Articles

Perquisitionner les nuages – *CLOUD Act*, souveraineté européenne et accès à la preuve dans l'espace pénal numérique

Frederick **T. Davis**
Avocat – Lecturer in Law, Columbia Law School

Charlotte **Gunka**
Ancien avocat au barreau de Paris – Membre du barreau de New York.
Chargée d'enseignement, Université Paris-Dauphine

Résumé
À l'heure où la crise du Covid-19 a fait prendre conscience de la nécessité pressante pour les États européens de renforcer leur souveraineté nationale à travers celle de l'Union européenne, un retour aux possibilités offertes par le CLOUD Act américain en matière de procédure pénale et de souveraineté numérique s'impose. Le CLOUD Act propose en effet de réformer les mécanismes d'entraide judiciaire en consacrant le critère de l'accès à la preuve numérique autorisant des perquisitions informatiques hors des frontières étatiques, quelle que soit la localisation des données. Bien que ce critère permette une application extraterritoriale plus étendue des procédures pénales américaines, l'analyse des législations en vigueur en France et au Royaume-Uni confirme que l'approche européenne n'est pas si différente de celle proposée par les États-Unis. L'émergence du monde informatique et l'accélération des nouvelles technologies ont créé un « espace pénal numérique », immatériel et sans frontière, qui nécessite une réforme des procédures pénales permettant une coopération internationale plus rapide et efficace contre la criminalité transnationale. Cette réforme doit permettre à l'Europe, notamment par le biais de son nouveau Parquet européen, d'affirmer son indépendance numérique aux moyens des droits fondamentaux qu'elle contribue à véhiculer et en assurant le respect des intérêts stratégiques de ses États membres.

Summary

At a time when the Covid-19 crisis has raised awareness over the urgent need for European Member States to enhance their national sovereignty through the European Union, it is essential to go back to the possibilities offered by the U.S. CLOUD Act with regard to criminal procedures and digital sovereignty. The CLOUD Act proposes a reform of current mutual legal assistance mechanisms by establishing access to digital evidence as the benchmark authorizing computer searches outside state borders, regardless of the location of the relevant data. Although this benchmark allows for more extensive extraterritorial application of U.S. criminal proceedings, an analysis of the legislation currently in force in France and the United Kingdom confirms that the European approach is not so different from the one proposed by the U.S. government. The emergence of the computer world and the acceleration of new technologies have created a "criminal digital space", ephemeral and borderless, which requires a transformation of criminal procedures allowing for faster and more efficient international cooperation against transnational crime. This should give an opportunity to Europe, in particular through its new European Public Prosecutor's Office, to assert its digital independence through the fundamental rights that it continues to promote and by ensuring the strategic interests of its Member States.

Adopté par les États-Unis en mars 2018, le *Clarifying Lawful Overseas Use of Data Act* (le « *CLOUD Act* ») a très rapidement suscité l'émoi de l'Union européenne (UE) et de la France en raison du caractère prétendument extraterritorial [1] de ses dispositions en matière de perquisition de données informatiques. [2] Le *CLOUD Act* permet aux autorités américaines dans le cadre d'enquêtes pénales ou administratives diligentées pour des infractions graves de demander auprès de tout fournisseur de services de communication (en anglais Communication Services Provider, ou « CSP ») soumis à la compétence du juge américain – l'obtention de données – qui appartiennent à des citoyens américains ou des personnes ayant une présence minimum aux Etats-Unis – qui sont accessibles depuis les Etats-Unis, – mais qui peuvent être stockées sous forme numérique hors du territoire américain. Bien que le *CLOUD Act* vise différents moyens de communication (notamment les e-mails et les messageries instantanées), [3] c'est la propagation de la technologie *Cloud computing* [4] qui a précipité son adoption puisque celle-ci permet le stockage de données au sein d'un « nuage numérique » sans réelle localisation matérielle ou territoriale. Au-delà d'une volonté d'imposer les procédures

(1) R. Bismuth, *Every Cloud has a silver lining* – Une analyse contextualisée de l'extraterritorialité du *Cloud Act*, JCP E 2018, p. 1497.

(2) Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et des mesures à portée extraterritoriale, rapport à la demande du Premier ministre, avr. 2019, dit « Rapport Gauvain ».

(3) G. de Bentzmann, *Cloud Act* : halte à la désinformation !, Le Cercle des Échos, 2 oct. 2018.

(4) Le terme *Cloud computing* ou « informatique en nuage » est défini comme le « mode de traitement des données d'un client, dont l'exploitation s'effectue par l'Internet, sous la forme de services fournis par un prestataire. L'informatique en nuage est une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients ». Vocabulaire de l'informatique et de l'Internet, JO n° 0129, 6 juin 2010, p. 10453.

américaines en dehors des frontières du territoire américain, le *CLOUD Act* propose d'adopter de nouvelles procédures de coopération judiciaire internationale aux fins d'obtention de preuves informatiques qui apparaissent plus adaptées au monde numérique actuel et aux nouvelles technologies à venir.

En droit américain, le *CLOUD Act* a apporté une réponse pragmatique à la fragmentation géographique de la preuve numérique, en privilégiant le critère de l'accès aux données plutôt que celui du lieu de stockage. L'affaire *United States v. Microsoft* avait donné l'occasion à la Cour suprême américaine de se prononcer sur une problématique lourde de sens : le *Stored Communication Act* (SCA) de 1986 permettait-il aux autorités américaines de réquisitionner auprès d'un CSP les données d'une personne physique accessibles depuis les États-Unis, mais hébergées sur un serveur localisé à l'étranger, sans passer par les traités d'assistance judiciaire internationale (plus communément désignés sous l'acronyme anglo-saxon « MLAT », *Mutual Legal Assistance Treaty*) ? Pour certains, une réponse positive à cette question signifiait un « tour de passe-passe » contribuant à assoir la souveraineté – c'est-à-dire l'autorité et le pouvoir – du juge américain sur le territoire d'États étrangers [5], le *CLOUD Act* ayant d'ailleurs été promulgué en anticipation du verdict de la Cour suprême afin de devancer celle-ci par l'affirmative, sans se soucier des critiques que l'adoption de cette loi provoquerait Outre-Atlantique.

Pourtant, l'analyse des procédures françaises et britanniques en matière de perquisitions informatiques révèle que les mesures introduites par le *CLOUD Act* ne sont pas si éloignées des pratiques applicables en Europe. En France et au Royaume-Uni, l'accès aux données peut également justifier dans certains cas la saisie de preuves informatiques même si celles-ci sont stockées à l'étranger. Au-delà des considérations politiques, le *CLOUD Act* pourrait donc représenter une opportunité pour les États de revisiter leur conception de la souveraineté, traditionnellement attachée au territoire, en investissant pleinement l'espace numérique créé par Internet et en consolidant leurs procédures pénales autour des dernières évolutions informatiques, en particulier le *Cloud computing*. Les accords bilatéraux (*executive agreements*) proposés par le *CLOUD Act*, à l'instar de celui conclu pour la première fois depuis son adoption avec le Royaume-Uni en octobre 2019, renvoient à la nécessité de s'interroger sur les normes d'entraide judiciaire pénale établies en réponse au caractère toujours plus dématérialisé et transfrontalier de la criminalité. L'utilisation de la technologie a accru la rapidité et la portée extraterritoriale de certaines infractions, dont les preuves – et ce n'est pas un constat récent – se trouvent le plus souvent localisées à l'étranger et dispersées à travers plusieurs États, jusqu'à aboutir à une « déterritorialisation » [6] complète des éléments permettant de les reconstituer.

Face au développement exponentiel des outils de stockage et de traitement de données tels que le *Cloud computing* [7]

(5) G. Tissier, USA v. Microsoft : Quel impact ? Statut des données, souveraineté numérique et preuves dans les nuages, The Chertoff Group, déc. 2017.

(6) A. Kirry, F.T. Davis, A. Bisch et A.R. Gressel, L'impact du *Cloud Act* : orage ou lueur d'espoir ?, Debevoise & Plimpton, mai 2019, p. 2.

(7) Les plateformes de données proposées par les services *forensics* et permettant la revue de plusieurs milliers de documents dans le cadre, notamment, d'enquêtes internes menées par les entreprises et leurs avocats, utilisent de plus en plus la technologie *Cloud computing* afin de stocker les données confidentielles traitées dans le cadre de l'enquête.

ainsi que la *blockchain*[8] et l'intelligence artificielle,[9] ce constat n'est que susceptible de se renforcer. Il devient donc urgent pour l'UE d'élaborer des procédures ayant pour but de concilier les intérêts souverains de ses États membres comme la sécurité et l'information stratégique – éternelle source de tensions entre les États-Unis et l'Europe – avec ceux plus individuels de ses citoyens et de ses entreprises, que la lutte contre le crime permet de consolider. C'est pourquoi, après avoir exposé le caractère obsolète de la localisation des données en matière de perquisition informatique (I), l'accès à la preuve dans un nouvel « espace pénal numérique » sera envisagé, en tant que critère uniforme autorisant la saisie de données et attestant de la nécessité de réformer les dispositifs d'entraide judiciaire pénale transatlantiques afin de consacrer une souveraineté numérique européenne[10] (II).

I – La localisation des données : une manifestation obsolète de la souveraineté territoriale limitant la recherche de la preuve numérique

Le territoire est le socle historique de la souveraineté ayant engendré la création d'un espace territorial qui a permis de légitimer, à l'intérieur d'une zone géopolitique limitée, l'exercice du pouvoir répressif d'un État souverain (A). L'avènement d'Internet a bouleversé les frontières géographiques fixées artificiellement par les États, créant un « cyberespace »[11] confronté à une conception de la souveraineté nationale encore plus étendue. En matière pénale, cela signifie que les limites géographiques posées à la recherche de la preuve numérique par les États souverains sont révolues, justifiant l'abandon définitif du critère de localisation des données au sein de l'espace pénal numérique (B).

A – L'espace territorial ou la souveraineté historique légitimant l'exercice du pouvoir répressif par les États

Critère historique ayant donné naissance au principe de souveraineté des États (1), la territorialité est composée de plusieurs espaces terrestres, maritimes et aériens qui délimitent l'application de la procédure pénale de chaque État (2). C'est cette limitation territoriale de la mise en œuvre de la puissance pénale étatique qui a obligé les États souverains à coopérer et créer des instruments légitimant le recours à la force publique dans la recherche de la preuve pénale (3).

(8) La technologie *blockchain* et le dispositif d'enregistrement électronique partagé permettent notamment un échange d'information en temps réel, transparent et infalsifiable grâce à des algorithmes qui assurent une cryptographie ultra-sécurisée. Cette technologie qui est à la base de la création du Bitcoin, crypto-monnaie apparue en 2011, a connu un essor considérable pendant la pandémie du Covid-19. R. Van Hoek et M. Lacity, *How the Pandemic Is Pushing Blockchain Forward, Harvard Business Review*, 27 avr. 2020.

