CLOUD Act : vers un changement de paradigme pour la détermination de la souveraineté sur le champ numérique ?

Par Sara Benhadji, alumni d'IRIS Sup' en Géoéconomie, gestion des risques et responsabilité de l'entreprise, et de Grenoble École de management

« Développer un cloud français fait avec des logiciels libres », *« sortir des dépendances extérieures »*[1]… les propositions politiques prônant une souveraineté des données se multiplient en France et en Europe, illustrant une volonté forte : la réappropriation par la puissance publique d'un champ numérique aux contours incertains. Les États s'étant historiquement construits sur le principe de territorialité, leur autorité légitime s'exerce dès lors dans un périmètre géographique déterminé.

Dans cette perspective, le CLOUD Act (texte adopté par les États-Unis en 2018 autorisant, dans le cadre d'une enquête judiciaire, les autorités américaines à demander la production de données situées en dehors de leur territoire) touche deux points sensibles. D'une part, son caractère extraterritorial remet en question l'idée d'une souveraineté numérique fondée sur le principe de territorialité. D'autre part, il s'intéresse aux données dans le cloud, largement dominé par des fournisseurs américains, et met ainsi en exergue une forme de dépendance technologique européenne.

Au-delà des critiques et craintes qu'il suscite, il sera également intéressant d'étudier les changements de paradigme initiés par le CLOUD Act, dans un contexte de lutte contre la criminalité transfrontalière. Le texte questionne en effet la pertinence d'une souveraineté des données dans le cloud fondé sur leur localisation et propose de donner un plus grand rôle aux fournisseurs pour l'accès aux preuves électroniques.

1) Le cloud comme objet de souveraineté numérique

La souveraineté trouve ses fondements dans le principe de territorialité, qui légitime l'autorité d'un État sur un espace déterminé. Même sur le champ des réseaux, qui sont par nature sans frontières, le territoire occupe une place centrale dans la représentation de la souveraineté. Les stratégies étatiques pour favoriser l'implantation de centres de données sur leur territoire, ou faciliter l'émergence de champions nationaux du numérique en sont une illustration. Derrière l'apparente immatérialité des réseaux se trouvent donc en réalité des actifs physiques (tels que les centres de données, ordinateurs, serveurs, câbles), conférant un ancrage territorial aux technologies. De ce fait, les sociétés portant ces technologies doivent obéir aux lois édictées par des États, applicables selon divers critères (nationalité, localisation…).

Utilisé la première fois en France par Laurent Sorbier et Bernard Benhamou en 2006[2], le terme de souveraineté numérique a connu un regain d'intérêt après les révélations d'Edward Snowden, qui ont joué un effet catalyseur dans la prise de conscience de la dépendance européenne aux firmes américaines, et des liens que celles-ci entretiennent parfois avec la Maison-Blanche. L'importance prise par ce concept dans le discours politique français et

[1] Piquard, A. "Souveraineté numérique : les candidats à la présidentielle critiquent la politique d'Emmanuel Macron », *Le Monde*, [consulté 15 février 2022], disponible sur https://www.lemonde.fr/economie/article/2022/02/07/souverainete-numerique-les-candidats-a-la-presidentielle-critiquent-la-politique-d-emmanuel-macron_6112643_3234.html

[2] Benhamou, B., & Sorbier, L. (2006). Souveraineté et réseaux numériques. *Politique étrangère*, (3), 519-530.

européen ces dernières années marque l'intention de se réapproprier un espace aux contours fragiles et développer une industrie du numérique compétitive.

La conception européenne de la souveraineté numérique se traduit ainsi de deux façons : d'une part réguler des acteurs étrangers aux positions de plus en plus systémiques, et dont les pouvoirs entrent en concurrence avec les prérogatives étatiques, et de l'autre, favoriser le développement d'acteurs nationaux en mesure de rivaliser avec ces géants du numérique. Partant du principe que le cyberespace ne serait pas un lieu si distinct de l'espace physique habituel, l'Europe en calque ainsi la maitrise sur un modèle connu : le principe de territorialité. Et elle appréhende la question des réseaux à travers des éléments tangibles : les technologies et infrastructures sous-tendant le cyberespace.

