

Preuve
Le Cloud Act à la lumière du projet européen E-evidence

Critiqué pour son extraterritorialité et la menace qu'il fait peser sur le droit à la protection des données personnelles, le Cloud Act repose en fait sur des mécanismes similaires à ceux de la proposition de la Commission européenne d'avril 2018 de règlement «E-evidence».

Le Cloud Act (pour Clarifying Lawful Overseas Use of Data Act) est une conséquence directe de l'affaire Microsoft v. United States. Celle-ci trouve son origine dans un mandat (warrant) exigeant que Microsoft communique aux autorités plusieurs informations associées au compte email d'une personne suspectée de trafic de stupéfiants. La demande était fondée sur le Stored Communications Act (SCA)[1] adopté en 1986 et qui n'envisageait pas à l'époque la situation où les données électroniques pouvaient être accessibles depuis les États-Unis mais stockées sur des serveurs à l'étranger.

La société Microsoft exécuta le mandat concernant les informations stockées sur des serveurs localisés sur le territoire américain mais refusa de divulguer celles stockées dans son data center en Irlande, soulignant qu'il fallait emprunter les voies prévues par les traités d'entraide judiciaire (« *mutual legal assistance treaties* » ou « *MLAT* »). La Cour d'appel du 2nd circuit fit droit en 2016 aux positions de Microsoft[2] et le gouvernement américain décida de porter l'affaire devant la Cour suprême. La position de la cour d'appel combinée à celles en sens contraire d'autres juridictions fédérales de première instance généraient une incertitude pour les autorités susceptible d'entraver l'efficacité des procédures pénales. Le Congrès américain a ainsi adopté le Cloud Act afin de clarifier la portée du SCA, et ce, avant l'issue de la procédure devant la Cour suprême qui a mis fin à l'instance en avril 2018.

Promulgué par le président américain le 23 mars 2018, le Cloud Act donne la possibilité aux autorités américaines d'exiger des prestataires de services électroniques la divulgation de données, et ce, « *whether such communication, record, or other information is located within or outside of the United States* »[3]. Cette dimension extraterritoriale a suscité de nombreuses controverses, certains suggérant qu'elle reflétait une hégémonie américaine dans le domaine numérique. Une analyse attentive du Cloud Act conduit toutefois à nuancer ces critiques d'autant plus qu'il y a quelques similarités entre le Cloud Act et la proposition de la Commission européenne d'avril 2018 de règlement relatif à l'accès aux preuves électroniques en matière pénale (projet de règlement « *E-evidence* »)[4] qui instaure une procédure d'injonction européenne de production et de conservation de données pouvant viser les prestataire offrant des services dans l'Union, et ce, sans avoir à recourir aux procédures MLAT.

Une portée extraterritoriale à reconsidérer

Le Cloud Act précise que les données dont la divulgation est demandée peuvent être situées aux États-Unis ou à l'étranger. Le projet E-evidence n'indique pas que les seules données localisées dans l'UE peuvent être sollicitées et il s'applique dès lors, à l'instar du Cloud Act, aux données que les prestataires stockent aussi à l'étranger. S'il y a une dimension extraterritoriale dans les deux dispositifs, celle-ci mérite d'être nuancée.

Le lieu de stockage des données sollicitées est à l'origine inconnu des autorités. Les données sont fragmentées et dispersées par les prestataires

sur plusieurs serveurs localisés dans des États différents, parfois selon des processus algorithmiques.

Prenons aussi l'exemple de Google qui dispose de huit data centers aux États-Unis, quatre en Europe, deux en Asie et un au Chili(5). Un utilisateur de services e-mail ou cloud Google habitant sur le continent africain, en Inde ou au Brésil ne peut ainsi avoir ses données stockées dans son État de résidence. Un État souhaitant accéder à ces données dans le cadre d'une procédure pénale qui ne présenterait par ailleurs aucun autre élément d'extranéité serait obligé d'activer des procédures MLAT avec plusieurs États si l'on s'en tient au seul critère formel du lieu de stockage des données. Il en découlerait une inégalité entre États difficilement justifiables : ceux sur le territoire desquels sont localisés les serveurs des principaux prestataires de services auraient en pratique davantage la possibilité d'obtenir la communication des données tandis que les autres devraient emprunter des procédures plus longues qui affectent l'efficacité de la justice. De la fracture numérique découlerait donc une fracture juridique.

