diploweb.com La revue géopolitique
ISSN : 2111-4307

Le "Cloud Act", trois ans après : révélateur du besoin de définition de notre souveraineté dans l'espace numérique

dimanche 16 mai 2021,par Laura BRINCOURT

Citer cet article / To cite this version :
Laura BRINCOURT, **Le "Cloud Act", trois ans après : révélateur du besoin de définition de notre souveraineté dans l'espace numérique**, *Diploweb.com : la revue géopolitique, 16 mai 2021.*

Hum... Vous semblez apprécier le DIPLOWEB.COM. Nous vous en remercions et vous invitons à participer à sa construction.

Le DIPLOWEB.COM est LE media géopolitique indépendant en accès gratuit, fondé en l'an 2000. Nous vous proposons de participer concrètement à cette réalisation francophone de qualité, lu dans 190 pays. Comment faire ? Nous vous invitons à verser un "pourboire" (tip) à votre convenance via le site **https://fr.tipeee.com/diploweb** . Vous pouvez aussi rédiger un chèque à l'ordre du DIPLOWEB.COM et l'adresser à Diploweb.com, Pierre Verluise, 1 avenue Lamartine, 94300, Vincennes, France. Ou bien encore faire un virement bancaire en demandant un RIB à l'adresse expertise.geopolitique@gmail.com.

Avec 5 000€ par mois, nous pouvons couvrir nos principaux frais de fonctionnement et dégager le temps nécessaire à nos principaux responsables pour qu'ils continuent à travailler sur le DIPLOWEB.COM.
Avec 8 000€ par mois, nous pouvons lancer de nouveaux projets (contenus, événements), voire l'optimisation de la maquette du site web du DIPLOWEB.COM.

Au coeur des facteurs enchevêtrés du numérique, se joue une partie essentielle de notre souveraineté. Le *Cloud Act* des Etats-Unis n'est qu'un révélateur d'un besoin plus général : la définition d'une véritable stratégie nationale et européenne dans l'espace numérique ciblée sur des secteurs et des technologies phares. Il nous faut redevenir stratèges dans une époque dominée par la donnée où chacun a son rôle à jouer pour gagner en souveraineté. Cet article s'intéresse aux besoins, pour l'Etat et les entreprises, de s'organiser, de s'adapter mais aussi de collaborer avec les puissances du numérique dans une géopolitique inédite des données.

LA CRISE du Covid-19 a remis au-devant de la scène des problématiques de puissance et d'autonomie des États dans la gestion de la crise sanitaire. La France en a été à ses dépens un témoin privilégié, de l'absence de masques aux déficits d'équipements médicaux en passant par notre retard dans la découverte d'un vaccin français.

Ces événements accumulés ont fait prendre conscience d'une forme de déclassement et la question de la restauration de la souveraineté nationale et européenne s'est invitée au cœur de l'agenda politique. Cette prise de conscience a créé un *momentum* favorable à un débat vivifié sur plusieurs dimensions de la souveraineté. La souveraineté dite numérique en est une et on le comprend aisément.

En effet, depuis mars 2020, chacun aura pu constater le rôle clé joué par les technologies du numérique pour permettre une continuité de l'activité économique. Nous étions cloîtrés chez nous, mais grâce à elles, nombre d'entre nous ont pu poursuivre leur activité professionnelle. Un autre constat, plus cruel, s'est aussi imposé à nous et aux leaders politiques : Amazon Web Services, Zoom, WhatsApp, LinkedIn, l'Apple Store et dans une toute autre catégorie plus distrayante HouseParty et les apéritifs du premier confinement… toutes ces solutions ont pour point commun d'être américaines.

La souveraineté numérique, ou pour être plus précis la souveraineté dite numérique est donc plus que jamais au cœur des débats. Elle touche autant les pouvoirs publics, les entreprises que les individus. Tous se retrouvent confrontés à la nécessité de maîtriser ce nouveau terrain d'affrontements et d'opportunités.

> Guillaume Poupard, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sur la question de la cyber sécurité : « je ne voudrais pas donner l'impression que tout va bien, parce que tout va mal objectivement. »

Dans une chronique du mois de mars 2021, plusieurs députés et spécialistes du monde digital alertaient : « *nous livrons gratuitement nos données à des entreprises étrangères. Nous ne maîtrisons ni nos réseaux sociaux, ni nos messageries privées, ni nos moteurs de recherche, ni nos systèmes d'exploitation, ni les services numériques personnels ou professionnels hébergés chez des acteurs non européens du cloud*. » [1] Le champ de ces préoccupations témoigne de l'importance et de la complexité de l'enjeu. Cette question de la souveraineté numérique est complexe, car protéiforme. Elle recoupe des enjeux majeurs : cybersécurité, cyberdéfense,

lutte contre la déstabilisation et la désinformation, régulation des géants du numérique, ou encore développement d'une autonomie matérielle et industrielle du numérique sont autant de facettes du phénomène. Le 15 avril 2021, Guillaume Poupard, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) s'exprimait sans détour sur la question de la cyber sécurité « *je ne voudrais pas donner l'impression que tout va bien, parce que tout va mal objectivement* » [2].

D'autant que les acteurs publics sont au premier chef concernés. En début d'année, un collectif composé de députés et de professionnels de la *tech* publiait une lettre ouverte au Président Emmanuel Macron en y dénonçant tant la dépendance de la France à des technologies étrangères que les choix d'équiper des secteurs publics majeurs de solutions numériques proposées par des entreprises étrangères (Education Nationale, Finances, Transports) [3]. On se souviendra des contrats remportés par Palantir auprès de la Direction générale de la sécurité intérieure (DGSI) ou encore du partenariat entre la Banque Publique d'Investissement et Amazon. L'un des derniers exemples en date, ayant provoqué une importante polémique, a été le choix du gouvernement de stocker le « *health data hub* », c'est-à-dire des données de santé des citoyens français, sur un *cloud* Microsoft.

Et le secteur privé n'est pas en reste. On sait que de grands groupes français confient aussi leurs données à des entreprises étrangères via l'utilisation de leurs solutions de *cloud* ou encore en nouant des partenariats commerciaux avec ces géants américains du numérique. C'est le cas par exemple d'Airbus, Thalès, Sanofi, Veolia, Engie ou encore Capgemini. Certaines grandes entreprises françaises du CAC 40 deviennent même des intégrateurs de solutions informatiques américaines, à l'image de Capgemini qui s'allie fréquemment avec Amazon pour accompagner la transformation numérique des entreprises françaises.