Les rapports de force étatiques sont particulièrement visibles au travers des flux de données, qui sont la matière première de toute technologie structurante. De fait, la souveraineté numérique implique une maîtrise des données. Le besoin croissant de capacités pour leur stockage a démocratisé l'utilisation du cloud, qui cristallise désormais les débats autour de la souveraineté numérique. En France par exemple, le cloud ne s'appréhende plus uniquement sous le prisme de la compétitivité, mais bien sous celui de la sécurité publique et de la souveraineté[3] comme en témoigne le développement d'offres de *« cloud souverain ».*

L'importance prise par le cloud, tant dans les sphères publiques que privées en fait donc un objet de pouvoir et de rivalités où le contrôle des données sert l'exercice de sa puissance. C'est sur cette toile de fond que le CLOUD Act a été promulgué.

2) Que prévoit le CLOUD Act ?

Le CLOUD Act contient deux principales provisions :

- La première, à portée extraterritoriale, prévoit l'accès des autorités américaines aux données sous la *« possession, garde ou contrôle »*[4] de fournisseurs de services de communication soumis à la juridiction américaine, et ce, peu importe le lieu de stockage des dites données.
- La seconde[5] permet au gouvernement américain de signer des accords bilatéraux – nommés *executive agreements* – avec des gouvernements étrangers. Cet accord autorise les deux pays à adresser leurs requêtes de données directement auprès des fournisseurs de services de communication en cas d'enquêtes portant sur des *« crimes graves »*.

Le texte soulève néanmoins plusieurs questions d'interprétation juridique. La première d'entre elles est la notion de *« possession, garde ou contrôle »*, utilisée depuis des décennies dans les litiges pénaux et civils aux États-Unis, avec des interprétations judiciaires variant d'une affaire à l'autre. Il n'est donc pas possible de prévoir avec certitude comment les tribunaux interpréteront ces termes[6].

[3] Douzet, F. (2020). Éditorial. Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique. *Herodote*, (2), 3-15, p.11.
[4] 18 U.S. Code § 2713
[5] 18 U.S. Code § 2523.
[6] Hemmings, J., Srinivasan, S., & Swire, P. (2019). Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act. *J. Nat'l Sec. L. & Pol'y*, *10*, 631.

D'après une étude[7] menée par le *Cross Border Data Forum*[8] à partir de la jurisprudence des *Federal Rules of Civil and Criminal Procedure*, la notion de *« contrôle »* est la plus incertaine. Trois questions permettraient à un tribunal de qualifier le *« contrôle »* : 1) l'entreprise a-t-elle un droit légal sur les données ? 2) l'entreprise est-elle en capacité opérationnelle d'accéder aux données ? 3) l'entreprise est-elle partie prenante ou un tiers de l'affaire ? Plus les degrés de contrôle légal et de contrôle quotidien sont élevés, plus il est probable qu'une cour américaine établisse le *« contrôle »* de l'entreprise sur les données.

Cas n°1
Prenons l'exemple d'une société mère basée aux États-Unis, qui détiendrait 100% du capital de sa filiale britannique. Même si la filiale est une entité juridique distincte de la société mère, il est fort probable qu'un tribunal établisse le *« contrôle »* de la société mère sur les données de la filiale. Une participation entre 25 et 100% serait en effet suffisante pour légitimer un contrôle légal des données.

Cas n°2
Imaginons maintenant qu'une société américaine agisse en tant que prestataire de services pour une société britannique. Si la société américaine reçoit, manipule et traite régulièrement des données de la société britannique, alors une cour pourrait tout à fait établir la notion de *« contrôle »*. Bien que la société américaine ne dispose pas d'un contrôle légal des données, il existe un lien fort entre les deux sociétés dans le cours des affaires. La force et la fréquence de ce contrôle quotidien sur les données pourraient donc suffire à établir la notion de *« contrôle »* telle qu'énoncée dans le CLOUD Act.