(9) Livre blanc de la Commission européenne, Intelligence artificielle – une approche européenne axée sur l'excellence et la confiance, COM(2020) 65 final, 19 févr. 2020.

(10) La construction du marché unique numérique européen a été l'une des priorités stratégiques de la Commission européenne présidée par Jean-Claude Juncker. Si le bilan après cinq années s'avère contrasté, la crise du Covid-19 et les mesures de relance prises conjointement par la France et l'Allemagne en mai 2020 n'ont fait que renforcer la volonté des États membres de bâtir une souveraineté européenne s'imposant dans tous les domaines stratégiques, y compris le numérique et l'action contre la criminalité transnationale. Pour une analyse du bilan sur la construction du marché unique numérique européen, v. V.-L. Benabou, L. Cytermann et C. Zolynski, Bilan de l'agenda numérique européen : quand la poussière retombe, Rev. UE 2020. 15.

(11) J.P. Barlow, Déclaration d'indépendance du Cyberespace, févr. 1996.

1 – La territorialité à l'origine du principe de souveraineté

Pierre angulaire du droit international public depuis l'avènement des traités aux XVI-XVII[e] siècles,[12] le principe de souveraineté demeure encore aujourd'hui au cœur des règles que les États se fixent afin de régir leurs rapports mutuels et l'ensemble des situations relatives au fonctionnement de leurs pouvoirs publics.[13] Ce principe fut particulièrement bien formulé par Louis le Fur en 1896 dans sa thèse de doctorat comme « la qualité de l'État de n'être obligé ou déterminé que par sa propre volonté, dans les limites du principe supérieur du droit, et conformément au but collectif qu'il est appelé à réaliser »[14], mais encore, par l'arbitre Max Huber dans la sentence arbitrale rendue dans l'affaire de l'*Ile des Palmes* en 1928 qui constatait que « la souveraineté dans les relations entre États signifie l'indépendance. L'indépendance relativement à une partie du globe est le droit d'y exercer à l'exclusion de tout autre État les fonctions étatiques ».[15]

À l'origine, le territoire est donc l'élément géographique de l'État souverain qui permet à son gouvernement d'exercer ses compétences à l'intérieur d'un espace délimité et internationalement reconnu. Le concept classique de souveraineté exprimé par Jean Bodin retient en effet l'État et ses frontières comme cadre unique d'organisation du pouvoir et d'élaboration de la norme.[16] C'est cette idée qui a donné naissance à la notion moderne d'État,[17] définie comme un groupement d'individus établi sur un territoire déterminé sous l'autorité exclusive et effective d'une puissance publique. C'est le territoire qui représente le socle historique de la souveraineté étatique permettant la production et la libre application du droit national.

2 – La création souveraine des lois pénales face à la limitation territoriale de la procédure pénale

a – Les lois pénales

Les lois pénales de fond symbolisent la manifestation la plus complète de cette souveraineté étatique en ce qu'elles participent au maintien de l'ordre public interne[18] au sein de, ou en connexion avec, un territoire géographique indépendant et consacré. Expression matérielle de la souveraineté de l'État, la territorialité – c'est-à-dire, le rattachement nécessaire à une zone géographique de nature terrestre, maritime ou aérienne – constitue le premier critère d'application des normes répressives. Il en résulte une interdiction pour les États d'intervenir afin de réprimer des faits qui relèvent de la compétence nationale exclusive d'un autre État. C'est cette interdiction qui a elle-même donné naissance à la consécration en droit international contemporain d'un principe corolaire et complémentaire de non-ingérence dans les affaires intérieures des États.[19]

(12) Notamment les Traités de Westphalie signés en 1648. T. De Montbrial, Interventions internationales, souveraineté des États et démocratie, Politique étrangère, 1998, n° 3, p. 549-566.
(13) E. David, Brèves remarques sur les origines du droit international, déc. 2012.
(14) L. Le Fur, *État fédéral et confédération d'États,* 1896, p. 443.
(15) Cour permanente d'arbitrage, affaire États-Unis c/ Pays-Bas, 4 avr. 1928, p. 7.
(16) J. Bodin, *Les six livres de la République*, Fayard, Corpus des œuvres de philosophie de langue française, 6 vol, 1576.
(17) Dans son ouvrage (*La contribution à la théorie générale de l'État*, 1921), C. De Malberg définit l'État comme une « communauté d'hommes, fixée sur un territoire propre et possédant une organisation d'où résulte pour le groupe envisagé dans ses rapports avec ses membres une puissance suprême d'action, de commandement et de coercition ».
(18) D. Rebut, *Droit pénal international*, Précis Dalloz, 3[e] éd., 2019, § 8, p. 45.
(19) Charte des Nations unies, 26 juin 1945, Chap. 1, Art. 2, § 7.

La fixation de la compétence répressive est exclusive en ce sens que les États sont libres de délimiter eux-mêmes le champ d'application de leur loi pénale dans l'espace afin de réprimer, même en dehors de leurs frontières terrestres, les atteintes à leur ordre public national. [20] C'est ainsi que la volonté de préserver l'ordre public souverain a naturellement conduit les États à admettre qu'une infraction commise en dehors du territoire souverain peut porter atteinte à leurs intérêts fondamentaux. Toutefois, l'application extraterritoriale des lois pénales d'un État n'est justifiée que par la présence d'un élément de rattachement objectif (localisation géographique) ou subjectif (citoyenneté de l'auteur ou de la victime) dont le dénominateur commun demeure le territoire souverain.

b – La procédure pénale

Si les États décident eux-mêmes de la portée extraterritoriale de leur loi pénale, la mise en œuvre de la procédure pénale a toujours été étroitement liée aux frontières souveraines de l'État pour des raisons d'ordre public international. La procédure pénale désigne l'ensemble des règles de forme qui organisent le processus de recherche des auteurs de l'infraction et de répression des infractions pénales, elles-mêmes fixées par les lois pénales de fond. [21] La distinction entre nécessaire territorialité des lois pénales de forme et libre détermination des lois pénales de fond a été consacrée par un arrêt fondateur du droit pénal international rendu dans l'affaire *Lotus* en 1927, dans laquelle la Cour permanente de justice internationale déclarait : « la limitation primordiale qu'impose le droit international à l'État est celle d'exclure – sauf l'existence d'une règle permissive contraire – tout exercice de sa puissance sur le territoire d'un autre État. Dans ce sens la juridiction est certainement territoriale ; [...] pour les autres cas, chaque État reste libre d'adopter les principes qu'il juge les meilleurs et les plus convenables ». [22]

De ce fait, le monopole de la compétence d'exécution des lois répressives de forme sur le territoire est conféré par la souveraineté de l'État sur ce territoire. En France, cette prérogative a valeur constitutionnelle depuis 1999 puisque le Conseil constitutionnel a considéré que l'accomplissement sur le territoire français d'actes d'enquêtes par une autorité étrangère portait atteinte aux conditions essentielles d'exercice de la souveraineté nationale. [23] Cette souveraineté implique également que les procédures nécessaires à la prévention des atteintes à l'ordre public soient conciliées avec l'exercice des libertés individuelles des citoyens, notamment en ce qui concerne le respect de leur vie privée. [24]

3 – L'entraide judiciaire internationale en réponse à la territorialité de la procédure pénale

En pratique, la limitation territoriale réservée aux procédures pénales n'a cessé de s'assouplir grâce à l'adoption par les États de dispositifs d'entraide judiciaire mutuelle, en même temps que la conception de la souveraineté a évolué depuis la seconde moitié du xx^{e} siècle. [25] La division de la communauté internationale en États séparés territorialement et politiquement, ainsi que la nécessité pour ces États de

(20) D. Rebut, *op.cit.,* § 1024, p. 1044.
(21) Selon Jean Larguier, la procédure pénale représente « le droit pénal en action ». J. Larguier, *La procédure pénale*, Que sais-je ?, PUF, 13^{e} éd., août 2007.
(22) CPJI aff. « Lotus », arrêt du 7 sept. 1927.
(23) Cons. const., 22 janv. 1999, décis. n^{o} 98-408.
(24) Cons. const., 2 mars 2004, décis. n^{o} 2004-492.
(25) T. De Montbrial, Interventions internationales, souveraineté des États et démocratie, *op. cit.,* p. 553.

veiller au maintien de leur souveraineté respective lors de la recherche de preuves à l'étranger, a donné lieu à la création de mécanismes interétatiques de coopération. L'entraide judiciaire pénale est née de l'évolution de la criminalité transfrontalière et de la nécessité pour les États de rechercher les preuves des violations de leurs lois pénales localisées sur le territoire d'un autre souverain. Elle permet aux États de faire accomplir sur le territoire d'un autre État des actes de procédure dirigés contre les auteurs présumés d'infractions et réputés coercitifs (extradition) ou non coercitifs (saisies, perquisitions, auditions), qu'ils estiment nécessaires au respect de leurs lois pénales.

Les MLATs ont été développés il y a une trentaine d'années en réaction à ce constat d'une criminalité transcendant les frontières territoriales et à la naissance d'une communauté d'intérêts souverains. Il s'agit généralement d'accords entre deux États (le plus connu étant le Traité entre la France et les États-Unis adopté en décembre 1998) visant à faciliter la coopération policière et judiciaire, notamment en termes d'échanges de renseignements lors d'enquêtes en cours, ou encore, par exemple, de conventions multilatérales visant à éviter l'évasion fiscale.[26] À l'origine fondés sur des rapports de concurrence et de défiance,[27] ces mécanismes fondateurs d'entraide judiciaire sont devenus inadaptés face au développement de nouveaux moyens de communication (téléphone puis Internet). L'avènement d'une société interconnectée a incité certains États à se rapprocher politiquement et même territorialement, en particulier au sein de l'UE,[28] appelant à la création de nouveaux instruments afin de lutter plus efficacement contre la criminalité transnationale. C'est le cas, par exemple, de la Convention d'entraide judiciaire du 29 mai 2000 qui régit notamment l'interception des télécommunications, ou de la Convention sur la cybercriminalité du 23 novembre 2001 adoptée en réponse à cette « révolution des technologies de l'information qui a changé radicalement la société ».[29]

Ainsi, il convient de prendre conscience au plus vite des opportunités offertes par le numérique afin de réinventer une souveraineté s'exerçant, sur le plan de la puissance publique pénale, bien au-delà des limites artificielles posées par la territorialité. Comme le souligne avec bon sens un rapport au sujet de la gouvernance d'Internet remis en avril 2019 au Gouvernement français, la technique du téléphone constituait déjà, à l'époque, « une césure entre la localisation des personnes et ce qu'elles peuvent faire entre elles. Ce que le monde digital démultipliera, le téléphone lui-même le contient : la libération du lien avec les contraintes du monde physique au bénéfice de la liberté de la personne, alors que l'État a un rapport consubstantiel à son territoire et ne peut agir qu'avec difficulté et lourdeur en dehors de celui-ci ».[30] C'est précisément de cette contrainte physique qu'il faut libérer l'État souverain à l'ère du numérique.

