de la formation des enquêteurs spécialisés.

Elle est également titulaire d'un diplôme d'université en Cybercriminalité obtenu à l'Université de Montpellier 1, ainsi que d'un LL.M. en droit américain obtenu à la University of Texas School of Law.
Elle est également auditrice de la 1ère session nationale INHESJ-IHEDN sur la Souveraineté numérique et la Cybersécurité, et préside actuellement l'association des auditeurs de la session nationale.