Ainsi, même si le degré de contrôle légal est faible, un fort degré de contrôle quotidien permettrait d'établir la notion de *« contrôle »,* et vice versa.

La notion de *« crime grave »* interroge également. Ne trouvant pas de définition dans le CLOUD Act, ce concept doit être précisé lors des négociations d'un *executive agreement.* À titre d'exemple, l'accord signé entre les États-Unis et le Royaume-Uni retient toute conduite s'apparentant à un crime grave dans le droit de la partie émettrice ainsi que toute *« offence that is punishable by a maximum term of imprisonment of at least three years »*[9]*.* Cette définition, très large, ne permet pas d'identifier avec certitude les conduites comprises dans le champ d'application du texte. Par ailleurs, seule la partie du CLOUD Act consacrée aux accords bilatéraux introduit la notion de *« crimes graves »*. Ce n'est pas le cas de la première partie du texte, qui pourrait s'appliquer à d'autres régimes de répression.

Les incertitudes juridiques autour du texte alimentent ainsi un sentiment de défiance et font craindre une incursion des États-Unis dans la souveraineté numérique européenne.

3) Au cœur des tensions : respect de la vie privée et protection des informations économiques sensibles

La conception américaine de sa compétence personnelle permet au DOJ de cibler des données situées en Europe, et donc potentiellement soumises à l'application du Règlement

[7] Ibidem
[8] Organisation à but non lucratif travaillant sur les politiques de transferts transfrontaliers de données. Étude disponible sur : https://www.crossborderdataforum.org/the-legal-nature-of-the-uk-us-cloud-agreement/
[9] "Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime", 3 octobre 2019, USA No.6.

général sur la Protection des Données (RGPD). Les requêtes étant directement adressées aux hébergeurs, les États membres n'ont pas de droit de regard sur celles-ci, ce qui alimente un sentiment de défiance. Dans un contexte concurrentiel accru, le texte est aussi parfois envisagé comme un outil de collecte d'informations stratégiques sur des entreprises européennes – et ce d'autant plus que les lois de blocage sont dans les faits peu créditées[10].

L'importance accordée à la protection de la vie privée, la volonté de créer des acteurs forts du numérique, mais également l'expérience de certains abus comme l'affaire Snowden font donc craindre un détournement du texte sous couvert d'une enquête judiciaire.

Toutefois, un certain nombre de spécificités liées au droit américain permettent de nuancer ces préoccupations.

Justin Hemmings et Nathan Swire[11] ont fait remarquer qu'il existe un certain nombre de garanties procédurales, juridiques et politiques qui cadrent la protection des secrets commerciaux aux États-Unis. Ainsi, si un procureur, dans le cadre d'une enquête, souhaitait partager des informations obtenues avec des entreprises privées américaines, il lui faudrait les divulguer avant le dépôt d'un acte d'accusation. Ce comportement constituerait une entorse grave à l'éthique. De plus, les informations susceptibles de former un secret commercial sont classifiées et leur partage relève d'une violation du droit pénal. Les deux auteurs soulignent également, à juste titre, que l'application du CLOUD Act requiert l'aval d'un juge indépendant, entrave supplémentaire au détournement de cette loi. Ces obstacles procéduraux induisent en outre des limites pratiques : le respect des délais fixés par la loi pourrait rapidement rendre les informations récoltées obsolètes une fois les données déclassifiées ou l'enquête terminée. Ainsi, le recours au CLOUD Act comme outil d'intelligence économique serait bien peu efficace, eu égard aux limitations juridiques et procédurales rencontrées.

