L'impact du Cloud Act : orage ou lueur d'espoir ?

Une version anglaise de cet article, rédigée par Frederick T. Davis et Anna R. Gressel, a été publiée dans l'American Bar Association Litigation Journal ("Storm Clouds or Silver Linings? The impact of the U.S. Cloud Act", ABA Litigation Journal, Vol. 45, No 1, Fall 2018).

Debevoise & Plimpton

En mars 2018, le budget américain d'un montant de 1 300 milliards de dollars a été promulgué par le président des Etats-Unis. Noyé au milieu de 2 232 pages, et passé inaperçu aux yeux de presque tous, le *Clarifying Lawful Overseas Use of Data Act* (le "CLOUD Act") pose de nouvelles règles de coopération internationale des autorités pénales aux fins d'obtention de données informatiques stockées à l'étranger. La portée de ces nouvelles règles est considérable.

Le CLOUD Act comble les vides juridiques récemment révélés devant la Cour Suprême des Etats-Unis à l'occasion de l'affaire United States v. Microsoft. Cette affaire avait conduit les Juges de la Cour Suprême à interpréter le *Stored Communications Act* de 1986 ("SCA") à l'aune du progrès technologique constant. La Cour n'a finalement jamais tranché cette affaire, mais l'a classée après que l'adoption du CLOUD Act l'eu vidée de son objet.

Le CLOUD Act apporte des réponses innovantes à certains des défis posés par la technologie dans le cadre des enquêtes pénales. Toutefois, il suscite aussi de nouvelles questions et inquiétudes. La digitalisation (les données étant, pour la plupart, encodées en bits), l'absence de frontière sur Internet, et la globalisation effrénée compliquent, dans les enquêtes pénales transnationales, l'obtention d'informations au moyen des instruments juridiques traditionnels. Le problème de fond est que les données sont parfois stockées dans un pays différent de celui de la personne ou de l'entité qui souhaite y avoir accès.

Dans le cadre des enquêtes menées par les autorités pénales et administratives américaines, les officiers de police, procureurs ou autres ont régulièrement besoin d'accéder à des informations privées détenues par des suspects ou par des tiers. Les procédures dont ils disposent à ce titre sont connues. Tout d'abord, les enquêteurs peuvent obtenir d'une autorité judiciaire locale une assignation (*subpoena*), un mandat (*warrant*) ou d'autres types d'ordonnances. Ensuite, ils doivent la faire signifier dans le respect de la compétence juridictionnelle de l'autorité en question, et ainsi obliger son destinataire à produire les informations ou les faire saisir par une autorité locale.

Le fait que des informations à caractère personnel soient digitalisées (par exemple, des emails et des données financières, telles que des comptes bancaires) ne fait pas obstacle aux procédures traditionnelles d'obtention des informations. Une banque ou une société du secteur des communications peut se voir ordonner de produire une information, quand bien même elle serait stockée sous forme de données informatique. En principe, ce processus est similaire aux procédures d'obtention d'écrits sur support papier ou autre support matériel. Ainsi, ces pratiques assurent-elle la régularité procédurale, la protection de la vie privée, et la transparence.

Cependant, d'autres problèmes se posent lorsque les données recherchées sont physiquement stockées dans une autre juridiction. Dès lors, ce n'est plus seulement la vie privée – et l'équilibre entre les besoins légitimes de l'Etat et les intérêts des individus – mais aussi la souveraineté qui sont en jeu. Quelles lois et procédures s'appliquent à cette situation ? La "déterritorialisation des données" apparaît, pour certains, comme une menace fondamentale pour le principe même de souveraineté.

Le CLOUD Act met en place un régime judiciaire international de demandes transfrontalières des données, comblant ainsi les lacunes du SCA, telles que mise en exergue dans l'affaire Microsoft. Bien que le CLOUD Act ait modernisé certaines règles et procédures, des questions demeurent quant à son champ d'application, la façon dont il sera appliqué au niveau national, et ses conséquences sur les traités d'assistance judiciaire mutuelle (*mutual legal assistance treaties*, "MLAT") existants, ainsi que sur les commissions rogatoires, qui sont les instruments traditionnels de la coopération judiciaire transnationale.