Les inquiétudes sont donc légitimes : une partie de notre souveraineté est-elle rognée par des acteurs privés, le plus souvent américains et chinois, dès lors que ces derniers maîtrisent nos données, prétendent être en mesure d'émettre une monnaie, proposent des solutions d'identité numérique, se dotent de leurs propres services de règlement des différends, sont en position de contrôler la liberté d'expression des citoyens ou encore se voient confier la majorité des données de nos entreprises et de nos citoyens ? L'utilisation massive de services proposés par des géants étrangers du numérique est-elle cohérente avec la protection de notre souveraineté nationale, particulièrement dans un contexte de guerre industrielle et économique ?

De son côté, l'Union européenne publiait en décembre 2020 deux projets de loi majeurs, le *Digital Services Act* et le *Digital Markets Act*, pour réguler les géants de la *tech* tout en réitérant sa volonté de bâtir une véritable souveraineté numérique au sein de l'Union européenne. L'attention politique est donc plus que jamais portée sur la question de savoir comment maîtriser son devenir dans ce nouvel espace numérique.

Le paysage étant posé, nous avons fait le choix de mettre ici la focale sur la question de la donnée, souvent définie comme « *l'or noir du XXIe siècle* ». Pourquoi ? Parce qu'elle est devenue un outil majeur de puissance au service des États, mais aussi des acteurs économiques. L'hébergement de ces données et plus particulièrement la technologie du *cloud computing* tient donc une place capitale dans le débat sur la souveraineté dans l'espace numérique.

> La crise sanitaire a mis en exergue la centralité du "cloud" qui nous a permis de travailler depuis n'importe quel lieu et de faire transiter des informations parfois sensibles, à travers des systèmes et des réseaux généralement gérés par des entreprises étrangères, principalement américaines.

Le *cloud computing* désigne une technologie qui permet à ses utilisateurs d'accéder à des services informatiques tels que des serveurs, du stockage, des applications ou des logiciels *via* internet (par opposition à l'utilisation d'un stockage local) à partir d'un fournisseur de *cloud* sur une durée identifiée et à un coût adapté [4]. En d'autres termes, l'utilisateur, par exemple une entreprise, externalise ses données (et autres services ou produits informatiques) de ses bureaux, locaux ou serveurs tangibles, pour les confier à un prestataire de *cloud*.

La crise sanitaire a mis en exergue la centralité du *cloud* qui nous a permis de travailler depuis n'importe quel lieu et de faire transiter des informations parfois sensibles, à travers des systèmes et des réseaux généralement gérés par des entreprises étrangères, principalement américaines. Preuve en est, le secteur est en pleine expansion. À titre d'illustration, Microsoft, acteur majeur du *cloud*, a vu dans certains pays, la demande de ses services *cloud* exploser de 775 % en période de confinement [5].

Représentation artistique des problématiques géopolitiques du "Cloud"
Crédit photographique : Laura Brincourt pour *Diploweb.com*
Brincourt /Diploweb.com

Dans ce contexte, **le *Cloud Act* américain (*Clarifying Lawful Overseas Use of Data*)**, loi promulguée en 2018 sous la présidence de Donald Trump, illustre les défis auxquels peuvent être confrontés États, entreprises et citoyens s'agissant du contrôle et de la protection de leurs données. En effet, **cette législation permet aux autorités de poursuites américaines de demander directement — sous certaines conditions — aux fournisseurs de *cloud* la transmission de données sur des citoyens ou des entreprises non américains**, et ce, peu importe la localisation de ces données. Les entreprises et les citoyens français (et européens) sont donc directement concernés par cette législation. Après les innombrables commentaires et craintes suscités par la promulgation de ce texte à portée extra territoriale, le débat actuel sur la souveraineté dans l'espace numérique a remis le *Cloud Act* en lumière.

Trois ans après son entrée en vigueur, le *Cloud Act* témoigne en réalité d'un besoin plus général : la nécessité de définir une véritable politique française et européenne de souveraineté dans l'espace numérique aujourd'hui encore trop tâtonnante et peu

lisible.

Après une introduction du concept de souveraineté numérique, nous expliquerons en quoi la maîtrise de la donnée, et notamment la technologie du *cloud computing*, est devenue un enjeu important du cyberespace (**I**). Nous verrons par l'illustration du *Cloud Act* que les États-Unis n'hésitent pas à compléter leur domination technologique sur la maîtrise de la donnée par des armes législatives agressives (**II**). Face à ce constat, différentes solutions seront envisagées dans une perspective plus générale de définition de notre souveraineté dans l'espace numérique (**III**).

> NDLR : Alors que plusieurs documents officiels sont en cours de finalisation, cet article offre une précieuse présentation du contexte et des enjeux géopolitiques.

I. La donnée, clé de voûte de la souveraineté dans l'espace numérique

Naviguer parmi les définitions de souveraineté dans l'espace numérique

Le concept de souveraineté numérique est souvent associé à des représentations de l'espace sur lequel il s'applique et qui varie selon les interlocuteurs ou les domaines de recherches (cyberespace, data sphère, espace informationnel, etc.) [6]. Par souci de commodité, nous préférerons parler ici de souveraineté dans l'espace numérique ou dans le cyberespace. Comme l'explique Frédérick Douzet, cet espace numérique est à la fois ancré dans le monde physique du fait de ses infrastructures physiques et ses acteurs économiques, mais il en est aussi indépendant étant donné sa fluidité, son ubiquité et par les informations et les données qui y circulent [7].

On représente généralement cet espace numérique comme composé de plusieurs couches : (i) une couche tangible (infrastructures, câbles sous-marins, *datacenters,* etc.) (ii) une couche logicielle (codes, protocoles, etc.), et (iii) une couche sémantique (contenu informationnel d'internet, messages, etc.) [8]. Il possède sa propre géographie et se distingue des espaces traditionnels que nous connaissons (maritime, terrestre, ou encore aérien).

Il possède donc sa propre géopolitique, ses propres rivalités de pouvoir, mais aussi une multiplicité d'acteurs. La souveraineté dans l'espace numérique inclut à la fois la souveraineté des États, celle des opérateurs économiques (et notamment Google, Apple, Facebook, Amazon et Microsoft dits GAFAM), ou encore celle des utilisateurs ou d'une communauté d'utilisateurs (individus, entreprises, etc.) [9]. La souveraineté dans l'espace numérique repose donc sur un espace complexe dont les contours, la tangibilité et la mutation constante en complexifient la définition.

D'un point de vue juridique, la souveraineté numérique est un concept émergent qui n'obéit à aucun consensus. Le monde juridique s'y réfère généralement en partant de la définition classique du concept de souveraineté, c'est-à-dire le caractère suprême d'une puissance qui n'est soumise à aucune autre. De son côté, la littérature stratégique française préfère

généralement le terme d'autonomie stratégique. Comme le rappelle Alix Desforges, chercheuse au centre de recherche et formation GEODE, l'autonomie stratégique est perçue comme le moyen pour un État d'exercer sa souveraineté [10]. Elle vise à détenir une capacité autonome d'appréciation, de décision et d'action.