La territorialité des données est donc le plus souvent déconnectée de la réalité des relations sociales dans le cadre desquelles ces données sont générées et exploitées. Ainsi, il n'y a à l'origine pas d'intention extraterritoriale dans la démarche des autorités consistant à les solliciter. S'il faut avoir à l'esprit les impératifs du Règlement général sur la protection des données (RGDP) qui protègent les données stockées sur des serveurs localisés dans l'UE, ce sont aussi les critères de compétence utilisés par le juge pénal américain ou des Etats membres de l'UE quant à l'infraction poursuivie qui constituent un premier filtre à l'extraterritorialité – par exemple : l'infraction concerne-t-elle des faits s'étant déroulés sur le territoire de cet État ? Concerne-t-elle des ressortissants ou des résidents de cet État ?

Il faut donc distinguer, d'une part, la conduite litigieuse qui fait l'objet des poursuites et qui doit avoir un lien avec l'État exerçant sa compétence pénale et, d'autre part, les données permettant de caractériser les faits constitutifs de l'infraction.

Un champ d'application personnel potentiellement vaste

Le champ d'application personnel du Cloud Act – c'est-à-dire les prestataires visés – demeure encore incertain. L'exposé des motifs fait référence aux « *communications-service providers that are subject to the jurisdiction of the United States* »[6], expression qui selon le Code of Federal Regulations inclut les sociétés instituées en vertu du droit américain ainsi que leurs filiales[7] (donc les géants américains de l'internet que sont Google, Microsoft, Facebook, etc.) mais aussi toute personne (y compris société) « *actually within the United States* »[8]. Si l'on se réfère à la manière dont sont appliqués certains dispositifs extraterritoriaux américains (par exemple en matière de sanction), il n'est pas exclu que les sociétés européennes qui ont une filiale aux États-Unis de même que celles qui n'ont pas de filiales mais qui y conduisent des activités en ciblant le marché américain puissent entrer dans le champ d'application du Cloud Act[9].

La proposition de règlement E-evidence procède de la même démarche. Le texte indique en effet qu'il « *s'applique aux fournisseurs de services qui proposent des services dans l'Union* »[10]. Son champ d'application personnel n'est donc pas limité aux seuls prestataires ayant une société établie dans un État membre. D'ailleurs, en imposant une obligation aux fournisseurs étrangers qui proposent des services dans l'UE d'y désigner un « *représentant légal* » vers lequel les demandes seront dirigées[11], ce dispositif créerait de toutes pièces un élément de rattachement territorial qui n'existait pas à l'origine… permettant ainsi à l'UE de ne pas être taxée d'extraterritorialité !

La possible modération par le juge des effets extra-territoriaux du Cloud Act

Le Cloud Act ne consacre pas un droit unilatéral et immédiat d'accès aux données conservées par les prestataires de services au bénéfice des autorités exécutives américaines et il permet d'intégrer une analyse plus subtile et plus substantielle afin de tenir compte des situations où se déploierait une extraterritorialité qui pourrait être problématique. Les prestataires peuvent en effet s'opposer aux demandes de communication de données, en particulier lorsqu'une telle démarche impliquerait pour eux de se placer en contravention avec les exigences du droit d'un État étranger. Il faut envisager deux situations en fonction de la conclusion ou non d'un accord international sur l'accès aux données avec l'État étranger concerné.

Le Cloud Act donne la possibilité à un prestataire de services de contester dans un délai de 14 jours la demande de communication de données dès lors que celui-ci considère, entre autres, que cette communication « *would create a material risk that the provider would violate the laws of a qualifying government* »[12] – un qualifying government étant défini comme un État ayant conclu un executive agreement avec le gouvernement américain en vertu du Cloud Act[13]. La législation liste les trois conditions qui doivent être réunies par la juridiction américaine :

1. le prestataire est en situation de violer le droit de l'État étranger,
2. l'intérêt de la justice (« *the interests of justice* ») exigent d'annuler ou de modifier la demande des autorités,
3. l'utilisateur concerné qui n'est pas une personne américaine et ne réside pas aux États-Unis[14].

Afin de caractériser cet « *intérêt de la justice* », le Cloud Act mentionne huit éléments15, parmi lesquels : les intérêts de l'État étranger au non-dévoilement de l'information, la probabilité, l'ampleur et la nature des sanctions auxquelles s'exposent les prestataires ou leurs employés, 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, l'ampleur et la nature des liens et de la présence du prestataire avec les États-Unis, et l'importance de l'information sollicitée pour les investigations.