L'Union Européenne élabore actuellement un règlement relatif à ces enquêtes transnationales, qui viendrait concurrencer le CLOUD Act. Cela étant, et compte tenu des limitations applicables aux transferts de données vers des pays tiers posées dans le nouveau Règlement général sur la protection des données ("RGPD"), le CLOUD Act parviendra-t-il à imposer les règles internationales applicables aux enquêtes judiciaires transnationales ?

L'affaire *Microsoft*

L'affaire *Microsoft* était liée à une enquête pour trafic de stupéfiants ; elle a posé la question de la portée extraterritoriale du SCA. En 2013, l'utilisation d'un compte Hotmail pour la commission de l'infraction de trafic de stupéfiants avait constitué un motif suffisant (*probable cause*) pour l'obtention d'un mandat (*warrant*) que les procureurs américains ont signifié à Microsoft. Le mandat (*warrant*), émis en application des procédures prévues par le SCA pour l'accès aux données stockées, enjoignait à Microsoft de produire des emails du suspect.

Microsoft a immédiatement produit des informations relatives au suspect (nom, adresse, etc.) mais a refusé de produire le contenu des emails. En effet, le suspect avait au préalable indiqué, lors de la création de son compte Hotmail, être de nationalité irlandaise. Microsoft avait donc stocké le contenu de ses emails sur ses serveurs dublinois, conformément à sa politique habituelle consistant à stocker les données à proximité de l'utilisateur afin de minimiser le temps de latence entre le stockage et la récupération de ces données.

Microsoft a alors déposé une requête en annulation du mandat concernant ces emails, au motif que le SCA était dépourvu de tout effet extraterritorial et ne pouvait donc pas enjoindre à un prestataire de services de télécommunications américain de produire des données stockées sur le territoire d'une juridiction étrangère. Microsoft prétendait que le procureur devait recourir à un traité d'assistance judiciaire mutuelle ou tout autre moyen autorisant la coopération des autorités irlandaises.

Le tribunal du District sud de New York a ensuite ordonné à Microsoft de s'exécuter, au motif que la révélation au Département de la Justice américaine (*Department of Justice*), par une société américaine, d'informations dont elle a la garde et le contrôle, n'exigeait pas de faire une application extraterritoriale du SCA, ne prenant pas en compte la juridiction dans laquelle les données étaient stockées. Dans son jugement, le tribunal a considéré que Microsoft "contrôlait" les données informatiques localisées en Irlande, car cette société y avait, à tout moment, facilement accès depuis les Etats-Unis. Le tribunal en a alors déduit que la question de l'extraterritorialité du mandat américain ne posait pas véritablement de question juridique, car le mandat (warrant) devait alors être exécuté à l'intérieur des Etats-Unis et qu'aucune démarche nécessaire à son exécution n'avait à être menée à l'étranger.

La Cour d'appel Fédérale a infirmé cette décision et a jugé qu'un mandat émis conformément au SCA ne pouvait pas enjoindre une société de révéler des emails stockés en Irlande. Selon la Cour, la présomption d'absence d'extraterritorialité, posée par la Cour Suprême dans *Morrison v. National Australia Bank*, 561 U.S. 547 (2010), s'applique au SCA, du fait de l'absence de toute indication contraire dans le texte du SCA et dans les travaux parlementaires. La Cour d'appel a ainsi retenu, comme critère d'analyse, le lieu de stockage des données plutôt que le lieu d'accès aux données.

En octobre 2017, la Cour Suprême des Etats-Unis a accepté de se prononcer sur la décision de la Cour d'appel (*certiorari*). Cette affaire, dont les enjeux concernaient à la fois des questions judiciaires et technologiques, et dont l'issue emportait des conséquences pour la vie privée des individus, a été abondamment commentée. Les recours ont donné lieu à un nombre inhabituel de mémoires déposés par des *amici curiae*, et peuvent être regroupés en quatre catégories :

- des parquets, suivant l'avis du Département de la justice américaine, précisaient que le SCA devait être interprété comme permettant d'accéder aux données stockées à l'étranger, dès lors qu'elles étaient accessibles depuis les Etats-Unis ;

- la République d'Irlande et les représentants de l'Union Européenne, ont exprimé leurs préoccupations quant aux atteintes à leur souveraineté, soulignant à de nombreuses reprises que la vie privée est protégée différemment, et généralement plus rigoureusement, en Europe qu'aux Etats-Unis ;

- des sociétés des technologies de l'information et de la communication, ont soutenu Microsoft, soulignant que les données stockées à l'étranger ne devaient pouvoir être appréhendées au moyen de procédures de droit américain ; et

- des ONGs pour la protection de la vie privée ont soutenu qu'il était nécessaire de limiter la portée des mandats émis conformément au SCA afin de prévenir les intrusions transfrontalières dans la vie privée.