(26) Par ex., les conventions multilatérales pour la mise en œuvre des mesures relatives aux conventions fiscales pour prévenir l'érosion de la base d'imposition et le transfert de bénéfices élaborées par l'Organisation de coopération et de développement économiques.

(27) F.-X. Roux-Demare, Vers la suppression de l'exequatur en Europe ? Approches générales de l'exécution des décisions au niveau européen, Rev. Jur. de l'Ouest, 2012-2 p. 151-182.

(28) À travers, notamment, la création du Conseil de l'Europe en 1949, d'Europol en 1998 et d'Eurojust en 2002, ainsi que de l'Espace européen de liberté, de sécurité et de justice en 1997.

(29) Rapport explicatif de la Convention sur la cybercriminalité (dite « Convention de Budapest »), Conseil de l'Europe, série des traités européens, nº 185, 23 nov. 2001, p. 1.

(30) M.-A. Frison-Roche, L'apport du droit de la compliance à la gouvernance d'Internet, avr. 2019, p. 24.

B – L'espace pénal numérique ou la naissance d'un concept de souveraineté amplifiant les prérogatives étatiques en matière de recherche de preuve

Le développement accéléré de l'Internet et du numérique dans les années 2000, en particulier de la technologie connue sous le nom de *Cloud computing*, a bousculé l'autorité souveraine des États en créant un espace immatériel et indivis que les frontières territoriales et géopolitiques ne peuvent plus délimiter (1). Les données gravitant à l'intérieur de cet espace sont elles-mêmes des biens immatériels qui se sont détachés du monde physique grâce à leur capacité à se propager immédiatement par-delà les territoires des États.[31] Comme l'a montré l'affaire *Microsoft*, ces données se composent d'une multitude de renseignements accessibles depuis plusieurs pays qui constituent autant d'informations à caractère personnel que de preuves déterminantes à la découverte d'une infraction (2).

Le lien de rattachement de ces données à plusieurs territoires souverains, ou leur absence de rattachement à un territoire particulier, rend leur localisation multiple voire impossible à identifier lorsqu'il s'agit de les rechercher pour leur aspect probant. La limitation territoriale posée par les États dans l'application de leurs procédures pénales constitue donc un frein qui les limitent dans l'exercice de leur souveraineté au sein d'un espace pénal numérique sans frontière (3).

1 – Le *Cloud* et l'espace informatique au-delà des frontières territoriales

C'est dans un contexte de globalisation effrénée et d'innovation technologique qu'est apparu le *Cloud computing*. Comme son nom l'indique, cette technologie permet de stocker des données sur un ou des serveurs non pas de manière locale – sur un disque dur d'ordinateur ou dans un coffre-fort, par exemple – mais au sein d'un « nuage numérique » (le « *Cloud* ») souvent accessible de n'importe où et relié à des serveurs informatiques distants gérés par des CSP, grâce à l'intermédiaire d'un réseau généralement établi par des fournisseurs d'accès Internet (FAI).

L'échange des données contenues dans ce *Cloud* s'effectue presque instantanément sans pouvoir en assurer la traçabilité ou les rattacher à un espace géographique quelconque, notamment celui du propriétaire des données. La grande souplesse du *Cloud* est en effet de permettre aux données d'être placées là où le CSP ou le propriétaire des données souhaitent les placer, en se limitant à un pays (ou plusieurs), ou à un centre de données (ou plusieurs), ou même à un ensemble de serveurs dans un centre de données.

Par conséquent, l'information numérisée stockable dans un *Cloud* crée un paradigme fondamentalement nouveau s'agissant de la recherche de preuves par les États. La référence à la localisation sur le territoire souverain n'a plus de sens dans un espace numérique non défini par les frontières géographiques et géopolitiques traditionnelles. L'avènement de cette nouvelle réalité se manifeste plus particulièrement par les éléments suivants :

- la localisation des données, c'est-à-dire l'endroit où les unités d'informations « bits » qui les contiennent sont stockés électroniquement sur un support magnétique, est souvent inconnue de l'utilisateur du *Cloud* et n'a pas vraiment d'importance, les CSP stockant généralement les données auprès de *data*

(31) *Ibid.* p. 27.

centers, appelés également « fermes de données », localisées en dehors de l'État où les données sont effectivement accessibles et utilisées.

- pour réduire les coûts liés au stockage et au traitement des données, les CSP peuvent diviser dynamiquement n'importe quel élément d'information numérisé en différents fragments, qui seront stockés séparément là où le stockage est le moins cher ; un seul élément d'information (par exemple, un e-mail) peut dès lors être stocké dans l'espace souverain de différents États puis rassemblé à nouveau pour être consulté.

- les données peuvent également être stockées dans des lieux qui échappent à tout contrôle souverain, comme un satellite ou un navire en haute mer.

- à moins d'utiliser du papier ou d'autres supports physiques, les données numérisées peuvent être reproduites et copiées presque sans frais.

- les utilisateurs du *Cloud* peuvent choisir l'endroit où leurs données sont stockées et donc les placer en dehors de l'État dans lequel celui-ci ou le propriétaire des données accède et utilise l'information ; certains CSP permettent même aux utilisateurs de choisir le lieu de stockage des données, tant il est peu coûteux et simple d'un point de vue technologique d'installer un serveur dans un État étranger.

l- e chiffrement de bout en bout est le plus souvent proposé par les CSP pour que seul l'utilisateur puisse accéder aux informations contenues et échangées dans le *Cloud*.

À la lumière de ces éléments, il apparaît évident que la référence à la localisation du stockage physique des données est devenue de moins en moins pertinente dans le cadre de la recherche par les États de preuves numériques. Si les personnes peuvent encore être soumises aux lois souveraines d'un État lorsqu'elles utilisent des informations stockées sous forme numérique à des fins criminelles, les informations auxquelles elles ont accès peuvent n'avoir aucun lien physique avec cet État.

2 – L'affaire *Microsoft*

Pour autant, un État souverain, du fait du numérique, devrait-il se trouver dépossédé d'une partie de sa souveraineté au bénéfice d'utilisateurs et de CSP localisés dans un autre État ?[32] C'est de ce constat qu'est née la polémique autour de l'affaire *Microsoft*, pour laquelle le *CLOUD Act* a signé le dénouement prématuré. À l'instar d'Apple en 2015 ou de Google en 2018, la société Microsoft est devenue un des symboles de ces CSP américains, plus connus sous l'acronyme « GAFAM »[33], diabolisés en raison de leur monopole numérique mondial.

Dans cette affaire, un procureur américain avait tenté d'obtenir auprès de Microsoft en décembre 2013 le contenu de la messagerie électronique d'un utilisateur non identifié, que l'on désignera sous le nom de John Doe. Cet utilisateur avait déclaré être résident irlandais et faisait l'objet d'une enquête pénale par le parquet fédéral de New York pour des faits de trafics de stupéfiants. En vertu du SCA, législation américaine adoptée en 1986 bien avant que les e-mails ne deviennent le principal vecteur de communication, le procureur a obtenu un mandat ordonnant au CSP américain *Microsoft* de produire les e-mails de John Doe « stockés dans des locaux

(32) P.-Y. Quiviger, Une approche philosophique du concept émergent de souveraineté numérique, Les Nouveaux Cahiers du Conseil constitutionnel, 2017/4, n° 57, p. 25-28.

(33) Acronyme apparu au milieu des années 2000 d'abord sous la forme de « GAFA » et désignant les entreprises considérées comme les « géants du numérique », en particulier les entreprises américaines suivantes : Google, Apple, Facebook, Amazon et Microsoft.

appartenant à Microsoft Corporation, entretenus, contrôlés ou exploités par elle ». [34]

Afin d'obtenir ce mandat, le procureur devait présenter préalablement à un juge des documents démontrant qu'il y avait des « motifs raisonnables » (*probable cause*) de croire que John Doe avait commis une infraction et que les preuves de cette infraction étaient contenues dans les e-mails générés sous son compte Microsoft. Même si John Doe n'avait pas été informé de cette demande (pour des raisons évidentes de confidentialité de l'enquête), il aurait eu l'opportunité de contester ultérieurement la saisie de ses emails si on lui avait présenté les éléments de preuve établis par le procureur sur la base des informations recueillies. Dans le but d'obtenir ces preuves, le juge américain a appliqué une procédure qui, de fait, encadrait soigneusement l'intervention de la police fédérale américaine et semblait respecter les droits de la défense et la vie privée de John Doe. Ces procédures auraient été mises en œuvre de manière équivalente dans l'hypothèse où le procureur ou la police avaient souhaité organiser une perquisition au domicile de John Doe ou mettre sur écoute sa ligne téléphonique.

Néanmoins, refusant de se soumettre à la requête des autorités américaines, Microsoft a opposé au procureur américain sa politique interne qui l'empêchait de transmettre les données concernant John Doe car celui-ci avait prétendu résider en Irlande. Microsoft avait en effet comme politique de stocker les données contenues dans les e-mails de ses utilisateurs en Irlande, et ce même si Microsoft conservait l'accès à ces mêmes données depuis les États-Unis grâce à un système de cryptage. Dans une décision rendue le 14 juillet 2016, la cour d'appel du *second circuit* a donné raison à Microsoft, en estimant que les dispositions du SCA n'avaient pas de portée extraterritoriale et qu'un mandat délivré sur la base du SCA ne pouvait donc s'appliquer qu'aux données stockées sur le territoire américain. C'est à la suite de cette décision que le *Department of Justice* américain a saisi la Cour suprême des États-Unis, cette dernière ayant accepté en octobre 2017 de statuer sur cette affaire.

Dès lors, il est clair que le débat dans l'affaire Microsoft ne concernait pas tant le respect des libertés individuelles de John Doe et la protection de ses données à caractère personnel, que les effets de la mise en œuvre de procédures pénales d'un État sur le territoire souverain d'un autre État. Il ne semble pas déraisonnable de considérer, aux États-Unis et ailleurs, que le contrôle d'un juge indépendant et impartial sur les procédures engagées par un procureur afin de récupérer des moyens de preuve, constituent une garantie suffisante permettant la protection des droits fondamentaux de la personne. Le sujet dans cette affaire portait en réalité sur l'étendue des compétences nationales exclusives des États-Unis, les procédures pénales étant la traduction en matière répressive du principe de souveraineté des États.