Concernant une éventuelle collecte massive de données personnelles par le CLOUD Act, rappelons que les autorités américaines doivent fournir un mandat spécifique et s'intéressent donc à des données ciblées avec précision dans le cadre d'une enquête judiciaire[12].

Le peu de recul et le manque de jurisprudence complexifient l'appréhension de ce texte et nourrissent les spéculations autour du CLOUD Act.
Bien que les procédures cadrant l'application du CLOUD Act compliquent fortement un usage détourné du texte, elles ne rendent pas la divulgation de données totalement impossible. Aussi, dès la promulgation du CLOUD Act, la Commission européenne a rapidement fait part de son souhait de négocier un accord commun avec les États-Unis, afin d'encadrer les modalités de partage de données. Un *executive agreement* est donc en cours de négociation. Peut-on espérer une réciprocité dans cet accord ? Et en cas d'aboutissement favorable des négociations, les critiques à l'égard du CLOUD Act deviendraient-elles désuètes ?

4) Le cas des accords britannique et australien

[10] Par exemple, la loi de blocage française de 1968, qui n'a donné lieu qu'à une seule condamnation entre 1980 et 2020, ne représente pas un risque de sanctions avérées selon les autorités américaines.
[11] Hemmings Justin, Swire Nathan, "The Cloud Act is not a tool for theft of trade secrets", *Lawfare*, 23 avril 2019 [consulté le 15 mai 2021], disponible sur https://www.lawfareblog.com/cloud-act-not-tool-theft-trade-secrets
[12] Sur ce point, on pourra s'intéresser aux décisions liées au *Health Data Hub*, qui offrent un exemple concret des limites d'accès des autorités américaines à des données hébergées par un fournisseur soumis à la juridiction américaine.

À ce jour, deux *executive agreements* ont été signés : l'un avec le Royaume-Uni en 2019, et l'autre avec l'Australie en 2021[13]. Aussi l'échantillon est-il trop réduit pour en inférer des tendances générales et anticiper la teneur d'un *executive agreement* avec l'Europe.

On peut cependant noter plusieurs asymétries d'exigences dans l'accord signé avec le Royaume-Uni. Le texte contient notamment des restrictions de ciblage et des dispositions de minimisation inégales en fonction de critères tels que la nationalité et le lieu de résidence. Par exemple, en cas de requête britannique auprès d'un fournisseur basé aux États-Unis, le Royaume-Uni n'est pas autorisé à cibler les données d'une « *U.S person »*[14]. En revanche la réciproque n'est pas vraie.
L'accord australien, moins inégal, veille à instaurer un certain niveau de réciprocité pour l'acquisition, la conservation et la diffusion d'informations liées à des *« Australian persons »* [15]*.*
Ce terme ne recouvre cependant pas tout à fait le même périmètre que les *« US persons ».*
La conclusion d'un accord avec l'UE pourrait donc se voir freiner par ce type d'asymétries dans les provisions.

Un autre point important qu'il convient de souligner est que la signature d'un *executive agreement* ne prévient pas obligatoirement contre une utilisation unilatérale d'une provision du texte par les États-Unis. Les accords signés avec le Royaume-Uni et l'Australie spécifient que les procédures convenues ne sauraient être exclusives. Les États-Unis se réservent donc le droit de contourner certaines limitations prévues par l'*executive agreement*.
Dans ce contexte, quel est donc l'intérêt pour un État de conclure un *executive agreement* avec les États-Unis ? Interrogé au sujet de l'accord signé avec le Royaume-Uni lors d'une conférence publique[16] le DOJ a plaidé que les autorités britanniques étaient désormais en mesure d'accéder à des données de contenu hébergées par des fournisseurs américains. La signature d'un accord entre les États-Unis et l'Europe ne mettra donc pas nécessairement de point final au débat sur le CLOUD Act en Europe.