Bien que la terminologie utilisée varie selon les observateurs [11], nous tenterons de définir le concept de souveraineté dans l'espace numérique comme **notre capacité à maîtriser l'espace numérique, d'y acquérir une certaine autonomie à la lumière de nos valeurs et de nos intérêts et d'y maintenir une liberté de choix, de décision et de stratégie.**

Partant de cette définition, la souveraineté dans l'espace numérique peut s'analyser selon différentes grilles de lecture qui peuvent éventuellement se combiner ou se compléter.

Premièrement, la souveraineté dans l'espace numérique peut s'analyser à travers ses **différentes dimensions et priorités nationales**. Comme l'expliquait Claire Landais en 2019 lors de son audition devant une commission d'enquête du Sénat [12], cette souveraineté implique d'abord la nécessité pour l'État de préserver ses monopoles régaliens classiques à l'ère numérique face à des acteurs de substitution privés. Elle implique ensuite la capacité de l'État à apprécier et identifier la menace qui pèse sur le cyberespace afin de protéger ses administrations publiques, ses individus ou encore ses opérateurs les plus importants de cyber attaques et de tentatives de pillage ou de déstabilisation. Enfin, une troisième dimension essentielle de la souveraineté dans l'espace numérique consiste pour l'État à maîtriser les outils du numérique afin de garder un contrôle sur ses réseaux, ses communications électroniques et ses données [13].

Deuxièmement, la souveraineté dans l'espace numérique peut s'analyser à travers les différentes couches qui composent cet espace, à savoir matérielle, logicielle et sémantique. Comme l'explique Amaël Cattaruzza dans son ouvrage *Géopolitique des données numériques*, cette conceptualisation du cyberespace permet une **analyse géopolitique** de celui-ci avec une matérialisation géographique du pouvoir exercé sur cet espace conceptualisé. Cette méthode est souvent utilisée dans la réflexion stratégique de l'État. La puissance d'un État sera alors analysée par son poids économique, technique et politique sur les différentes strates du cyberespace et visible à différents niveaux (infrastructures matérielles, développement de technologies et de capacités humaines, développement de la recherche, poids économique ou encore outils juridiques extraterritoriaux) [14].

Enfin, la souveraineté dans l'espace numérique peut, lorsque cela est possible, s'analyser selon une grille de **lecture technologique** en découpant les différentes composantes et/ou étapes du cycle de vie d'une technologie choisie pour ensuite déterminer le degré de souveraineté qu'on estimera essentiel à chacune de ces composantes ou étapes. Cette méthode d'analyse prend donc comme point de départ une technologie donnée pour y appliquer différents niveaux de souveraineté spécifiques. Elle s'intéresse plus particulièrement aux armes technologiques nécessaires pour pouvoir jouer un rôle sur l'échiquier mondial de l'espace numérique.

Autrement dit, l'objectif de cette approche est de scinder les différentes briques qui composent une technologie et de déterminer le degré critique de souveraineté requis pour chacune de ces briques selon nos principes, nos valeurs et nos intérêts, ou autrement dit, selon notre définition de la souveraineté dans l'espace numérique. Comme pour les autres grilles de lecture

mentionnées ci-dessus, différents leviers pourront alors être mobilisés afin d'atteindre le niveau de souveraineté souhaité sur le segment technologique visé : moyens réglementaires et normatifs, développement d'une politique industrielle sur le segment technologique en question ou encore choix de nouer des partenariats constructifs avec des acteurs déjà en place (même étrangers). Cette approche a le mérite de répondre à un certain degré de réalisme sans tomber dans l'illusion d'une pleine souveraineté numérique. En effet, s'il existe des technologies sur lesquelles la France pourrait ambitionner une pleine autonomie de décision et d'action, de nombreuses technologies du cyberespace impliquent encore un degré plus ou moins important de dépendance ou de collaboration avec une ou plusieurs puissances étrangères (exemple la 5 G).

Quelle que soit la grille de lecture adoptée, la souveraineté dans l'espace numérique implique nécessairement une réflexion sur la donnée. En effet, la donnée est devenue un véritable instrument de pouvoir et de puissance pour les États, mais aussi pour les acteurs économiques et toute technologie qui la concerne prend nécessairement une place centrale dans le débat sur la souveraineté dans l'espace numérique.

Qu'importe l'enjeu, on y retrouve toujours la donnée

La donnée s'invite très régulièrement dans notre actualité économique et politique. La prolifération des cyberattaques et autres rançongiciels (Wannacry, NotPetya en 2017, etc…), l'affaire Snowden en 2013, l'utilisation abusive des données des Européens dans des contextes électoraux (Cambridge analytica) ou encore les *Macronleaks* de 2017 ont entraîné une prise de conscience mondiale sur l'importance stratégique de la maîtrise et du contrôle des données.

Depuis plusieurs années, la production de données est exponentielle. Elle est le fruit de l'activité humaine, des entreprises, des institutions ou autres capteurs. Ces données obtiennent une valeur économique inédite résultant essentiellement de leur traitement notamment à travers le *big data*, le *machine learning* ou l'intelligence artificielle. Les entreprises sont d'ailleurs de plus en plus conscientes que les données font partie de leur patrimoine informationnel et qu'il convient de les protéger.

La donnée est également devenue un enjeu de puissance pour les États. Ces derniers doivent faire face à des exercices et des manifestations de puissances multiples pouvant directement mettre en jeu leur souveraineté. Des tentatives de cyberattaques aux questions de désinformation ou d'influence sur les scrutins électoraux, la menace est variée.

Enfin, les individus sont eux aussi directement concernés par la protection de leurs données notamment au regard de la protection de leurs données personnelles. Du *Big Data* au *Big Brother*, la frontière est ténue. Quotidiennement sujets à la captation et à l'analyse de leurs données, ils sont en quelque sorte confrontés à une observation continue de leur personne et de leur activité.

Plus

Découvrez la Masterclass Diploweb : Pourquoi les données numériques sont-elles géopolitiques ?

La numérisation de pans entiers de l'activité humaine est aujourd'hui une évidence. De moins en moins d'actes du quotidien échappent aux réseaux sur lesquels on les pratique, a fortiori en temps de pandémie : passer un coup de fil à des proches, suivre un cours, se déplacer dans la rue avec un smartphone … Toutes ces activités anodines génèrent des données numériques qui font l'objet de bien des convoitises, qu'elles soient commerciales, politiques ou stratégiques.

Parce qu'elles circulent à la surface du globe via un maillage complexe de câbles, de protocoles et de plateformes, **nos données sont géopolitiques.** A la fois objet et source de pouvoir, elles sont au cœur d'un nombre croissant de conflits, tandis que plus aucune guerre n'échappe au numérique. C'est d'ailleurs cette réalité qui est au centre du concept de Datasphère.