En l'absence d'executive agreement, l'analyse des juridictions américaines ne serait pas fondamentalement différente. D'ailleurs, le Cloud Act indique

que les « *common law standards governing the availability or application of comity analysis* » restent applicables[16]. La comity analysis déclinée dans le Cloud Act se retrouve en effet dans la jurisprudence fédérale précisant que les juridictions doivent tenir compte des principes d'international comity qui exigent « *a particularized analysis of the respective interests of the foreign nation and the requesting nation* »[17]. Les juridictions américaines ont mis en œuvre une analyse multi-factorielle tenant compte notamment des intérêts essentiels des États intéressés par la procédure, de la nature et de l'ampleur des sanctions en cas de divulgation des informations sollicitées, de la mesure dans laquelle la communication requiert une intervention sur le territoire de l'État étranger ainsi que la nationalité de la personne visée dans le cadre de la procédure[18].

La similarité des critères retenus dans le Cloud Act et ceux de la jurisprudence conduit à envisager les règles de droit étranger que le prestataire de services pourrait violer en accédant à une demande de communication de données formulée par les autorités américaines.
Du point de vue du droit français, la loi de blocage du 26 juillet 1968 interdit sous réserve des accords internationaux, la communication « *des documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci* »[19].

Du point de vue du droit de l'UE, outre la directive 2016/943 « *secrets d'affaires* » en cours de transposition, le RGDP constitue un autre dispositif permettant aux prestataires de service de s'opposer aux demandes des autorités américaines. En effet, le RGDP dresse une liste limitative des situations dans lesquelles des données à caractère personnel peuvent être transférées vers un pays tiers. Un transfert de données vers les États-Unis réalisé dans le cadre du Cloud Act ne pourrait être justifié sur le fondement des différents cas prévus par le RGDP. En particulier, il n'y a pas de décision d'adéquation de la Commission (article 45), il n'existe pas de mécanisme conférant aux personnes concernées des garanties appropriées et équivalentes à celles du RGDP (article 46) et le transfert ne serait pas fondé sur un accord international conclu entre l'État tiers et l'UE ou un État membre (article 48). Il n'est aussi pas possible de soulever l'exception de l'article 49(1)(d) autorisant le transfert lorsqu'il « *est nécessaire pour des motifs importants d'intérêt public* » car l'intérêt public visé est celui « *reconnu par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis* » (article 49(4)).

Les risques de conflits d'obligations entre les exigences du Cloud Act et celles du droit français et, surtout, européen ne sont donc pas théoriques pour les prestataires concernés qui s'exposent à des sanctions. Ces risques sont immédiats et sérieux et pourraient être pris en considération par les juridictions américaines dans le cadre d'une comity analysis.

Le règlement E-evidence proposé par la Commission européenne repose sur des considérations similaires. Il envisage la situation dans laquelle le destinataire de l'injonction considère que sa mise en œuvre « *serait contraire aux lois applicables d'un pays tiers interdisant la divulgation des données concernées au motif que cela est nécessaire pour protéger les droits fondamentaux des personnes concernées ou les intérêts fondamentaux du pays tiers en matière de sécurité ou de défense nationales* ». Dans cette hypothèse une procédure « *d'objection motivée* » est prévue et est examinée par la juridiction qui « *évalue s'il existe un conflit, en examinant (a) si la législation du pays tiers s'applique en fonction des circonstances spécifiques de l'affaire en question et, si tel est le cas, (b) si la législation du pays tiers, lorsqu'elle est appliquée aux circonstances spécifiques de l'affaire en question, interdit la divulgation des données concernées* »[20]. Cette évaluation repose sur des critères proches de ceux de la comity analysis des juridictions américaines et aurait pour fonction de tenir compte et si besoin d'atténuer les effets extraterritoriaux du futur règlement E-evidence.

Vers un cadre coopératif UE/États-Unis en matière de preuves électroniques ?

Une mise en œuvre unilatérale du Cloud Act et du projet de règlement E-evidence ne se fera pas sans placer les prestataires dans un conflit d'obligations. Cette question présente un enjeu pour l'efficacité des procédures pénales aussi bien pour les États-Unis que pour les États membres de l'UE qui sollicitent de manière significative les géants américains de l'Internet sans passer par les procédures MLAT. Les parties à la Convention de Budapest sur la cybercriminalité[21] autres que les États-Unis (au sein desquelles les États membres de l'UE) envoient en moyenne 150.000 demandes annuelles aux principaux prestataires de services américains qui communiquent volontairement les informations requises par les autorités judiciaires dans 60% des cas[22].