L'affaire *Google*

Au cours des procédures d'appel, une autre affaire, similaire en son espèce, est venue compliquer l'affaire *Microsoft*. Un procureur de Philadelphie cherchait à accéder aux emails d'un client de Google (voir *In re Search Warrant No. 16-960-M-01 to Google*). Lorsque la société Google a reçu notification du mandat émis en application du SCA, elle a soulevé les mêmes arguments que Microsoft, selon lesquels elle ne devrait pas être tenue de s'exécuter, dans la mesure où les données relatives aux emails n'étaient pas stockées aux Etats-Unis.

A la différence de l'affaire *Microsoft*, dans laquelle les données étaient localisées de manière permanente sur des serveurs en Irlande, les données de la messagerie de Google étaient divisées en fragments, stockés sur différents serveurs à différents endroits, dont les lieux variaient fréquemment suivant un algorithme permettant de gagner en efficacité. Il s'agissant d'une nouvelle étape sur la voie de la "déterritorialisation" des données, puisqu'aucun endroit de stockage ne pouvait être identifié avec précision et donc qu'aucun pays ne pouvait revendiquer un rattachement à ces données sur la base de leur lieu de stockage. Bien que cette question ait été absente des affaires *Microsoft* et *Google*, un détachement similaire de tout régime juridique résulterait du fait que les données soient stockées dans des satellites ou en haute mer.

Le CLOUD Act

Avec une extraordinaire rapidité, en l'absence de tout débat, et avant que la Cour Suprême des Etats-Unis ne rende sa décision dans l'affaire *Microsoft*, le Congrès des

Etats-Unis a adopté le CLOUD Act, qui a été intégré à la loi de finance promulguée par le Président des Etats-Unis. Cette loi était soutenu à la fois par le Département de la justice américaine et Microsoft, parmi d'autres sociétés de services de communication.

Le CLOUD Act apporte une réponse claire à la question soulevée dans l'affaire *Microsoft*, bien qu'il soulève également de nouvelles interrogations. Si un prestataire de services situé aux Etats-Unis reçoit un mandat émis en application du SCA, il ne peut plus faire valoir que les données informatiques, accessibles depuis les Etats-Unis, ne peuvent pas être obtenues au moyen du SCA au motif qu'elles sont stockées à l'étranger. Le CLOUD Act prévoit ainsi expressément que les données visées par le mandat ou l'assignation, émis conformément au SCA, doivent être "conservées, sauvegardées, ou révélées" par celui qui en a la "possession, la garde ou le contrôle," indépendamment du fait que les données soient localisées à l'intérieur ou à l'extérieur des Etats-Unis.

Les dispositions du CLOUD Act reflètent l'intention univoque du Congrès en faveur de l'application extraterritoriale du SCA, que la Cour d'appel du deuxième Circuit avait rejeté. Ainsi, pour Microsoft comme pour toute autre société américaine de services de communication, la règle est désormais claire – ils doivent révéler toute donnée en leur possession, garde, ou contrôle, quel que soit le lieu de stockage de ces données. Après que le DOJ eut émis un nouveau mandat relatif aux emails stockés en Irlande, et que Microsoft en eut reconnu la validité, la Cour Suprême a classé l'affaire.

Dans la plupart des cas, une société qui se verra signifier une ordonnance lui enjoignant de produire des données devra s'y conformer. S'agissant des quelques affaires qui font intervenir des intérêts étrangers, le CLOUD Act permet aux prestataires de services de contester, par requête, les ordonnances rendues en application du SCA, si les intérêts d'un gouvernement étranger coopérant avec les Etats-Unis sont visés.

Plus précisément, la société peut démontrer qu'elle "croît raisonnablement" que la personne ciblé n'est pas soumise au droit américain et ne réside pas aux Etats-Unis, et qu'il existe un "risque substantiel" (*material risk*) que la révélation d'informations soit exécutée en violation des lois d'un Etat étranger coopératif (*qualifying foreign government* (QFG)) – ce terme sera précisé infra.