Pourquoi les données numériques sont-elles géopolitiques ? MasterClass de Kevin Limonier

L'objectif de **ce cours de Kevin Limonier** est donc de comprendre les enjeux géopolitiques inhérents à cette datasphère dans laquelle nous évoluons toutes et tous. Loin d'être déconnectée du monde physique, elle en est plutôt un prolongement – comme une sorte de réalité augmentée que nous autres géographes commençons à peine à explorer.

Quelle que soit l'échelle considérée, le contrôle et la gestion des données sont donc devenus des outils centraux et incontournables d'exercice de la puissance dans une sphère géopolitique inédite. Logiquement, la technologie du *cloud* se situe au cœur des préoccupations relatives à la maîtrise de la donnée, et plus généralement à la souveraineté dans le cyberespace.

Aujourd'hui, dans leur grande majorité, les données sont stockées dans des *data centers* et via le *cloud computing*. Ce remplacement de l'informatique en local pour offrir les mêmes services à distance par une connexion internet permet aux entreprises d'utiliser des prestations depuis n'importe quel endroit et sous forme de services payés à l'usage. Cette externalisation permet

généralement d'accroître l'efficacité économique des traitements de données. On estime par exemple que le stockage des activités sur le *cloud* induirait une baisse des coûts liés à internet en moyenne de 20 à 50 %, rendant ainsi les entreprises plus compétitives [15].

En 2020, le marché du *cloud* représentait à lui seul près de 300 milliards de dollars [16]. Or, ce marché est largement dominé par des sociétés américaines telles qu'Amazon, Microsoft ou encore Google. Par exemple, les administrations et les entreprises françaises utilisent encore très largement les systèmes de *cloud computing* Microsoft Azure, Google Cloud ou encore Amazon Web Services. La France se trouve donc dans un rapport de dépendance manifeste aux États-Unis en matière de *cloud* et lui confie l'intégrité et la confidentialité de la grande majorité de ses données.

Les raisons d'opter pour les solutions *cloud* de ces entreprises américaines ne manquent pas : technologies très avancées (stockage, analyse de donnée, intelligence artificielle, etc.) proposition de *packages* de produits informatiques attractifs, prix compétitifs, habitudes d'utilisation de leurs services, représentations mentales associant les Etats-Unis à des valeurs positives (innovation, démocratie, …), etc.

Le problème réside dans le fait que ces entreprises proposent généralement des **contrats d'adhésion laissant peu de marge de négociation pour l'utilisateur et qui désignent la plupart du temps le droit américain comme droit applicable**. Mais plus important encore, ces entreprises, du fait de leurs liens étroits avec les États-Unis, **sont soumises à des législations intrusives qui participent à la puissance américaine sur le contrôle des données** [17].

II. Le *Cloud Act* et la réponse française — révélateur d'une absence de stratégie dans le numérique

Les États-Unis ont bien compris l'enjeu et ont fait de la maîtrise de la donnée un axe majeur de leur stratégie de puissance sur le cyberespace.

Cette stratégie s'est illustrée tant au niveau de ses acteurs économiques initialement largement soutenus par les pouvoirs publics américains (comme les GAFAM) qu'au niveau de sa politique de défense et de sécurité nationale à travers la captation massive de données (*National Security Agency* ou NSA). Cette stratégie passe aussi par une politique législative ambitieuse et parfois à visée extraterritoriale permettant aux autorités américaines d'avoir accès à un nombre important de données à travers le monde (création de la NSA, le *Foreign Intelligence Surveillance Act*, *USA Patriot Act*, *Freedom Act* ou encore le *Stored Communication Act*). Avant le *Cloud Act*, les fournisseurs de *cloud* étaient donc déjà amenés à transférer sur demande des données ou métadonnées aux services de renseignement ou aux autorités de poursuite américaines.

Le *Cloud Act*, adopté le 23 mars 2018 par le Congrès américain, est venu clarifier les règles relatives aux demandes de communication de données stockées **en dehors** des États-Unis formulées par les autorités américaines.

Dès son adoption, le *Cloud Act* a créé un émoi particulièrement important. Nombreux sont ceux qui se sont interrogés sur le danger potentiel que représenterait cette législation sans

forcément distinguer les types de données sur lesquels portaient leurs inquiétudes (données personnelles ou non) ou encore la portée réelle de cette législation. Le *Cloud Act* ayant déjà été largement analysé par de nombreux commentateurs, nous reviendrons brièvement sur ses dispositions principales pour mieux nous concentrer sur sa portée concrète.

Le Cloud Act, une arme législative américaine ?

Dans sa première partie, le *Cloud Act* permet aux autorités américaines (autorités de poursuite, services de renseignement) de demander directement aux opérateurs et fournisseurs de services en ligne soumis aux juridictions américaines la communication de données placées sous leur contrôle, sans considération de la localisation de ces dernières. En d'autres termes, **cette loi permet aux autorités américaines de contourner les procédures classiques de demande d'entraide et de coopération judiciaire internationale entre États [18] et permet au juge américain d'aller directement chercher les données chez le prestataire de communications électroniques ou le prestataire de services informatiques à distance**. En théorie, une entreprise française qui stockerait des données sensibles sur un *cloud* américain pourrait donc voir ses données communiquées par son fournisseur *cloud* aux autorités américaines sans même être mises au courant.

Certes, une demande en vertu du *Cloud Act* doit impliquer une enquête pénale et l'autorité américaine devra au préalable être en possession d'un mandat (« *warrant* ») délivré par une juridiction, une injonction (« *subpoena* ») ou encore une ordonnance judiciaire (« *court order* »). À ce titre, l'autorité requérante devra démontrer en quoi les informations visées sont utiles à l'enquête. Cependant, le champ d'application du *Cloud Act* reste large tant du point de vue des entités concernées (tous les fournisseurs de services de communications électroniques et prestataires de *cloud* relevant de la juridiction américaine et leurs filiales), des données collectées (peu importe leur localisation géographique) ou des infractions visées par la demande de communication de données (notion floue de « *serious crime* » pouvant potentiellement relever d'un nombre considérable d'infractions).

La deuxième partie du *Cloud Act* prévoit quant à elle la possibilité pour les autorités américaines de conclure des accords internationaux avec des gouvernements étrangers afin de permettre aux autorités respectives des États signataires de ces accords de demander directement aux fournisseurs de services de communication, traitement et stockage relevant de leur juridiction, la communication de données en dehors de toute procédure d'assistance judiciaire mutuelle [19]. Ces accords ont donc vocation à fixer les règles de communication de données entre les États signataires [20]. Pour le moment la France n'a pas signé d'accord bilatéral avec les États-Unis, mais, en février 2019, le Conseil de l'Union européenne a autorisé l'ouverture de négociations en vue d'un accord entre l'Union européenne et les États-Unis [21]. Tout l'enjeu de cet accord est d'aboutir à un régime équilibré et réciproque entre l'Union et les États-Unis qui permette un transfert efficace des données pour une lutte plus fluide contre la criminalité.