Ainsi, en supposant que les États-Unis et l'UE parviennent à un accord réciproque, il est peu probable que celui-ci mette un terme au débat sur le CLOUD Act en Europe. Si le texte est critiquable à de nombreux égards, il convient toutefois de prêter attention aux mutations dont il est le symptôme. En particulier : la nécessité croissante de partage de preuves transfrontières pour la résolution d'enquêtes pénales. Le CLOUD Act se veut l'instrument d'une simplification des méthodes de coopération judiciaire.

5) Aux origines du CLOUD Act : la difficulté d'accès aux preuves électroniques

Si le caractère unilatéral et extraterritorial du CLOUD Act suscite des critiques, le texte a néanmoins le mérite de poser la question de l'efficacité de l'accès aux preuves électroniques pour la résolution d'enquêtes transfrontières.
Le texte s'inscrit en effet dans un contexte d'essoufflement des traités d'entraide judiciaire (MLAT – *mutual legal assistance treaties*), qui sont la solution la plus couramment utilisée pour le partage de preuves d'un État à l'autre.

---

[13] Les accords sont consultables ici : Cloud Act Resources (justice.gov)
[14] Tout citoyen ou ressortissant des États-Unis. Mais aussi tout étranger légalement admis à la résidence permanente, toute association non constituée en société dont un nombre important de membres sont des citoyens américains ou des étrangers légalement admis à la résidence permanente, et toute société constituée aux États-Unis.
[15] Cette notion exclut les ressortissants australiens et les étrangers légalement admis à la résidence permanente.
[16] Christakis, T. (2019). 21 Thoughts and Questions about the UK/US CLOUD Act Agreement:(and an Explanation of How it Works–With Charts). *European Law Blog, October*.

Imaginons qu'un État souhaite obtenir des données hébergées par un fournisseur localisé aux États-Unis. Il envoie une demande au *Department of Justice* (DOJ). S'ensuivent alors de nombreuses étapes devant sécuriser la procédure et éviter que des juridictions tierces n'adressent des requêtes illégales aux hébergeurs. La demande est ainsi examinée par le bureau du procureur, qui doit obtenir un mandat de justice avant de la transmettre à l'hébergeur. Si ce dernier accepte de produire les données demandées, le DOJ procède alors à leur analyse avant transmission à l'État requérant[17].

Les critiques à l'égard des MLAT sont doubles. D'une part, des mois voire des années peuvent s'écouler avant que la procédure n'aboutisse, laissant le temps aux accusés de supprimer ou déplacer les preuves. D'autre part, l'augmentation du nombre d'enquêtes requérant l'accès à des preuves électroniques exerce une pression sur les services de justice américains. Les États-Unis concentrant une grande partie des centres de données sur leur territoire, ils sont de fait impliqués dans la plupart des procédures de divulgation de données et doivent supporter à leur charge l'augmentation de capital humain et financier liée à la hausse des demandes sous MLAT. Selon le DOJ[18], les États-Unis auraient donc adopté le CLOUD Act pour pallier ces problèmes d'efficacité.

Jusqu'ici, les MLAT ont donc représenté le meilleur outil pour faciliter la collecte de données tout en respectant la compétence territoriale de chacun. Mais dans un contexte de numérisation des preuves, ces procédures se heurtent aujourd'hui à des limites. Aussi, les MLAT considèrent le lieu de localisation des données comme critère d'identification de la juridiction compétente.

6) Le lieu de localisation des données, un critère contestable

Dans les modèles de coopération judiciaire actuels (les MLAT), c'est le lieu de localisation des données qui permet d'identifier la juridiction compétente, critère d'autant plus évident qu'il puise ses sources dans le principe de territorialité. Dès lors, l'État souverain sur le territoire où sont localisés les centres de stockage de données peut y appliquer sa juridiction.

On peut toutefois contester la pertinence de ce critère. Dans les faits, les gouvernements ne savent pas toujours où le contenu recherché est localisé, avant tout parce que les hébergeurs stockent les données de leurs utilisateurs dans des centres aux géolocalisations diverses, le plus souvent en fonction de considérations techniques ou économiques.