Le Cloud Act délègue à l'exécutif américain la compétence de conclure des accords internationaux en forme simplifiée permettant aux autorités étrangères de solliciter directement des informations auprès des prestataires américains avec, en contrepartie, de permettre aux autorités américaines de solliciter la communication de données détenues par des prestataires étrangers. La question qui mérite d'être soulevée est de savoir si un executive agreement conclu dans le cadre du Cloud Act est susceptible de satisfaire aux exigences européennes.

Les États-Unis ont entamé des négociations avec le Royaume-Uni à ce sujet avant le Cloud Act[23] mais un accord conclu à l'échelle de l'UE apparaît comme la meilleure option. Le projet E-evidence constitue une opportunité intéressante pour envisager un cadre harmonisé avec les procédures prévues par un futur executive agreement[24].

Celui-ci pourrait s'adosser à l'accord États-Unis/UE sur la protection

des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière[25].

Cet accord – qui n'organise pas l'échange d'informations – s'applique aussi bien aux informations à caractère personnel transférées entre autorités compétentes qu'à celles « *transférées autrement conformément à un accord conclu entre les États-Unis et l'Union européenne ou ses États membres à des fins de prévention et de détection des infractions pénales, dont le terrorisme, d'enquêtes et de poursuites en la matière* »[26].

En définitive, on peut faire au projet E-evidence certains des reproches, souvent excessifs, adressés au Cloud Act. Plutôt qu'une hostilité de principe et finalement improductive, il faudrait davantage envisager ces deux textes comme une opportunité pour l'UE et ses États membres, leur permettant de façonner un futur droit global de l'accès aux preuves numériques qui reste encore à élaborer.

Régis BISMUTH
Professeur à l'École de Droit de Sciences Po

Notes

(1) *18 U.S.C. § 2703.*

(2) *Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016).*

(3) *18 U.S.C. § 2713.*

(4) *Commission européenne, 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 avril 2018.*

(5) *Liste consultable au lien suivant : <https://www.google.com/about/datacenters/inside/locations>.*

(6) *Cloud Act, Sec. 102(2).*

(7) *31 C.F.R. §515.329(c) et (d).*

(8) *31 C.F.R. §515.329(d) et 31 C.F.R. §515.330(a)(2).*

(9) *En ce sens, v. Ron Cheng, « Seizing Data Overseas from Foreign Internet Companies under the CLOUD Act », Forbes.com, 29 mai 2018 (soulignant : « Even before the CLOUD Act, overseas service providers with a presence in the U.S. had to prepare for U.S. law enforcement demands for data, including data that the providers maintained on servers overseas. Now, under the Act, overseas providers will have to consider how much activity they can conduct in the U.S. before being subject to a warrant to turn over data »).*

(10) *Article 3(1) de la proposition de règlement E-evidence.*

(11) *V. l'article 3 de la Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale, COM(2018) 226 final, 17 avril 2018.*

(12) *18 U.S.C. § 2703(h)(2)(ii).*

(13) *18 U.S.C. § 2703(h)(1)(A)(i).*

(14) *18 U.S.C. § 2703(h)(2)(B).*

(15) *18 U.S.C. § 2703(h)(3).*

(16) *Cloud Act, Sec. 6.*

(17) *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa, 482 U.S. 522, 543-544 (1987).*

(18) *V. par exemple, Wultz v. Bank of China Ltd, 910 F.Supp.2d 548 (S.D.N.Y. 2012).*

(19) *Artice 1bis de la loi n° 68-678 du 26 juillet 1968.*

(20) *Article 15(3) de la proposition de règlement E-evidence.*

(21) *Convention de Budapest sur la cybercriminalité, STE n°185, 23 novembre 2001.*

(22) *Comité de la Convention sur la cybercriminalité (T-CY), T-CY(2018)16, 21 mai 2018, p. 6.*

(23) *V. l'audition devant un comité du Sénat de Jennifer Daskal, (24 mai 2017, p. 9, <https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Daskal%20Testimony.pdf>).*

(24) *Sur ces aspects, v. J. Daskal & P. Swire, « A Possible EU-US Agreement on Law Enforcement Access to Data ? », 21 mai 2018, <https://www.lawfareblog.com/possible-eu-us-agreement-law-enforcement-access-data>.*

(25) *JOUE, 10 décembre 2016, L 336/13.*

(26) *Umbrella Agreement, article 3(1).*