En l'attente d'un tel accord, il est intéressant de s'intéresser aux effets concrets du *Cloud Act* depuis sa promulgation il y a trois ans.

Des effets limités, mais surtout un révélateur de nos carences

Concrètement, l'effet combiné de la domination du marché du *cloud* par les entreprises américaines et cette législation à portée extraterritoriale expose les données de nos entreprises, parfois sensibles, à l'œil indiscret des États-Unis **dans un contexte croissant de guerre économique**. C'est avant tout l'inquiétude d'un transfert abusif (par exemple relavant de **l'espionnage économique et industriel**) qui vient nourrir les craintes suscitées par le *Cloud Act*.

Il convient néanmoins de nuancer ces inquiétudes. Si un tel abus ne peut être exclu, il reste difficile d'imaginer que des enquêteurs américains puissent facilement motiver leurs besoins spécifiques d'informations sensibles et commerciales (brevet, savoir-faire, etc.) et surtout obtiennent d'un juge indépendant américain un tel transfert dans le cadre de poursuites pour des faits graves comme des actes de corruption ou de terrorisme. Il est donc important de garder à l'esprit que les demandes en vertu du *Cloud Act* (et leur périmètre) sont contrôlées en amont par une autorité judiciaire indépendante.

Aujourd'hui, les principaux acteurs du *cloud* se veulent rassurants quant à l'effet du *Cloud Act*.

D'abord en termes de chiffre : ils assurent que le *Cloud Act* n'a pas changé le paysage juridique de la communication des données aux autorités américaines et publient régulièrement des rapports de transparence sur la proportion des données communiquées (notamment en vertu de lois à portée extraterritoriale telle que le *Cloud Act*). En début d'année 2020, un représentant de Microsoft, n° 2 du marché mondial du *cloud*, expliquait déjà : « *Si on parle en volume, l'inquiétude que nous avons pu cerner à la naissance du Cloud Act ne se ressent pas sur le terrain* ». Il indiquait également que l'immense majorité des demandes visait des clients individuels et que les demandes concernant les entreprises étaient extrêmement rares [22].

Amazon Web Services, n° 1 du marché mondial du *cloud*, affirmait dans son dernier rapport biannuel de juillet-décembre 2020 qu'aucune donnée de contenu d'entreprise (« *enterprise content data* ») localisée en dehors des États-Unis n'avait été communiquée aux autorités américaines [23]. Ici, la notion de « *contenu d'entreprise* » mériterait quelques éclaircissements du fournisseur de *cloud*. De son côté, Microsoft expliquait que pour cette même période (juillet-décembre 2020), l'entreprise avait reçu 165 demandes de données stockées en dehors des États-Unis (« *content data stored outside the United States* ») et qu'une seule de ces demandes avait donné lieu à une transmission de données dites « *enterprise content data* » [24]. De nouveau, les termes utilisés mériteraient d'être définis par le fournisseur pour une meilleure compréhension des informations publiées. Autre difficulté : les rapports de ces entreprises ne contiennent pas toujours les mêmes catégories ou les mêmes types d'information d'année en année, ce qui ce qui rend parfois difficile une analyse temporelle (et notamment depuis la promulgation du *Cloud Act*) des demandes formulées et du volume de données transmis.

Ensuite, les entreprises de *cloud* se veulent rassurantes sur leur manière de traiter les demandes des autorités américaines. Ces géants du *cloud* tel que Microsoft décrivent généralement leur procédure face à une demande fondée sur le *Cloud Act* de la manière suivante : (i) premièrement, l'entreprise répondrait aux autorités américaines de demander les données en question directement aux clients concernés, (ii) deuxièmement, l'entreprise de *cloud* avertirait immédiatement son client de la demande le concernant (sauf cas

d'impossibilités prévues par la loi) et (iii) troisièmement, l'entreprise de *cloud* s'opposerait à la demande de communication de données devant le juge américain en cas de demandes non réalisables, imprécises ou encore en cas de conflit de loi précis et clair [25].

Cette question du conflit de lois est centrale dans tout débat sur le *Cloud Act*.

Avec ou sans *executive agreement*, et selon des modalités et des fondements différents en fonction de l'existence d'un tel accord, le fournisseur de *cloud* pourra toujours faire valoir qu'une divulgation des données en vertu du *Cloud Act* le conduirait à enfreindre les lois locales de l'État où se trouvent les données. À ce titre, le juge américain devra analyser et mettre en balance la probabilité et l'étendue des risques et sanctions encourus par le prestataire de *cloud* qui serait conduit à enfreindre une législation locale s'il se conformait à une demande de communication de données fondée sur le *Cloud Act*. Plus ce risque sera élevé, plus le juge américain sera enclin à s'opposer à la demande de communication sollicitée par les autorités américaines.

En réalité, ce conflit de lois sera en quelque sorte révélateur de rapports de forces s'inscrivant plus généralement dans une géopolitique des données en plein essor et au sein de laquelle les États usent de tous les moyens (notamment réglementaires et juridiques) pour étendre leur contrôle sur les données.

En théorie, l'application du *Cloud Act* par un fournisseur pourrait le conduire à être en conflit avec plusieurs lois françaises et européennes.

Concernant les données personnelles, l'Union européenne s'est dotée d'un instrument solide de protection de ce type de données : **le Règlement Général sur la Protection des Données (RGPD)** qui réglemente strictement le transfert de données personnelles vers toute autorité étrangère. Cette réglementation est susceptible de faire obstacle à une demande américaine fondée sur le *Cloud Act* et fait déjà l'objet de contentieux et de négociations importants entre l'Union européenne et les États-Unis [26]. Dans ce rapport de force, la France et l'Union européenne peuvent donc tenir tête à la force de frappe américaine.

Concernant les données des personnes morales, la loi de blocage française du 26 juillet 1968 ou encore la loi du 30 juillet 2018 relative au secret des affaires pourraient potentiellement entrer en conflit avec une demande de communication fondée sur le *Cloud Act*. En effet, ces deux législations interdisent en principe la communication de données en dehors de tout accord international, c'est-à-dire sur le seul fondement d'une demande unilatérale d'une administration étrangère (comme le permet le *Cloud Act*).

Malheureusement, ni la loi de blocage ni la législation relative au secret des affaires ne prévoient un cadre juridique suffisamment contraignant et des sanctions assez dissuasives pour encourager un juge américain à écarter l'application de la loi américaine au profit de la législation française. Aujourd'hui, il paraît donc **difficile de prévoir ce qu'un juge américain déciderait s'il devait mettre en balance une demande de communication de données d'une personne morale française fondée sur le *Cloud Act* avec les lois françaises de blocage ou sur le secret des affaires. Force est de constater que sur le plan des données non personnelles, la législation française (et européenne) peine à apporter un gage de sécurité suffisant**.