Mais surtout, il est rare que toutes les données d'un même utilisateur soient stockées au même endroit et qu'elles y restent. Elles sont fragmentées et réparties parfois arbitrairement[19]. Dans le cadre d'enquêtes pénales, les autorités américaines ont rapporté des cas où les courriels d'utilisateurs américains se trouvaient sur des serveurs aux États-Unis, tandis que les pièces jointes associées étaient stockées à l'étranger[20].

---

[17] Barnett, S. & Hohmann, M., "Improving Cross-Border Access to Electronic Evidence", *Global Public Policy Institute,* 21 janvier 2019, [consulté 31 décembre 2020], disponible sur https://www.gppi.net/2019/01/21/system-upgrade

[18] Livre blanc "*Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act"*

[19] Bismuth, R. (2019). Le Cloud Act face au projet européen e-evidence: confrontation ou coopération?. *Revue critique de droit international prive*, (3), 681-694, p.683.

[20] Ibidem

Les déplacements réguliers de données par les hébergeurs et la part d'aléatoire dans ces flux en complexifient le traçage. Ainsi, il peut arriver qu'un gouvernement effectue une requête auprès des États-Unis, pour finalement activer un traité d'entraide judiciaire avec un autre pays. En effet, il faut d'abord solliciter la coopération américaine pour déterminer le lieu de localisation des données visées, puis engager un processus d'entraide judiciaire avec le pays en question dans un second temps seulement. Ceci a pour effet d'accroître un peu plus la charge de travail des services de justice américains, parfois sollicités alors que la requête ne les concerne pas directement.
À cette complexité s'ajoute une inégalité géographique ; toutes les nations ne disposant pas des mêmes ressources pour attirer les centres de données sur leur territoire. À titre d'exemple, la France propose (sous certaines conditions) un abattement fiscal sur l'un des plus grands coûts d'exploitation des centres de données : l'électricité consommée[21]. Tandis que les États-Unis concentrent 38% des capacités d'hébergement mondiales[22] sur leur territoire. À l'inverse, certains pays, en Afrique notamment, ne comptent que très peu, voire pas du tout de centres de données.
En déterminant la compétence à partir de la localisation géographique des données, on désavantage de fait les pays aux capacités d'hébergement réduites. Dès lors, comment s'assurer que cette fracture numérique ne se traduise pas en une fracture juridique[23] et garantir à chaque État un exercice équitable de sa souveraineté ?

La véritable question derrière le CLOUD Act est donc celle de l'avenir des MLAT et de la résolution des conflits de juridiction sur le champ numérique. Le texte remet en perspective le principe d'une souveraineté dans le cloud fondé sur la localisation des données, et nous invite à repenser la question de l'accès aux preuves électroniques.
À travers son projet E-evidence, l'UE ouvre également la voie à un dialogue direct entre État requérant et fournisseur hébergeant la donnée ciblée.

7) CLOUD Act et E-evidence : vers un changement de paradigme pour l'accès aux preuves électroniques ?

De son côté, l'UE a également présenté un projet de règlement pour l'accès transfrontalier aux preuves électroniques. Comme le DOJ, la Commission a mis en avant la longueur des délais pour accéder aux informations via les voies d'entraide judiciaire.

Aussi, si le CLOUD Act est parfois décrié en Europe, le projet E-evidence repose sur des mécanismes similaires. Des données hébergées à l'étranger peuvent théoriquement être la cible de demandes gouvernementales européennes puisque tout fournisseur proposant des services dans l'Union doit être soumis au texte. Le texte recrée un lien de rattachement territorial en imposant aux prestataires étrangers de désigner un représentant légal européen vers lequel les demandes seront dirigées[24].

CLOUD Act et projet E-evidence sont donc deux réponses unilatérales à une même problématique : celle de l'essoufflement des voies de coopération traditionnelles.