L'affaire Microsoft a en effet démontré que, s'agissant de données numériques, les procédures et les traités relatifs à la saisie de preuves matérielles sont inadaptés à la recherche de preuves informatiques. Dans l'hypothèse où le procureur américain avait souhaité agir de manière coercitive à l'encontre de John Doe ou de Microsoft en ordonnant, par exemple, une perquisition à domicile ou dans les locaux de Microsoft en Irlande ou en procédant à des écoutes téléphoniques par le biais de canaux de téléphonie irlandais, il y aurait là une intrusion évidente sur le territoire souverain irlandais. Une demande d'entraide judiciaire

(34) *United States v. Microsoft*, 584 U.S. ___, 138 S. Ct. 1186 (2018): « within Microsoft's possession, custody or control ».

aurait nécessairement dû être formulée par les autorités américaines auprès de leurs homologues irlandais sur la base d'un MLAT. Or, les données stockées en Irlande et contenues dans les e-mails de John Doe étaient accessibles par Microsoft depuis le territoire américain, ce qui n'entraînait aucune action des autorités américaines sur le territoire irlandais.

En somme, le critère de la localisation des données, c'est-à-dire le lieu où celles-ci sont stockées matériellement, se révèle insuffisant en raison de la nature immatérielle des nouveaux moyens de stockage qui permettent un accès presque sans frontière à ces données. C'est d'ailleurs pour cette raison qu'aucun des nombreux avis d'*Amici curiae* émis au soutien de *Microsoft* n'offrait une solution acceptable ou utile, [35] parce que ceux-ci visaient à promouvoir une approche radicale du « tout ou rien », à savoir : les pouvoirs publics d'un État souverain devaient toujours utiliser les mécanismes d'entraide judiciaire, même s'ils avaient accès aux données sur leur territoire, ou au contraire, ils n'avaient aucun besoin d'y recourir peu importe les territoires où les données étaient accessibles.

3 – Vers l'émergence d'un espace pénal numérique

Face à ce constat, une conception repensée de la souveraineté s'impose s'agissant de l'application des procédures pénales, afin de permettre aux États de s'affranchir du carcan territorial et de continuer à encadrer la recherche de preuve dans l'espace numérique. L'espace numérique est une zone métaphysique – et non géographique ou politique – constituée essentiellement par des réseaux Internet reliés entre eux par le biais de liens intangibles créant des sphères immatérielles permettant l'hébergement et la circulation libre de données. Pour conserver la terminologie propre au droit international public et au droit pénal international, ce domaine numérique sans territoire dans lequel évoluent les données pourrait être qualifié d'« espace pénal numérique » lorsqu'il est investi par les procédures pénales nationales.

Cet espace pénal numérique, inspiré également du concept de « souveraineté numérique » apparu en 2006, [36] ne délaisserait pas la souveraineté nationale mais transcenderait les frontières étatiques en s'appréciant davantage comme un lieu d'influence d'entités souveraines, [37] et ce pour plusieurs raisons :

- Internet et les technologies de stockage en réseau de données représentent un écosystème sans frontière qui n'a été créé et n'est géré par aucun État ou autre entité supranationale, mais « par des décisions économiques prises par des entreprises qui ont développé des technologies nouvelles, permettant à des personnes d'entrer en contact sans se déplacer et sans coût ». [38]

(35) V. not. les avis suivants : Brief of International and Extraterritorial Law Scholars as *Amici Curiae* in Support of Respondent, January 18, 2018 ; Brief of *Amici Curiae* of J-P. Albrecht, S. in't Veld, V. Reding, B. Sippel and A. Voss, members of the European Parliament, in Support of Respondent, January 18, 2018 ; Brief of *Amici Curiae* of European Company Lawyers Association in Support of Respondent, January 18, 2018 ; Brief of EU Data Protection and Privacy Scholars as *Amici Curiae* in support of respondent, January 18, 2018.

(36) B. Benhamou et L. Sorbier, Souveraineté et réseaux numériques, Politique Étrangère, 2006, p. 530 ; M. Brenac, La souveraineté numérique sur les données personnelles – Étude du règlement européen n° 2016/679 sur la protection des données personnelles à l'aune du concept émergent de souveraineté numérique, Mémoire ? ?, 2017.

(37) V. Martin, La République numérique en débat au Parlement : le projet de commissariat à la souveraineté numérique, Les Nouveaux Cahiers du Droit constitutionnel, 2007/4, n° 57, p. 107-120 ; D. Danet et A. Cattaruzza (dir.), *La cyberdéfense : quel territoire, quel droit ?,* Paris : Economica, 2014, p. 286 ; F. Douzet et B. Giblin-Delvallet (dir.), *Des frontières indépassables : des frontières d'État aux frontières urbaines,* Paris, A. Collin, 2013, p. 314 ; E. Tardieu-Guigues, Internet et territoire, Revue Lamy Droit de l'immatériel, déc. 2013, n° 99, p. 59-70 ; B. Barraud, L'État territorial face au cyberespace mondial, Revue Lamy Droit de l'immatériel, janv. 2016, n° 122, p. 41-48.

(38) M.-A. Frison-Roche, L'apport du droit de la compliance à la gouvernance d'Internet, préc., p. 25.

- Les nouvelles technologies, telles que le *Cloud* ou la blockchain, vont connaître un développement sans précédent et permettent déjà à des acteurs non étatiques d'investir l'espace numérique, sans que la puissance souveraine des États ne puisse les limiter ; ces avancées allant de pair avec la naissance de nouvelles formes de cybercriminalité.

Il devient donc crucial que chaque État récupère sa souveraineté au sein de ce nouvel espace ayant été créé « sans l'État et au besoin contre l'État », [39] dans le respect du droit international et des droits fondamentaux consacrés.

S'agissant de l'application de la loi et de la procédure pénale, l'espace pénal numérique permettrait aux États d'exercer leur souveraineté nationale en matière répressive en leur attribuant des prérogatives autonomes de décision et d'action dans la couche dite « informationnelle » du cyberspace. [40] Comme expliqué dans le rapport sur la souveraineté numérique remis au Sénat en octobre 2019, le cyberespace est en effet composé de trois couches – matérielle (serveurs, routeurs, ordinateurs permettant l'interconnexion), logicielle (protocoles et logiciels permettant la communication entre machines et avec les humains) et sémantique ou informationnelle – cette dernière formant l'espace numérique avec toutes les informations qui transitent entre les deux premières couches. [41]

Par conséquent, les États doivent favoriser l'émergence d'un espace pénal numérique dans lequel ils pourront exercer efficacement, et de manière souveraine, leurs prérogatives répressives au sein de cette couche informationnelle. En d'autres termes, il ne s'agit pas pour les États de tenter de préserver leur souveraineté nationale respective « contre un numérique supra-étatique et supra-souverain », [42] mais à investir le champ du numérique de telle manière que l'équilibre entre prérogatives répressives souveraines et ordre public international soit conservé. Cette opportunité, bien qu'elle reste à l'heure actuelle difficile à conceptualiser en pratique, a déjà été illustrée ainsi par certains théoriciens du droit tels que Pierre-Yves Quiviger :

« C'est l'idée même de souveraineté qu'il faut repenser puisqu'il s'agit bien ici d'autre chose que de la manière dont la souveraineté fait face au numérique, ou lui résiste ou l'accompagne – le défi est celui de la construction d'un numérique souverain entendu non plus comme un numérique unique (en réalité américain) mais comme un univers numérique dans lequel cohabiteraient plusieurs souverains, de même que cohabitent plusieurs États sur Terre. Un État ne saurait être souverain numériquement comme il est souverain politiquement. Le défi, redoutable, à relever passe par un dialogue entre droit et informatique : les juristes vont devoir inventer une nouvelle modalité de la souveraineté, capable de s'adapter à ce que les informaticiens pourront décrire en termes de possibilité et d'impossibilité technique. » [43]

En outre, comme nous l'avons évoqué à travers nos développements précédents (v. I.A), cette révolution conceptuelle ne serait pas la première dans l'évolution du principe de souveraineté des États. La souveraineté a en effet dû « faire peau neuve » et se remodeler à plusieurs reprises au cours

(39) *Ibid.*, p. 26.
(40) Rapport fait au nom de la commission d'enquête sur la souveraineté numérique, remis à la Présidence du Sénat le 1er oct. 2019, p. 17.
(41) *Ibid.*
(42) P.-Y. Quiviger, *Une approche philosophique du concept émergent de souveraineté numérique*, préc. p. 26.
(43) *Ibid.*, p. 28.

de l'Histoire,[44] afin de s'adapter aux évolutions politiques et au constant développement de la société et de la technologie. Il s'agit en fait d'éviter que les entreprises (GAFAM, CSPs et autres FAIs) ne deviennent arbitres de l'opportunité de faire valoir les intérêts des États, tandis que ceux-ci ne seraient plus qu'exceptionnellement consultés s'agissant de l'obtention des données stockées sur leur territoire.[45]

En conclusion, la référence à la localisation des données comme critère d'application des lois et des procédures pénales en matière de perquisition numérique a perdu tout son sens.[46] Le critère de la localisation révèle plutôt « un certain malaise lié à la difficulté de s'abstraire de l'idée de territorialité ».[47] Ce constat a clairement été formulé par la Commission du Sénat sur la souveraineté numérique, ayant affirmé récemment l'absence d'utilité réelle d'une démarche focalisée sur l'obligation de localisation des données sur un territoire précis, qui « ne répondrait pas au défi posé par certaines législations à vocation extraterritoriale ».[48] Le *Cloud Act* n'est d'ailleurs pas la seule raison d'un tel changement de paradigme, le législateur européen ayant également choisi de limiter les exigences de localisation puisqu'elles sont désormais interdites « sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité ».[49]

II – L'accès aux données : un critère uniforme permettant un accès souverain à la preuve au sein de l'espace pénal numérique

Le constat est donc simple : les procédures pénales et les mécanismes d'entraide judiciaire, construits uniquement autour de la notion de souveraineté territoriale, sont devenus obsolètes en matière informatique. Dans un monde numérique radicalement immatériel, les États doivent apprendre à réinventer leurs normes pénales afin d'investir entièrement l'espace pénal numérique de leurs prérogatives publiques tout en préservant leur souveraineté ainsi que les droits fondamentaux et les libertés individuelles de leurs citoyens. Il faut donc que les États imaginent des instruments innovants répondant à l'absence de dimension physique et matériel du monde numérique, et ce afin de rétablir leur souveraineté au-delà des frontières s'agissant de la recherche de preuves informatiques.[50]

L'accès, et non plus la localisation, semble être un critère plus rationnel

(44) V. en ce sens : P.-Y. Quiviger, *op. cit.*,p. 28 ; B. Barraud, Souveraineté de l'État et puissance de l'État, Revue de la Recherche Juridique – Droit prospectif, 2017-1, nº 165, 2017 ; T. De Montbrial, Interventions internationales, souveraineté des États et démocratie, Politique étrangère, préc.

(45) B. Benhamou, Les dimensions internationales de la souveraineté numérique, Les Nouveaux Cahiers du Conseil constitutionnel, 2017/4, nº 57, p. 87-92. V. Martin, La République numérique en débat au Parlement : le projet de commissariat à la souveraineté numérique, Les Nouveaux Cahiers du Droit constitutionnel, préc.