En fin d'année 2020, Microsoft a souhaité apporter une assurance supplémentaire à ses clients en annonçant qu'elle contesterait toute demande de données émanant d'un gouvernement lorsqu'il existerait une base légale pour le faire (donc par exemple en cas de conflit de lois), mais surtout qu'elle s'engagerait à offrir une compensation financière aux utilisateurs dont les données auraient été divulguées en vertu d'une demande qui ne respecterait pas le RGPD. De son côté, en février 2021 Amazon Web Services adoptait une série d'engagements contractuels s'appliquant à l'ensemble de ses données clients soumises au RGPD. L'entreprise s'engageait par exemple à contester toute demande gouvernementale qui serait en contradiction avec la législation européenne [27].

Qu'en est-il des demandes qui ne respecteraient pas une autre loi que le RGPD ? Qu'en est-il des données commerciales sensibles des entreprises qui manquent d'un équivalent RGPD pour tenir tête aux Américains ? Dans tous les cas, l'initiative est révélatrice de la volonté de ces géants américains du *cloud* de ne pas perdre le marché européen et ses 447,3 millions d'utilisateurs.

Même si la portée concrète du *Cloud Act* ne semble pas avoir substantiellement modifié le volume de transfert de données vers les États-Unis, cette législation est révélatrice de conflits de lois potentiels et d'insécurité juridique pour les utilisateurs du *cloud*. **Le *Cloud Act* met ainsi en lumière les terrains d'affrontement sur lesquels la France a les moyens de défendre ses intérêts et ceux sur lesquels elle ne peut sortir victorieuse sans un renforcement urgent de son arsenal législatif et réglementaire. Finalement, il semble que le débat qui entoure le *Cloud Act* soit surtout un révélateur du manque de stratégie dans notre souveraineté sur la donnée et plus généralement sur l'espace numérique**. Heureusement, il n'est pas trop tard.

III. Redevenir stratèges au sein de l'espace numérique

En dehors d'une définition plus générale de notre politique sur la souveraineté dans l'espace numérique, le *cloud* offre une illustration des différents leviers pouvant être mis en œuvre par l'État et les acteurs économiques pour gagner en souveraineté dans un domaine déterminé. Sans être exhaustifs, nous en évoquerons quelques-uns.

L'État porteur de nos ambitions numériques

De manière générale, une **politique industrielle lisible et assumée** sur le *cloud computing* est plus que jamais nécessaire. Comme mentionné par Claire Landais lors de son audition au Sénat en 2019, il paraît opportun de penser la stratégie du *cloud* suivant une logique de cercles concentriques avec des exigences graduées en matière de protection des données et des communications. C'est aujourd'hui la logique utilisée par l'État avec ses données les plus sensibles comme les informations classifiées, qui peuvent impliquer une maîtrise nationale totale de certaines technologies (par exemple le recours à un *cloud* interne) ou un niveau de contrôle de sécurité renforcé. Pour le champ médian des données et des communications sensibles (autres données publiques, données sensibles d'entreprises, etc.), des exigences sont également imposées, notamment sous forme de label ou de certifications des *cloud* (voir notamment les certifications délivrées par l'ANSSI) [28].

De manière générale, l'idée est d'imposer les règles les plus strictes et les plus contraignantes

aux acteurs dont les activités sont les plus vitales ou les plus essentielles à la Nation pour lesquelles toute attaque ou vol de données présenterait un caractère très dommageable. Ces cercles concentriques peuvent ainsi s'affiner et se multiplier selon la sensibilité des données afin d'y appliquer le niveau d'exigence et de protection adapté allant de requêtes techniques précises à des certifications ou des recommandations.

À ce titre, nombre d'entreprises seraient gagnantes du développement et de l'évolution de labels et certifications de souveraineté (techniques, mais garantissant aussi le respect des critères de non-soumission à des réglementations extraeuropéennes). Avec qui peut-on travailler en confiance ? **Afin de pouvoir développer un écosystème de confiance, la souveraineté (notamment dans le *cloud*) doit être un élément à la fois lisible et visible pour les entreprises comme pour les utilisateurs**. Il est important de donner les outils nécessaires aux entreprises souhaitant mettre en avant leur positionnement en termes de souveraineté dans l'espace numérique.

Un autre aspect important de la définition d'une politique industrielle du numérique est bien évidemment la mise en avant de nos champions nationaux et européens, notamment du *cloud computing* .

En plus d'un accompagnement dans le développement des outils et des composantes techniques du *cloud*, l'État doit se montrer porteur des ambitions de ses acteurs économiques et se donner les moyens de renforcer sa filière souveraine. Les entreprises américaines ont souvent une longueur d'avance technologique dans les services qu'elles proposent aux entreprises françaises et les logiciels auxquelles ces dernières souscrivent s'enrichissent continuellement de nouvelles fonctionnalités. Le secteur public doit donc soutenir les entreprises nationales pour leur donner accès au marché et leur permettre de grandir.

Accompagner, financer et promouvoir nos entreprises passe par une prise de risque nécessaire. Choisir une entreprise française de *cloud* pour héberger des données dans le cadre de projets publics — même en présence d'alternatives étrangères plus avantageuses, plus développées ou moins coûteuses — constitue un choix assumé de soutenir son industrie, de donner accès au marché à cette entreprise nationale et de lui permettre ainsi de développer sa R&D, de s'adapter et de répondre aux besoins du marché. Ceci est d'autant plus nécessaire quand le projet est lui-même porteur d'intérêts souverains ou d'informations sensibles. A l'inverse, choisir un *cloud* étranger revient *de facto* à restreindre l'accès au marché à des entreprises nationales et ne pas leur donner les moyens de s'améliorer. Que ce choix soit motivé par des habitudes, un souci d'adopter la solution la plus optimale à court ou moyen terme, ou pour toute autre raison, celui-ci s'inscrit forcément à contre-courant d'une démarche d'encouragement de notre industrie numérique.

Le choix est donc stratégique, mais surtout politique. L'exercice est difficile et implique que la moindre décision sur le choix d'un fournisseur *cloud* puisse être porteur d'un message politique, souhaité ou non, dans un cadre de décision généralement complexe et limité par le temps politique. Cela n'exclut évidemment pas que certains projets publics (par exemple impliquant des données moins sensibles) puissent être associés à des offres de prestataires étrangers, mais il est essentiel que nos entreprises françaises (ou européennes) se sentent soutenues par une politique publique stimulante.