---

[21] Bastien, L, « Data Centers : La taxe sur l'électricité consommée réduite de moitié », Le Big Data, 24 septembre 2018, [consulté le 11 novembre 2020], disponible sur https://www.lebigdata.fr/data-centers-taxe-electricite-reduite
[22] « Colocation Data Centers », *Data Center Map*, [consulté 30 décembre 2020], disponible sur https://www.datacentermap.com/datacenters.html
[23] Bismuth. Le Cloud Act face au projet européen e-evidence. *Op.cit.,* p.684.
[24] Bismuth, R, « L'extraterritorialité du Cloud Act à la lumière du projet européen E-evidence », *Journal du Net*, 25 juillet 2018, [consulté le 15 mars 2021], disponible sur https://www.journaldunet.com/solutions/cloud-computing/1210752-l-extraterritorialite-du-cloud-act-a-la-lumiere-du-projet-europeen-e-evidence/

Il est intéressant de noter qu'aucun des deux textes ne s'affaire à améliorer la procédure des MLAT. Au contraire, ils s'appliquent à fournir un cadre pour l'accès direct des autorités publiques aux données hébergées par les fournisseurs, suggérant ainsi que l'approche retenue par les MLAT serait dépassée.

Dans une demande sous CLOUD Act, la personne dont les données sont visées n'est pas toujours notifiée d'une procédure la concernant. Aussi, le texte ne prévoit pas de possibilité de recours citoyen, seuls les fournisseurs sont habilités à contester une demande. Cette compétence les place donc de fait en garde-fous du respect des droits de leurs utilisateurs.
Sur ce point, rappelons que les fournisseurs communiquent largement sur les mesures juridiques, techniques et organisationnelles mises en place pour le respect de la protection des données hébergées. Ces garanties, en plus de s'intégrer dans un discours commercial, constituent une barrière supplémentaire contre un accès injustifié des gouvernements aux données.

Cependant, même si les fournisseurs tendent naturellement à mettre en place un certain nombre de protections afin de rester compétitifs sur un marché fortement concurrentiel, ils ne sauraient être les seuls gardiens du respect des droits des personnes visées.

À ce sujet, les discussions parlementaires autour du projet E-evidence ont introduit un mécanisme de notification obligeant l'État requérant à avertir l'État du prestataire de services (État d'exécution), ainsi que l'État du pays de résidence de la personne concernée quand celui-ci est différent de l'État effectuant ou recevant la requête.
Par exemple, si dans le cadre du projet E-evidence, les États-Unis (État requérant) souhaitent accéder à des données localisées en France (État d'exécution) et concernant un résident allemand (pays de résidence), alors ils devront notifier la France et l'Allemagne.
Ce mécanisme permettrait ainsi aux États membres d'exercer leurs fonctions traditionnelles de protection des droits fondamentaux, et d'alléger les responsabilités pesant sur les fournisseurs de services.

***

En somme, le CLOUD Act est le symptôme du besoin de coopération internationale pour répondre aux nouveaux enjeux de lutte contre la criminalité. Le texte nous invite à repenser la souveraineté dans le champ numérique, au-delà du seul principe de territorialité.
Aussi, si les États-Unis et l'UE parviennent à un accord, celui-ci devrait garantir le respect des droits humains et offrir un haut niveau de protection des données personnelles tout en rendant les processus d'obtention de preuves numériques plus efficaces.

Alumni d'IRIS Sup' en Géoéconomie, gestion des risques et responsabilité de l'entreprise et de Grenoble École de Management, Sara Benhadji s'est intéressée aux enjeux de souveraineté numérique dans le cadre de son alternance en Affaires publiques chez IBM. Elle y est désormais consultante en stratégie et fait partie du Conseil régional des Jeunes d'Île-de-France en parallèle.

Cet article est basé sur son mémoire de fin d'études à IRIS Sup' portant sur "La souveraineté numérique européenne face au CLOUD Act" dirigé par Sylvie Matelly, directrice adjointe de l'IRIS.