(46) V. égal. : P. Jacob, La compétence des États à l'égard des données numériques : du nuage au brouillard… en attendant l'éclaircie ?, Rev. crit. DIP 2019. 665.

(47) F. Jault-Seseke et C. Zolynski, Le règlement 2016/679/UE relatif aux données personnelles. Aspects de droit international privé, D. 2016. 1874.

(48) Rapport fait au nom de la commission d'enquête sur la souveraineté numérique, Sénat, t. 1 : Rapport, 1er oct. 2019, p. 69.

(49) *Ibid*. Article 4 du règlement européen du 14 novembre 2018 établissant une cadre applicable au libre flux des données non personnelles dans l'Union européenne.

(50) P. Jacob, Quand les nuages ne s'arrêtent pas aux frontières – Remarques sur l'application du droit dans l'espace numérique à la lumière du *Cloud Act*, Cahiers de droit de l'entreprise, nº 4, dossier 28, juill. 2018.

et pragmatique qui répond à la nature immatérielle de la donnée : il s'agit d'un droit d'entrer, de pénétrer, une porte, une ouverture à l'espace pénal numérique et aux preuves qu'il contient (A). L'adoption de ce critère de manière unanime appelle nécessairement à réfléchir à de nouveaux dispositifs d'entraide judiciaire, dont les accords bilatéraux proposés par le *CLOUD Act* pourraient constituer une première tentative compatible avec les libertés fondamentales protégées par l'UE et la souveraineté numérique de chaque État membre (B).

A – L'accès aux données comme critère de recherche de la preuve numérique aux États-Unis et en Europe

Si le *CLOUD Act* a été décrié pour avoir consacré une première fois, plus ou moins explicitement, la notion d'accès à la preuve numérique (1), il apparaît que la procédure pénale française (2) et les dispositions introduites en droit britannique (3) ne sont pas si éloignées en pratique de l'esprit du *CLOUD Act*, y compris s'agissant de leurs effets extra-territoriaux.

1 – Le *CLOUD Act*

L'apport principal du *CLOUD Act* est de confirmer que les mandats émis en vertu du SCA s'appliquent aux données stockées à l'extérieur des États-Unis, quelle que soit la localisation de ces données tant que leur accès est possible sur le territoire américain. Bien que le *CLOUD Act* ne fasse pas explicitement référence à la possibilité de saisir des données « accessibles » depuis le territoire américain, il est clair que la notion d'accès est au cœur du dispositif américain d'obtention des preuves numériques. [51]

En effet, le *CLOUD Act* vise à amender le SCA afin de garantir aux autorités américaines la communication de données numériques ou de quelconque information détenue sous forme électronique, peu importe son lieu de stockage, dont un CSP aurait « la possession, la garde ou le contrôle » pour le compte d'un client. [52] En d'autres termes, si un CSP, considéré comme un responsable de traitement, reçoit un mandat ou une assignation valablement délivrés en vertu du SCA, il ne pourra plus faire valoir – tel que Microsoft et Google l'avaient invoqué – que les données numériques recherchées, accessibles même en partie depuis les États-Unis, [53] ne peuvent pas être délivrées aux autorités américaines au motif qu'elles sont stockées sur le territoire d'un État étranger. [54] En plus d'assurer la délivrance de ces données, le CSP doit également les préserver préalablement à toute demande éventuelle en assurant leur conservation et leur sauvegarde.

(51) *Promoting public safety, privacy and the rule of law around the world : The purpose and impact of the Cloud Act, White Paper*, Département de justice américain, avr. 2019.

(52) Amendement introduit par le *U.S. Cloud Act* au Chapitre 121, Titre 18, du *United States Code*.

(53) Les affaires *Microsoft* et *Google* sont liées en ce qu'elles concernent toutes les deux des mandats prononcés par le juge américain sur la base du SCA visant à obtenir des données à l'étranger. Toutefois, à la différence de l'affaire *Microsoft* où la Cour s'est référée au critère de la localisation des données, le juge de première instance a estimé que les données demandées auprès de Google étaient accessibles des États-Unis par l'équipe en charge du soutien dans les enquêtes juridiques et pouvaient donc être délivrées en exécution du mandat. Les deux affaires illustrent en fait parfaitement les différences entre les deux principaux types de *Cloud computing* : la décision dans *Google* concernait un *Data Shard cloud* pour lequel les données étaient divisées en petites composantes individuelles que le système propageait vers différentes localisations à travers le monde, tandis qu'il s'agissait d'un *Data Localization cloud* dans *Microsoft* qui permettait la localisation de toutes les données hors des États-Unis. Un troisième modèle de Cloud, le *Data Trust*, utilisé uniquement par Microsoft en Allemagne, permet comme le *Data Localization cloud* de stocker les données totalement à l'étranger, tout en attribuant l'accès exclusif aux mêmes données à une entité séparée, le *Data Trustee*.

(54) A. Kirry, F.T. Davis, A. Bisch et A.R. Gressel, L'impact du *Cloud Act* : orage ou lueur d'espoir ?, *op. cit.*, p. 5.

Toutefois, s'il résulte du *CLOUD Act* une application étendue des procédures pénales prévues par le SCA hors des frontières du territoire américain, ses effets extraterritoriaux sont atténués par plusieurs facteurs :

- le CSP concerné par le mandat doit être soumis à la compétence des juridictions américaines. Ce qui signifie que le CSP doit être situé sur le territoire américain ou avoir un lien dit « personnel » avec les États-Unis, notamment en étant une filiale d'une société américaine à l'étranger ou en effectuant tout ou partie de son activité sur le territoire américain.

- le procureur américain recherchant les données doit justifier d'un motif raisonnable auprès d'un juge indépendant qui, afin de délivrer le mandat en vertu du SCA, devra approuver la présence d'indices graves et concordants d'une « infraction sérieuse » (acte de terrorisme et, par exemple, tout délit financier et économique puisque le *CLOUD Act* ne donne pas de précisions sur les infractions concernées) que seul l'exécution du dit mandat permettrait de « prévenir, détecter, investiguer ou poursuivre ». [55]

- bien que le juge ne soit pas contraint de rejeter une demande de mandat qui ne préciserait pas si le propriétaire des données recherchées est américain ou a une présence suffisante aux Etats-Unis, le CLOUD Act prévoit la possibilité pour le CSP de s'opposer à la communication des données s'il a des raisons de croire que le propriétaire n'est pas américain et que le mandat crée un conflit de lois.

- s'il existe un « risque substantiel » (*material risk*) que le CSP viole une législation étrangère en transmettant les données demandées aux autorités américaines en vertu du mandat émis, une demande d'annulation du mandat peut être formulée par le CSP dans l'« intérêt de la justice » (*interests of justice*) [56] en invoquant l'absence de lien personnel avec les États-Unis ou une présence insuffisante sur le territoire américain.

Du point de vue du droit comparé, le *CLOUD Act* permet une application de la procédure pénale américaine à des acteurs situés hors du territoire des États-Unis en appliquant les critères d'application de la loi pénale dans l'espace – compétences territoriale et personnelle – en vertu du standard américain de « *personal jurisdiction* », dit « lien personnel » ou « US nexus ». Il s'agit là d'un principe hérité du droit anglais de *Common law*, qui requière une présence physique quelconque, même très furtive et sous toute forme, de la personne physique ou morale visée sur le territoire américain. [57] Ce principe a été précisé et largement étendu par les juridictions américaines en application de plusieurs législations telles que le *Foreign Corrupt Practices Act*, en exigeant uniquement un « contact minimum » avec le sol américain [58] (un e-mail envoyé via le territoire américain, par exemple).

(55) V. not. : F. T. Davis, *American Criminal Justice, An Introduction*, Cambridge University Press, juill. 2019.

(56) Afin de caractériser cet « intérêt de justice », le *CLOUD Act* rappelle les éléments du « *comity analysis* » existant en droit américain, en particulier les critères suivants : (i) les intérêts des États-Unis à obtenir l'information, (ii) les intérêts de l'État étranger à ne pas communiquer l'information, (iii) la probabilité, l'ampleur et la nature des sanctions auxquelles s'exposent les prestataires ou leurs employés, (iv) la localisation et la nationalité de la personne dont les données sont sollicitées ainsi que l'ampleur et la nature de ses liens avec les États-Unis et l'État étranger, (v) l'ampleur et la nature des liens et de la présence du prestataire avec les États-Unis, (vi) l'importance de l'information sollicitée pour les investigations, (vii) la possibilité d'obtenir l'information par des moyens qui seraient moins dommageables et, cas plus particulier, (viii) les intérêts de l'autorité d'un État tiers qui a sollicité les informations auprès des États-Unis dans le cadre de la coopération internationale en matière pénale.

(57) D.C. Andrews et J.M. Newman, *Personal jurisdiction and choice of law in the Cloud*, 73 Md. L. Rev. 313, 2013, p. 332.

(58) US Supreme Court, *International Shoe Co.*, 326 U.S. 310 (1945).

Malgré des incertitudes sur l'étendue extraterritoriale du *CLOUD Act*, [59] si l'on se réfère aux dernières jurisprudences américaines [60] celui-ci devrait résolument s'appliquer à tout opérateur américain et étranger dans les cas suivants :

- entreprise qui a une présence physique aux États-Unis par le biais de ses activités ;

- entreprise dont les activités et les services ciblent les utilisateurs américains ou étrangers aux États-Unis ;

- entreprise qui, éventuellement, n'a pas de présence aux États-Unis et dont les activités ne s'adressent pas aux utilisateurs américains, mais dont les services sont néanmoins accessibles aux utilisateurs localisés aux États-Unis.

En pratique, dans la grande majorité des cas où un CSP recevrait un mandat en vertu du SCA, il devra s'y contraindre car seule une très faible proportion de ses clients est susceptible d'être identifiée comme non-résidents américains. La personne dont les données sont demandées auprès du CSP n'aura, en vertu des lois américaines, aucun recours contre la saisie de ses données puisque le procureur aura eu à se conformer aux procédures pénales justifiant de la délivrance d'un mandat, c'est-à-dire la nécessité de démontrer l'existence d'un motif raisonnable auprès d'un juge indépendant.

Toutefois, dans les cas où le CSP serait informé que son client réside hors des États-Unis, il peut s'adresser au juge américain pour faire annuler le mandat. Le juge a alors deux options : (i) refuser d'annuler le mandat, auquel cas les données stockées à l'étranger (mais accessibles depuis les États-Unis) seront transmises au procureur américain assortie de protections juridiques équivalentes à celles applicables aux citoyens et aux résidents américains ; ou (ii) annuler le mandat et exiger du procureur qu'il procède à la saisie des données recherchées par le biais d'une demande d'entraide judiciaire en vertu d'un MLAT ou de toute autre procédure de coopération judiciaire.