Les États ont ensuite un rôle à jouer en termes de régulation. On l'a vu, **le droit et la régulation** sont en effet devenus des armes de guerre économique majeures pour plusieurs puissances étatiques (notamment les États-Unis ou encore la Chine) et constituent à présent des leviers importants dans la définition d'une souveraineté dans l'espace numérique. **Au-delà du développement de solutions industrielles, l'écosystème juridique jouera sur nos rapports de force avec les puissances étrangères**.

À ce titre, comme cela a déjà été recommandé par plusieurs commentateurs du *Cloud Act*, il nous semble essentiel de renforcer notre réponse face à cette législation américaine et de prévenir au maximum tout conflit de législation porteur d'incertitude pour les utilisateurs. Ainsi, la conclusion d'un *executive agreement* entre l'Union européenne et les États-Unis mentionné plus haut devrait venir clarifier la gestion des conflits normatifs potentiels et apporter davantage de sécurité juridique aux acteurs concernés. Mais en parallèle de cette négociation, notre arsenal juridique applicable à la protection des données des personnes morales devra nécessairement être renforcé (par exemple la loi de blocage ou la loi sur le secret des affaires) : ces textes, une fois renforcés, auront d'une part un effet incitatif dans les négociations qui doivent s'engager entre États et, d'autre part, un effet dissuasif sur les entreprises étrangères concernées et exposées au risque d'être en infraction avec nos normes.

Un troisième levier est notre capacité à nouer des partenariats intelligents et souverains. L'exemple du partenariat OVH et Google illustre bien cette opportunité. En novembre 2020, ces deux entreprises (l'une française et l'autre américaine) ont annoncé leur partenariat stratégique pour co-construire une solution *cloud* de confiance en Europe. L'objectif annoncé : « *apporter aux organisations européennes des technologies de pointe, reposant sur une infrastructure de confiance, pour répondre à leurs besoins croissants en matière de contrôle strict de leurs données, de sécurité, de transparence et de confidentialité* (…) » [29]. Concrètement, les utilisateurs bénéficieront ainsi des logiciels et services avancés de Google et de l'infrastructure et l'hébergement en France d'OVH.

La recherche de souveraineté ne doit donc pas exclure notre liberté et notre capacité à choisir des partenaires - mêmes étrangers - et de travailler ensemble sur les solutions les plus innovantes et les plus adaptées. De leur côté, les GAFAM ont tout intérêt à chercher à établir ce type de partenariats au sein d'un marché européen très lucratif. Contrairement aux idées reçues, GAFAM et gouvernement américain n'ont pas toujours des intérêts concordants.

Au niveau européen la tournure que prend le projet Gaia X semble répondre à une même recherche d'efficacité dans la collaboration. En effet, ce projet d'initiative franco-allemande devenu un projet européen consiste à rassembler des entreprises du *cloud* (européennes, mais aussi extra européennes) autour d'un référentiel commun répondant à certaines exigences et à permettre aux utilisateurs un choix éclairé de leur fournisseur *cloud* au regard de divers critères (interopérabilité et portabilité des données, localisation des données, juridictions sous lesquelles sont placées les données, etc.). Le contenu de ce projet se précisera davantage dans les mois à venir.

Les entreprises : la souveraineté est aussi du côté des victimes potentielles

Enfin, la souveraineté doit aussi s'entendre eu égard aux acteurs économiques dans leur

ensemble qui participent à la souveraineté nationale par leur productivité, les emplois qu'ils créent, etc. Ces entreprises sont directement concernées par l'importance que revêt la protection de leurs données et ont leur propre rôle à jouer dans la maîtrise de l'externalisation de ces dernières. Comme le rappelle Guillaume Poupard, directeur de l'ANSSI, chacun doit être acteur de sa propre protection [30].

En effet, l'externalisation de l'hébergement des données à un prestataire de *cloud* implique nécessairement un risque pour l'intégrité, la protection et la confidentialité de données parfois sensibles pour les entreprises comme les informations stratégiques, les brevets, ou ce qui relève du secret d'affaires ou du savoir-faire.

Les entreprises devront d'abord être vigilantes en amont de la signature d'un contrat avec leur prestataire de *cloud* en procédant à une évaluation précontractuelle de la sensibilité des données, une classification des données selon leur degré de sensibilité ainsi qu'une évaluation de l'incidence potentielle économique et juridique d'une externalisation. La sensibilité est un concept très différent d'une entreprise à une autre et chaque entreprise doit ici jouer son rôle dans son appréciation.

Les entreprises devront également faire preuve de vigilance au moment de la négociation du contrat en prêtant une attention particulière aux différentes garanties prévues par celui-ci comme les engagements quantitatifs techniques, les engagements de disponibilités des données et de continuité de l'activité, les plans de gestion d'incident, les conditions de réversibilité, de destruction et de restitution des données ou encore les conditions de désengagement de l'utilisateur.

Elles devront ensuite choisir, selon la sensibilité des données hébergées, les moyens techniques et processuels nécessaires pour protéger la confidentialité de leurs données (anonymisation, pseudonymisation, techniques de chiffrement) [31]. À ce titre, les prestataires de *cloud* américains invoquent fréquemment la possibilité pour le client de détenir seul la clé de déchiffrement de données stockées dans leur *cloud* sans que le prestataire ne puisse y avoir accès. Ceci rendrait impossible le décryptage par les autorités locales, même en cas de coopération forcée du prestataire de *cloud*. De manière générale, de plus en plus d'autorités de surveillance élaborent des recommandations pour les entreprises utilisant des services de *cloud* (le Comité Européen de la Protection des Données, la CNIL, l'ACPR, etc.). Il revient ensuite à chaque entreprise, selon ses besoins, d'adopter les outils techniques ou contractuels appropriés pour atteindre le degré de souveraineté souhaité dans son utilisation du *cloud*.

Il est également intéressant de noter que face à une certaine lenteur du rythme politique et législatif, des autorités européennes régulatrices [32] de certains secteurs d'activités (tels que le secteur bancaire) incitent les acteurs à réguler l'externalisation massive de leurs services et notamment de leurs systèmes informatiques.

*****

Au milieu des facteurs enchevêtrés du numérique, se joue une partie essentielle de notre souveraineté. Notre stratégie face à la technologie du *cloud* en est une facette éloquente. **Le *Cloud Act* n'est qu'un révélateur d'un besoin plus général : la définition d'une véritable stratégie nationale et européenne dans l'espace numérique ciblée sur des**

secteurs et des technologies phares. Il nous faut redevenir stratèges dans une époque dominée par la donnée où chacun a son rôle à jouer pour gagner en souveraineté.

Copyright Mai 2021-Brincourt/Diploweb.com

P.-S.

Laura Brincourt exerce depuis plusieurs années en tant qu'avocate spécialisée en droit international. Depuis quelques années, elle se passionne pour l'espace numérique, ses enjeux industriels et géopolitiques, ainsi que l'importance et la protection des données. Courriel : infos.lbrin gmail.com

---

Notes

[1] https://www.journaldunet.com/solutions/dsi/1498549-dans-la-crise-actuelle-les-acteurs-publics-doivent-encourager-les-citoyens-a-opter-pour-les-solutions-numeriques-souveraines/

[2] http://videos.senat.fr/video.2251670_60761aa01efc4.table-ronde-sur--la-cybersecurite-des-eti-pme-tpe--la-reponse-des-pouvoirs-publics-

[3] https://www.latribune.fr/opinions/tribunes/souverainete-numerique-lettre-a-emmanuel-macron-879507.html

[4] Amaël Cattaruzza, *Géopolitique des données numériques - Pouvoir et conflits à l'heure du Big Data*, Le Cavalier Bleu, 2019, p. 71.

[5] https://www.forbes.com/sites/martingiles/2020/03/30/microsoft-cloud-service-775-percent-rise-covid-19/?sh=22725bd96862

[6] Frédérick Douzet, Éditorial. Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique, *Hérodote*, 2020/2-3 (n°177-178) ; voir aussi les explications de T. Breton devant la Commission du Sénat sur la souveraineté numérique du 28 mai 2019, http://www.senat.fr/compte-rendu-commissions/20190527/ce_souverainete.html

[7] Frédérick Douzet, Éditorial. Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique, *Hérodote*, 2020/2-3 (n°177-178), p.5.

[8] Amaël Cattaruzza, *Géopolitique des données numériques - Pouvoir et conflits à l'heure du Big Data*, Le Cavalier Bleu, 2019, pp. 15-16.

[9] P. Türk, *Définition et enjeux de la souveraineté numérique*, Cahiers français, Comprendre la souveraineté numérique, mai-juin 2020, n°415, p. 18 et s.

[10] Pour plus d'explications, voir l'article de D. Danet et A. Desforges, *Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques*, Hérodote, 2020/2-3, pp. 179-195.

[11] Pour plus d'explications, voir aussi P. Türk, *Définition et enjeux de la souveraineté numérique*, Cahiers français, Comprendre la souveraineté numérique, mai-juin 2020, n°415, p. 18 et s. ; voir aussi la définition retenue par A. Degans dans son article *Comment définir la sécurité économique* : https://www.diploweb.com/Radio-Diploweb-Comment-definir-la-securite-economique.html

[12] Claire Landais alors Secrétaire générale de la défense et de la sécurité nationale a été auditionnée le 23 mai 2019 par la commission d'enquête sur la souveraineté numérique du Sénat, voir notamment C. Landais, *Cyberdéfense : quelle stratégie pour la France ?*, Cahiers français, mai-juin 2020, n° 415, pp. 68 et s.

[13] Pour un compte-rendu de l'intervention de C. Landais : https://www.senat.fr/rap/r19-007-2/r19-007-2.html#toc1

[14] Amaël Cattaruzza, *Géopolitique des données numériques, Pouvoir et conflits à l'heure du Big Data*, Le Cavalier Bleu, 2019, pp. 16 et s.

[15] *Cloud* Computing, les grands enjeux réglementaires, sous la direction d'E. Jouffin, Hors-série Banque & Droit, février 2021, p. 4.

[16] https://www.marketsandmarkets.com/Market-Reports/{cloud-computing-market-234.html

[17] Voir sur ce sujet, O. Iteanu, *Pourquoi le cloud computing est un enjeu de souveraineté numérique*, Hors-série Banque & Droit, février 2021, pp. 8 et s.

[18] De manière classique, l'obtention de preuve se situant à l'étranger peut se faire via différents moyens, souvent longs à mettre en œuvre, tels que l'application de procédures spécifiques détaillées dans des traités d'entraide judiciaire entre pays (en anglais, *Mutual legal assistance treaty* ou MLAT), par commission rogatoires internationales etc.

[19] Voir notamment l'analyse d'E. Mignon : https://www.august-debouzy.com/fr/blog/1193-faut-il-avoir-peur-du-{cloud-act

[20] À titre d'exemple, un premier accord bilatéral a été conclu le 7 octobre 2019 entre les États-Unis et le Royaume-Uni.

[21] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A52019PC0070

[22] https://experiences.microsoft.fr/articles/cybersecurite/faut-il-avoir-peur-du-cloud-act/

[23] https://d1.awsstatic.com/certifications/Information_Request_Report_December_2020.pdf

[24] https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

[25] Rapport remis à M. le Président du Sénat le 1er octobre 2019 au nom de la commission d'enquête sur la souveraineté numérique présidé par M. Franck Montaugé, pp. 74-75 : http://www.senat.fr/rap/r19-007-1/r19-007-11.pdf

[26] Pour plus d'informations sur les conflits juridiques entre le RGPD et le cadre des transferts de données prévu aux Etats-Unis voir notamment : https://www.cnil.fr/fr/invalidation-du-privacy-shield-les-premieres-questions-reponses-du-cepd ; https://www.dalloz-actualite.fr/node/schrems-ii-repercussion-francaise#.YIWnFNyxWUk ; https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

[27] Pour Microsoft : https://www.usine-digitale.fr/article/microsoft-s-engage-a-dedommager-les-utilisateurs-en-cas-de-divulgation-gouvernementale-de-leurs-donnees.N1032309 ; pour Amazon : https://aws.amazon.com/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/

[28] C. Landais, Cyberdéfense : quelle stratégie pour la France ?, Cahiers français, mai-juin 2020, n° 415, pp. 68 et s.

[29] https://www.ovh.com/ma/news/presse/cpl1685.ovhcloud-google-cloud-annoncent-partenariat-strategique-co-construire-solution-confiance-europe

[30] http://videos.senat.fr/video.2251670_60761aa01efc4.table-ronde-sur--la-cybersecurite-des-eti-pme-tpe--la-reponse-des-pouvoirs-publics-

[31] Pour plus d'information voir les articles d'E. Jouffin et F. Coupez, *Cloud computing et collecte des données à des fins judiciaires et de renseignement : l'exemple des États-Unis* dans *Cloud Computing, les grands enjeux réglementaires*, Hors-série Banque & Droit, février 2021, pp. 30-36 et A. Bouillé et E. A. Caprioli, *Cloud computing et sécurité numérique* dans *Cloud Computing, les grands enjeux réglementaires*, Hors-série Banque & Droit, février 2021, pp. 23-29.

[32] ABE, Orientations relatives à l'externalisation du 25 février 2019 ; Pour plus de détails : voir l'article de C. Feunteun et D. Rimsevica, *Cloud Act et cloud computing : une menace pour les données ?* Revue de Droit bancaire et financier n° 5, Septembre 2020, dossier 27.