Par conséquent, les procédures introduites par le *CLOUD Act* ne semblent pas être irrationnelles ou constituer une extension inappropriée de la territorialité américaine. Elles sont justifiées au contraire par une réalité qui appelle à fonder la compétence territoriale sur le lieu d'accès aux données, et non en référence au lieu de stockage de celles-ci, tout en préservant les droits des personnes assujetties.

2 – La procédure pénale française

Malgré les critiques formulées en France à l'encontre du *CLOUD Act*, [61] les règles de procédures pénales françaises en matière de perquisition et de saisie

(59) De nombreuses questions ont été posées au sujet de l'application extraterritoriale du *CLOUD Act*, notamment s'agissant des opérateurs européens ayant une « présence » sur le territoire américain ou exerçant une « activité » quelconque aux États-Unis, ainsi qu'au sujet du concept d'« entité affiliée à une entreprise américaine » mais établie en Europe.

(60) Selon l'arrêt de la Cour Suprême des Etats Unis dans l'affaire *Morrison v. National Australia Bank Ltd., 561 U.S. 247 (2010),* il y a une « forte présomption » que toute législation américaine n'est pas applicable aux actes commis hors du territoire des Etats-Unis. Dans son arrêt *United States v. Vilar,* 729 F.3d 62 (2 Cir. 2013), la Cour d'Appel fédérale à New York a décidé que cette présomption s'applique en matière pénale. V. *United States v. Hoskins*, 902 F.3d 706 (2 Cir. 2018).

(61) Comme l'énonce le rapport Gauvain, le *CLOUD Act* apparaît « comme une étape supplémentaire de l'unilatéralisme extraterritorial américain » en ce qu'« il instaure un système de collecte de données au profit des autorités américaines ans égard d'aucune sorte envers la nationalité des personnes concernées ni envers la localisation géographique des données, et ignorant totalement la souveraineté des États et l'application de leurs règles de droit ».

informatiques n'apparaissent pourtant pas si éloignées de la solution américaine privilégiant l'accès aux données. Si les articles 60-1, 77-1-1 et 93-3 du code de procédure pénale visent généralement les réquisitions d'« informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives », sans possibilité d'opposition en dehors de motifs légitimes, les dispositions relatives aux perquisitions et saisies se réfèrent explicitement aux données « accessibles ». [62] L'article 57-1 du code de procédure pénale prévoit en effet que l'officier de police judiciaire ou les agents placés sous sa responsabilité, peuvent accéder à des données intéressant l'enquête « par un système informatique implanté sur les lieux où se déroule la perquisition » et qui sont « stockées dans le dit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial ». L'article 57-1 du code de procédure pénale, qui concerne spécifiquement les enquêtes de flagrance, est également applicable aux enquêtes préliminaires par renvoi de l'article 76-3 du code de procédure pénale et en exécution de commissions rogatoires dans le contexte d'une instruction en application de l'article 97-1 du code de procédure pénale. [63]

En pratique, il s'agit donc bien « de permettre l'accès à des données distantes, se trouvant dans des locaux eux aussi distants ». [64] L'accès aux données est donc un critère déterminant en droit français, même lorsque les données qui font l'objet de la perquisition ou de la saisie sont stockées à l'étranger. L'alinéa 3 de l'article 57-1 du code de procédure pénale indique en effet que :

« S'il est préalablement avéré que ces données, accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur. »

À première vue, la lecture de cette disposition tend à considérer que toute recherche et saisie de données stockées en dehors du territoire français, bien qu'accessibles depuis la France, devra faire l'objet d'une demande d'entraide judiciaire préalable auprès de l'État concerné où sont localisées les données en question. D'autant plus que l'article 18 du code de procédure pénale fixant les contours de la compétence territoriale des officiers de police judiciaires autorise ces derniers, avec l'accord des autorités compétentes de l'État concerné, à procéder à des auditions en territoire étranger sans pour autant permettre les perquisitions ou les saisies. [65]

Pourtant, le législateur a cru bon de préciser l'article 57-1 du code de procédure pénale par une condition non négligeable, puisque le recours au MLAT ne semble envisagé que « s'il est préalablement avéré » que les données sont stockées à l'extérieur de la France. Il en résulte que le droit français reconnaît indirectement la compétence extraterritoriale des autorités de poursuite françaises et la possibilité d'appliquer la procédure pénale française sur le territoire d'un autre État souverain, [66]

(62) C. Feral-Schuhl, La collecte de la preuve numérique en matière pénale, AJ pénal 2009. 115.
(63) V. en ce sens : A. Rousselet-Magri, Les perquisitions « informatiques » à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données, RSC 2017. 659.
(64) S. Sontag-Koening, Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel, AJ pénal 2016. 238.
(65) A. Rousselet-Magri, Les perquisitions « informatiques » à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données, préc. p. 662.
(66) *Ibid,*. p. 661.

dans le cas précis où l'officier de police judiciaire n'aurait pas connaissance avant de procéder à la perquisition que les données informatiques, accessibles depuis la France, sont en fait stockées à l'étranger. Aussi, ne serait-ce pas là un encouragement à feindre « l'ignorance du caractère extraterritorial du système distant » afin d'éviter « cette lourdeur procédurale » liée à l'entraide pénale internationale ? [67]

Force est de constater que les dispositions du droit français suscitent de nombreuses interrogations qui n'ont pas encore été clarifiées par la jurisprudence et qui, en l'état, ouvrent les portes à une application extraterritoriale de la procédure pénale française bien moins jalonnée que le *CLOUD Act*. Cette interprétation extensive a notamment été dégagée par un arrêt de la Chambre criminelle de la Cour de cassation du 6 novembre 2013, dans lequel la Cour a affirmé que :

« Si, selon l'article 18, alinéa 1er, du code de procédure pénale, les officiers de police judiciaire n'ont, en principe, compétence que dans les limites territoriales où ils exercent leurs fonctions habituelles, il ne leur est pas interdit de recueillir, notamment par un moyen de communication électronique, des renseignements hors du ressort de leur circonscription, fût-ce en adressant directement une demande à une personne domiciliée à l'étranger, celle-ci restant, dans ce cas, libre de ne pas y répondre. » [68]

La lecture croisée des dispositions ci-avant exposées permet de mettre en exergue une similitude troublante avec les règles introduites par le *CLOUD Act* : les autorités françaises sont autorisées à envoyer des réquisitions à l'étranger afin d'obtenir des données électroniques, en particulier lorsqu'elles ont accès à celles-ci depuis le territoire français. En tout état de cause, il est évident que la France limiterait l'exercice de sa souveraineté au sein de l'espace pénal numérique si le législateur décidait de contenir l'application de la procédure pénale française en matière de recherche de preuves numériques à la localisation des données. Revenir à une analogie entre perquisitions de locaux « physiques » et perquisitions « informatiques » [69] représenterait un retour en arrière qui aurait pour conséquence une ignorance totale de la réalité numérique actuelle et des nouvelles formes de cybercriminalité.

3 – La loi britannique

Il serait injuste de considérer le *CLOUD Act* uniquement comme une nouvelle manifestation unilatérale de la puissance étatique américaine ou une volonté d'anticiper la décision de la Cour suprême dans l'affaire *Microsoft*. Le *CLOUD Act* a également été adopté pour pallier l'absence de réciprocité des lois américaines en matière de demande d'entraide judiciaire, afin d'apporter une réponse rapide aux demandes d'entraide pénale envoyées aux États-Unis par d'autres pays tels que le Royaume-Uni.

En effet, la rédaction antérieure du SCA ne permettait pas à des CSP soumis au droit américain de transmettre des données à un État étranger dans le cadre d'une enquête. Lors des auditions au Congrès américain en vue de l'adoption du *CLOUD Act*, les autori-

(67) D. Benichou, Cybercriminalité : jouer d'un nouvel espace sans frontière, *in* Dossier Internet : un nouvel espace de délinquance, AJ pénal 2005. 225 ; S. Sontag-Koening, Les perquisitions 2.0 : quand l'informatique se saisit de l'immatériel, préc.

(68) Crim. 6 nov. 2013, n° 12-87.130.

(69) A. Rousselet-Magri, Les perquisitions « informatiques » à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données, préc. p. 661. V. égal. : C. Gaussel et A. Oesterreicher, Les juristes d'entreprise face aux saisies en droit pénal des affaires - Aspects pratiques, Cahiers de droit de l'entreprise n° 2, mars 2020, dossier 8.

tés britanniques se sont prononcées en faveur de mesures qui assureraient la réciprocité en matière d'échange de preuves pénales informatiques avec les États-Unis :

« Cela n'a pas de sens que deux criminels complotant sur une importante affaire de drogue, un meurtre, un enlèvement, s'adonnant à du trafic d'individus ou à des abus sexuels sur un enfant au Royaume-Uni peuvent avoir leur communications interceptées s'ils communiquent par sms, mais s'ils utilisent les services d'une société américaine leurs données sont en dehors de portée des autorités de poursuite britanniques… la situation juridique actuelle est mauvaise pour l'ordre public, mauvaises pour les entreprises et mauvaise pour la vie privée. » [70]

S'inspirant du *CLOUD Act* américain, les autorités britanniques ont adopté en février 2019 le *Crime Overseas Production Orders Act* (« COPO Act ») qui apparaît encore plus agressif que le *CLOUD Act* s'agissant de la portée extraterritoriale des saisies en matière de perquisition informatique. [71] Le COPO Act impose directement à la personne physique ou morale détenant des données électroniques, dans un délai de sept jours à compter de la réception de la réquisition, de s'en dessaisir si une juridiction britannique a des motifs raisonnables de croire que cette personne a commis ou a tenté de commettre un acte criminel, notamment terroriste, et si celle-ci :

- exerce ses activités ou a son siège dans un pays ou un territoire hors du Royaume-Uni qui est partie à un accord de coopération internationale prévu entre le Royaume-Uni et le pays en question selon la procédure du COPO Act ;

- est en possession ou exerce un contrôle sur tout ou partie des données électroniques demandées et que ces données ont une valeur substantielle et/ou pertinente intéressant l'enquête pénale ;

- est en possession de données électroniques dont l'intérêt public réclame la saisie.

Bien que le COPO ne fasse pas référence au critère de l'accès mais plutôt à celui de propriétaire ou « gardien » des données (c'est-à-dire responsable de traitement, comme pour le *CLOUD Act*), la localisation n'a pas été choisie par les britanniques comme critère de rattachement. À l'instar du *CLOUD ACT*, le COPO permet aussi de conclure des accords bilatéraux de coopération avec les États étrangers afin de rendre plus efficaces l'échange de preuves numériques.

B – Une réforme des instruments d'entraide judiciaire inspirée des accords bilatéraux proposés par le *CLOUD Act*

La possibilité offerte par le *CLOUD Act* de conclure des accords bilatéraux avec les États-Unis doit être prise au sérieux, essentiellement en raison de la réciprocité dans l'échange de preuves numériques que ces accords permettent d'instaurer. Intelligemment négociés, les accords bilatéraux pourraient utilement devenir des compléments indispensables aux conventions MLAT qui les ont précédées (1). Il s'agit là d'une évolution naturelle, inhérente à la procédure pénale et à l'émergence de l'espace pénal numérique, que les États doivent capter afin d'éviter de disparaître dans un cyberespace dans lequel ils ne sont plus souverains. Pour l'UE et ses États

(70) *Deputy Assistant Attorney General Richard W. Downing delivers remarks at the Academy of European Law Conference on « Prospects for transatlantic cooperation on the transfer of electronic evidence to promote public safety »*, Londres, 5 avr. 2019.

(71) R. Junck, S. Kwok, W. Ridgway et E. Robertson, *What recent US and UK reforms to information sharing mean for cross-border investigations, Global Investigations Review*, 18 juill. 2019.

membres, un accord bilatéral avec les États-Unis devra servir les intérêts stratégiques nationaux de chaque pays et promouvoir une souveraineté numérique européenne protégeant les citoyens et les résidents européens ainsi que les entreprises implantées en Europe (2).

1 – Les accords bilatéraux comme compléments nécessaires aux MLATs

Le *CLOUD Act* propose aux États « partenaires » de conclure des accords bilatéraux avec le gouvernement américain afin d'introduire un système réciproque et plus rapide d'échange de preuves informatiques localisées dans l'espace pénal numérique. Ces accords nécessitent avant tout un niveau suffisant et réciproque de garantie des libertés individuelles et de protection des données à caractère personnel entre les États-Unis et l'État partenaire. À ce titre, le *CLOUD Act* autorise l'accès direct de l'État partenaire aux données accessibles depuis le territoire américain, en accordant à ces données la protection déjà garantie par le SCA et en supprimant les sanctions prévues contre les opérateurs américains en cas de transmission directe de preuves à l'État partenaire. Les accords bilatéraux offrent, par conséquent, à tout État partenaire la possibilité de signifier ses requêtes pour l'obtention de preuves numériques aux individus et opérateurs américains, sans utiliser la procédure MLAT et donc sans passer par l'intermédiaire du gouvernement américain.

Le Royaume-Uni a été le premier pays à signer un accord bilatéral avec les États-Unis le 3 octobre 2019,[72] alors que les négociations avec l'UE sont en cours depuis le 25 septembre 2019. L'accord américano-britannique donne un aperçu des avantages et des garanties que pourraient offrir un accord bilatéral transatlantique avec l'UE, en particulier :[73]

- le contrôle par un juge ou un magistrat de l'État requérant les preuves numériques, qui devra s'assurer que toute demande est justifiée sur la base de faits intelligibles et crédibles, en particulier s'agissant de leur fondement juridique et leur sévérité (article 5(1)) ;

- la protection des intérêts essentiels de chaque nation dans le but d'éviter, par exemple, que les données récoltées par les États-Unis auprès d'entités au Royaume-Uni ne soient utilisées par la suite afin de justifier des condamnations telles que la peine de mort (article 8(4)) ;

- l'obligation de minimiser le traitement des données sollicitées strictement aux fins de prévention, détection, enquête ou poursuite d'infractions d'une certaine gravité (article 7) ;

- l'interdiction de formuler des demandes concernant directement les résidents de l'un ou l'autre pays, y compris les nationaux vivant hors des États-Unis, sans toutefois que cette dernière restriction ne soit réciproquement applicable aux citoyens britanniques (articles 1(12) et 1 (16)) ;

- l'obtention d'une réquisition écrite établie par l'autorité désignée dans chaque pays et préalable à toute de demande de saisie (article 5(7)) ;

- la possibilité pour les individus et entités concernées par la demande de formuler une objection à la mise en œuvre de la procédure (article 5(11)).

(72) *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*, oct. 2019.

(73) J. Feigelson, K. Seeger, J. Shvets, R. Loof, R. Maddox et A. M. Moztic, *U.K. and U.S. sign landmark cross-border data sharing agreement*, FCPA Update, vol. 11, nº 3, oct. 2019.

Cela étant dit, le cryptage des données dans les *Clouds* risque de compliquer la mise en œuvre des accords bilatéraux, pour au moins deux raisons. D'une part, le cryptage de bout en bout peut fournir aux individus les moyens de dissimuler le contenu de leur communication à toute demande d'accès émanant d'un État. Or, aucune loi américaine en vigueur (en particulier ni le *CLOUD Act*, ni le SCA) n'offre au gouvernement américain de moyen juridique obligeant les CSPs à décrypter les communications ou, le cas échéant, à offrir des services qui pourraient être décryptés. La législation américaine dans ce domaine peut en pratique paraître plus protectrice des droits et des libertés individuelles que d'autres pays ne le jugeront approprié.

D'autre part, afin de protéger les données appartenant à des citoyens ou à des résidents, un pays peut décider que seul un type de *Cloud* soit autorisé – le *Data Trust* – qui consiste en une combinaison de règles de « localisation » (obligeant les CSP à stocker des données appartenant à des citoyens sur le territoire de l'État) et de dispositions de « confiance » mutuelle. Ce dispositif binaire basé sur la confiance prévoit que le contenu des communications soit stocké derrière un « mur » crypté et autorisé par l'État en question de sorte que le CSP ne puisse contrôler les « clés » du décryptage. De manière générale, cela impliquerait qu'un État qui souhaiterait avoir accès à des données appartenant à un citoyen d'un autre État adoptant ce type de procédures devrait nécessairement avoir recours à une aide bilatérale ou multilatérale. Une telle approche peut augmenter les coûts ainsi que les délais de latence et pourrait être difficile à gérer.

Pour des raisons évidentes de célérité de la justice, il apparaît donc nécessaire d'adopter de nouveaux mécanismes d'entraide judiciaire qui pourraient faciliter et accélérer l'échange de preuves informatique, en particulier dans le cadre d'enquêtes menées par les États européens. En 2018, la Commission européenne a relevé que, dans plus de la moitié de l'ensemble des enquêtes pénales diligentées par un États membre, une demande transfrontière était présentée en vue de l'obtention de preuves électroniques détenues par des prestataires de services établis dans un autre État membre ou en dehors de l'UE. [74] Par ailleurs, pour deux tiers des infractions dans le cadre desquelles les preuves électroniques sont détenues dans un autre pays, le délai nécessaire pour recueillir les preuves électroniques et la fragmentation des cadres juridiques ne permettent pas de mener des enquêtes ou des poursuites correctement. [75]

2 – Un accord bilatéral avec l'UE assurant une souveraineté numérique européenne

En Europe, les débats qui ont suivi l'adoption du *CLOUD Act* ont surtout porté sur les mandats de perquisitions adressés en vertu de celui-ci par les autorités américaines à des CSPs (tous des GAFAMs), lorsque les données de leurs clients étaient hébergées au moins en partie sur le territoire d'un État membre de l'UE. [76] Les articles 48 [77] et 49 [78] du Règlement général sur la protection des données (« RGPD ») prévoient en effet que tout transfert de

(74) Commission européenne, Union de la sécurité : la Commission facilite l'accès aux preuves électroniques, communiqué, 17 avr. 2018. V. égal., C. Feral-Schuhl, *Cyberdroit- Le droit à l'épreuve de l'Internet,* Dalloz, 8e éd., 2020-2021, § 134.22, p. 374.

(75) *Ibid.*

(76) V. T. Christakis, La communication aux autorités américaines de données sur la base du *Cloud Act* est-elle en conflit avec le règlement général sur la protection des données ?, Rev. crit. DIP 2019. 695 ; C. Thierache, RGPD vs *Cloud Act* : le nouveau cadre légal américain est-il anti-RGPD ?, Dalloz IP/IT, 2019. 367 ; A. Deroudille et F. Fatah, L'extraterritorialité du RGPD dans le contexte du « *Cloud Act* », Rev. UE 2019. 442.

(77) (78) V. notes page suivante.

données à caractère personnel hors de l'UE en réponse à une requête judiciaire ou administrative d'un État tiers n'est exécutoire que si elle est fondée sur un accord international tel qu'un MLAT. Le RGPD a été adopté en mai 2016 avec une application directe à partir de mai 2018 dans tous les États membres, c'est-à-dire deux mois seulement après la promulgation du *CLOUD Act* en mars 2018. Le RGPD a par ailleurs été suivi très rapidement d'une proposition de règlement européen relatif aux preuves électroniques (« projet *e-evidence* »),[79] dont les dispositions sont étrangement similaires au *CLOUD Act*.[80] Loin d'être un hasard de calendrier,[81] cet enchaînement normatif témoigne de l'esprit de ces lois réactives, ayant pour objectif de permettre aux États-Unis et à l'UE de renforcer leur souveraineté numérique et d'assoir leur autorité sur l'espace pénal numérique.

En conséquence, la négociation d'un accord bilatéral entre les États-Unis et l'UE régissant l'accès aux preuves numériques à des fins d'entraide pénale, de manière harmonisée au niveau des États membres européens, est indispensable pour plusieurs raisons :

fixer précisément les critères appliqués par les juges américains et européens afin d'encadrer toute demande, recherche et communication de preuves numériques entre les États-Unis et les États membres de l'UE dans le cadre d'enquêtes pénales ou administratives. En effet, il est impératif de clarifier l'incertitude autour de la mise en œuvre du *CLOUD Act* et d'encadrer les conflits de lois qui pèsent actuellement sur les opérateurs européens.[82] Sans accord bilatéral créant une synergie de moyens, les CSP hébergeant les données des entreprises et des individus basés en Europe continueront à se retrouver dans des situations dans lesquelles le respect du RGPD (dont la violation peut entraîner des sanctions importantes) mais également de la loi française dite « de blocage »,[83] pourra s'avérer difficile en raison de la pression exercée par les autorités américaines.[84]

consacrer l'accès aux données sur n'importe quel territoire d'un État membre de l'UE comme critère justifiant la possibilité pour les parquets européens de saisir des preuves numériques, même si celles-ci sont matériellement localisées aux États-Unis. C'est le cas notamment de toutes les données hébergées sur des serveurs GAFAM situés sur le territoire américain.

permettre à ce titre aux entreprises établies aux États-Unis, en particulier les responsables de traitement de données proposant des services *Cloud* à l'intérieur de l'UE (ce qui est le cas des GAFAM),[85] de communiquer des preuves numériques aux autorités de chaque

(77) Art. 48 RGPD : « Transferts ou divulgations non autorisés par le droit de l'Union – Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre ».

(78) Art. 49 RGPD qui prévoit des dérogations pour situations particulières, notamment en cas de transfert nécessaire pour des motifs importants d'intérêt public (art. 49, al. 1, (d)).

(79) Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale, COM(2018) 225 final, 17 avr. 2018.

(80) R. Bismuth, Le *Cloud Act* face au projet européen e-evidence : confrontation ou coopération ?, Rev. crit. DIP 2019. 681.

(81) P. Jacob, La compétence des États à l'égard des données numériques : du nuage au brouillard… en attendant l'éclaircie ?, préc.

(82) *Ibid.*

(83) Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, amendée le 17 juillet 1980.

(84) (85) V. notes page suivante

État membre en exécution du projet *e-evidence* et sans crainte de violer le SCA.

assurer un respect strict des droits fondamentaux et des libertés individuelles consacrés par l'UE, en négociant des garanties spécifiques de protection sur la base du RGPD, de la Convention européenne des droits de l'homme et de la Chartre de droits fondamentaux de l'UE (qui consacrent des principes tels que celui de *ne-bis in idem*, selon lequel une personne physique ou morale ne peut être poursuivie et punie deux fois pour les mêmes faits). [86] Seul un accord bilatéral pourra en effet préciser la balance à établir entre la protection de ces droits fondamentaux (base légale, proportionnalité des traitements, minimisation ciblée de l'utilisation des données) et les nécessités d'une enquête au titre de la protection de la sécurité publique des États-Unis ou d'un État européen. [87]

interdire toute restriction spéciale au profit des citoyens ou résidents américains qui ne serait pas applicables aux citoyens et résidents européens. À cet effet, il conviendrait d'encadrer la possibilité offerte aux autorités américaines de formuler des demandes concernant directement ou indirectement les citoyens, résidents et personnes morales

(84) Lors de son audition le 18 juillet 2019 par la Commission d'enquête du Sénat sur la souveraineté numérique, M. Mosse, directeur juridique et des affaires publiques de Microsoft Europe, a détaillé l'approche de Microsoft en cas de conflit : « J'en reviens à la procédure de demande de données dans le cadre du *Cloud Act*. Si le Procureur s'adresse directement à nous, pour les besoins de l'enquête, en demandant l'accès à des données précises, nous nous sommes engagés à informer notre client de cette demande, sauf dans l'hypothèse où cela nous serait expressément interdit, ce qui est prévu dans certaines conditions, elles-mêmes précisément qualifiées – risque pour l'intégrité physique ou la vie d'une personne, intérêt de l'enquête… Si nous ne pouvons informer notre client, il nous reste la possibilité de considérer que la demande n'est pas fondée, soit parce qu'elle n'est techniquement pas réaliste, soit parce que les données ne sont pas stockées chez nous, soit parce que nous considérons qu'il existe un conflit de loi entre la demande et le droit français – loi protégeant les données en application du RGPD, ou future "loi de blocage" si par exemple les préconisations du rapport Gauvain étaient retenues. Nous pourrions alors envisager deux options dans le cadre du *Cloud Act*. En l'absence d'accord négocié entre les États-Unis et l'Union européenne, comme c'est le cas actuellement, et si nous considérons qu'il existe un vrai risque de conflit de lois, nous pouvons nous y opposer devant le juge américain à travers la procédure de "*comity analysis*" – principe de courtoisie internationale en *Common Law* – par lequel le juge, pour régler un conflit de lois et mettre en œuvre le droit international, procède à la balance entre un certain nombre de critères : l'intérêt des États-Unis dans l'obtention de ces preuves, les intérêts protégés par les lois de la France, et l'existence de moyens d'obtenir autrement ces preuves dans un délai raisonnable pour le bon déroulement de l'enquête. Aujourd'hui, en l'absence d'*executive agreement* entre les États-Unis et l'Europe, si la question se posait, nous pourrions fortement envisager de nous opposer à une demande d'accès dès lors que nous serions face à un conflit de lois fort, net et précis. » Rapport fait au nom de la Commission d'enquête sur la souveraineté numérique, Sénat, t. II : Comptes rendus, 1er oct. 2019, propos par M. Mosse, Directeur juridique et des affaires publiques de Microsoft Europe, p. 322-323.

(85) Dans l'attente de la création éventuelle d'un *Cloud* souverain européen, il convient d'adopter une approche pragmatique en constatant que malgré la publicité négative atour du *CLOUD Act*, les individus et les entreprises basés en Europe continuent à confier leurs données sensibles à des GAFAM dont le monopole sera complexe à détrôner. N. Steiwer, Un *cloud* européen très allemand… et américain, Les Échos, 29 oct. 2019 ; F. Debes, Le *cloud* européen franco-allemand dévoile ses services numériques souverains, Les Échos, 3 juin 2020.

(86) *Recommendation for a Council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters*, COM(2019) 70 final, Commission européenne, 5 févr. 2019.

(87) Rapport fait au nom de la Commission d'enquête sur la souveraineté numérique, Sénat, t. II : Comptes rendus, 1er oct. 2019, propos par M. Mosse, Directeur juridique et des affaires publiques de Microsoft Europe, p. 323. Par ailleurs, la Cour de justice de l'Union européenne (CJUE) a récemment jugé, s'agissant de l'interprétation de la 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, que « la réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause. À cet égard, un tel accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction. Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités. » (CJUE 2 mars 2021,aff. C-746/18).

établis dans un des États membres de l'UE (y compris les nationaux vivant hors UE), [88] et permettre aux individus et entités concernés de formuler des objections argumentées à la mise en œuvre du mandat de perquisition. Cette limitation permettrait d'encourager les autorités américaines et européennes à poursuivre activement leurs citoyens et leurs entreprises en vertu des principes de compétence personnelle active et passive.

contribuer à préserver les données informatiques considérées comme stratégiques par l'UE et chacun de ses États membres, [89] en précisant les informations considérées comme relatives à la souveraineté économique, industrielle, financière, commerciale ou technique de l'UE, ou toutes les données couvertes par le secret des affaires. [90] Ces informations stratégiques devront faire l'objet d'une évaluation préalable à la saisie et une ordonnance de refus de communication pourra être délivrée par un juge de l'État où se trouve l'opérateur ayant reçu le mandat de perquisition, en particulier dans le cas où certaines des données demandées n'auraient aucun lien avec une infraction potentielle.

définir les infractions qui nécessitent le recours à une entraide judicaire accélérée hors procédures MLAT, notamment le terrorisme et son financement, toutes les formes de cybercriminalité, la corruption, le blanchiment de capitaux, les fraudes à caractère transnational et les délits d'initié. Cela implique que certaines règles soient respectées avant toute communication de preuves, en particulier l'obligation d'une requête écrite et détaillée ainsi que le contrôle d'un juge indépendant confirmant le fondement juridique et la nécessité impérieuse d'une telle requête. [91]

Le démarrage des activités du Parquet européen à partir de novembre 2020, destiné à agir rapidement dans des affaires économiques et financières relatives aux intérêts de l'UE, ne fait que confirmer le besoin d'un accord bilatéral et la légitimité de l'UE à affirmer sa souveraineté au sein de l'espace pénal numérique face aux États-Unis. Le règlement du 12 octobre 2017 a en effet attribué comme compétence matérielle au Parquet européen les « infractions portant atteinte aux intérêts financiers de l'Union », [92] initialement la fraude mais également la corruption et le blanchiment de capitaux. [93] Bien que toute extension des compétences du Parquet européen à la lutte contre la criminalité ayant une dimension transfrontière requiert une décision complémentaire adoptée à l'unanimité par le Conseil européen, des extensions de son mandat

(88) Et ce bien que cette hypothèse soit peu probable en pratique. E. Mignon, Le *Cloud Act* ou l'impuissance européenne démasquée, Revues des juristes de Sciences Po, nº 16, janv. 2019.

(89) Les droits nationaux des États membres pouvant s'avérer insuffisant et inadapté au risque nouveau qui se développe, en particulier l'adoption toujours plus étendu de certaines nouvelles technologies. C. Ingrain et X. Philipps, Il est urgent de protéger les informations stratégiques des entreprises, Dalloz actualités, 16 mars 2018.

(90) Dir. (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites ; Loi nº 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires. V. égal. : S. Schiller, R. Amaro, T. D'ales, R. Laher, J-Y. Trochon, F. Audran, G. Cauvin, V. Chapuis-Thuault, O. Sicsic, P. De Robert Hautequere, N. Dostert, M. Gras et S. Van Kemmel, Le secret des affaires, Actes pratiques et ingénierie sociétaire, nº 1, dossier 1, janv. 2020.

(91) Une telle mesure permettrait d'éviter que les autorités américaines n'envoient des demandes de MLATs qui pourraient être considérées comme non-justifiées et dépourvues de bases légales ou factuelles, comme cela a été récemment mis en lumière par un ancien procureur fédéral des États-Unis dans le cadre d'une enquête pour fraude. V. *Motion for leave to intervene to address the Governement response to the defendant's motion to compel, USA v. James Vorley and Cedric Chanu*, US Northern District Court of Illinois, Eastern Division, 31 mars 2020.

(92) Règl. (UE) 2017/1939 du Conseil du 12 oct. 2017 mettant en œuvre une coopération renforcée concernant la création du Parquet européen.

(93) Dir. (UE) 2017/1371 du Parlement européen et du Conseil du 5 juill. 2017 relative à la lutte contre la fraude portant atteinte aux intérêts financiers de l'Union au moyen du droit pénal.

sont déjà envisagées à d'autres catégories d'infractions de nature transnationale (notamment le terrorisme, la criminalité informatique et la criminalité organisée). [94]

La souveraineté sur l'espace pénal numérique doit nécessairement être européenne pour s'inscrire dans la durée au-delà des frontières et en pivot à l'autorité créée par l'hégémonie américaine. [95] À cet égard, l'idée avancée par certains, de faire coïncider les territoires étatiques avec les sphères technologiques pour défendre la souveraineté de la France apparaît désuète et dénuée de sens pratique. [96] L'urgente nécessité d'adopter une nouvelle génération de MLATs et de conclure un accord bilatéral transatlantique porteur des droits fondamentaux protégés par l'UE a d'ailleurs été prônée par le Comité et le Contrôleur européens de la protection des données. [97] C'est l'UE qui doit avoir l'autorité nécessaire pour assurer à ses États membres des instruments permettant d'investir l'espace pénal numérique afin de lutter efficacement contre les nouvelles formes de criminalité transnationale, tout en offrant une protection renforcée des libertés fondamentales individuelles et des intérêts stratégiques nationaux et européens.

(94) H. Christodoulou, La protection extensible des intérêts financiers de l'Union européenne par le parquet européen, Lexbase pénal, nº 27, 28 mai 2020.
(95) B. Benhamou, Les dimensions internationales de la souveraineté numérique, préc., p. 92.
(96) O. De Maison Rouge, *Cloud Act* et collecte de preuves numériques à l'étranger : la souveraineté judiciaire en balance, AJ pénal 2019. 591.
(97) *Response to LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection*, 10 juill. 2019.