Par ailleurs, le CLOUD Act pose des règles innovantes pour l'examen des situations. Si les deux conditions que sont la citoyenneté étrangère du propriétaire des données et le risque substantiel de poursuites judiciaires étrangères sont réunies, alors il peut être décidé que la bonne administration de la justice (*interests of justice*) exige que l'ordonnance soit modifiée ou annulée. Pour la détermination de la bonne administration de la justice , le CLOUD Act introduit un système de reconnaissance juridique mutuel des actes législatifs, exécutifs et judiciaires (*comity analysis*), comprenant sept indicateurs, dont par exemple la nature et la portée des liens des clients

avec les Etats-Unis les Etat étranger coopératifs, et l'importance de l'information pour l'enquête.

En permettant un tel système de reconnaissance juridique mutuel, le CLOUD Act reconnaît expressément, dans certaines limites, que des pays étrangers puissent avoir des intérêts légitimes à s'opposer à la saisine par les autorités américaines des données détenues par leurs citoyens. La « loi de blocage » française (loi n°68-678 du 26 juillet 1968, modifiée par la loi n°80-538 du 16 juillet 1980) pourrait ainsi peut-être constituer une base légale à une telle opposition.

Cependant, le CLOUD Act laisse une autre question en suspens. Alors que tous les prestataires de services établis aux Etats-Unis doivent se conformer au CLOUD Act, celui-ci s'applique-t-il aussi aux prestataires de services établis à l'étranger ? Le CLOUD Act n'apporte pas de solution. On pourrait penser qu'il faille déterminer, pour l'application du CLOUD Act, si le prestataire de services étranger est soumis à la compétence américaine en raison d'activités sur le territoire des Etats-Unis.

Qu'arrivera-t-il, par exemple, si un prestataire de services établi à l'étranger non seulement stocke ses données à l'étranger, ne maintient aucune présence sur le territoire américain et n'y commercialise pas de services de manière régulière ? En raison de l' absence de frontière sur Internet, un client étranger pourrait toutefois accéder à ses emails et les utiliser tout en étant physiquement présent aux Etats-Unis, et ce afin de commettre un crime ou de participer à des activités criminelles ayant des effets sur le territoire américain, justifiant ainsi qu'il fasse l'objet d'une enquête pénale par les autorités américaines.

Si un procureur américain ouvre une enquête et veut accéder aux emails compromettants, il pourrait être confronté à des difficultés s'il soutient que le SCA (même dans sa version amendée par le CLOUD Act) exige que le prestataire de services transfère ses données et que la société, à son tour, soutient qu'elle n'est pas soumise à la compétence des autorités américaines.

Cette question est loin d'être seulement théorique. Etant donné que les potentiels contrevenants peuvent généralement choisir où leurs données sont stockées, ils pourraient être incités à choisir des prestataires de services n'étant pas établis aux Etats-Unis et n'ayant aucune présence sur le territoire américain dans l'espoir que les autorités américaines seront alors incapables d'utiliser à leur encontre les nouveaux moyens de pression mis à disposition par le CLOUD Act. En effet, il est probable que le désavantage compétitif qu'aurait engendré une décision défavorable dans l'affaire Microsoft ait en partie incité l'industrie à soutenir la position de *Microsoft*, en déposant des mémoires en tant qu'*amicus curiae*.

Le CLOUD Act ne traite pas non-plus la situation dans laquelle un prestataire de services américain voudrait faire annuler un mandat ou une assignation lorsqu'il existe un risque de poursuites par les autorités d'un pays qui n'est pas coopératif (QFG). Le prestataire de services pourrait faire valoir que le système de reconnaissance juridique mutuel appliquée en *common law* devrait combler cette lacune, mais un juge pourrait aussi déduire du silence du Congrès américain qu'une interprétation stricte de la loi est à préférable à cette analyse.

Alors que l'affaire *Microsoft* concernait des données informatiques recherchées par les autorités judiciaires américaines, une question distincte mais connexe consiste à se demander si (et comment) des autorités étrangères peuvent accéder aux données stockées aux Etats-Unis ou sous le contrôle d'entités américaines.

Avant le CLOUD Act, le SCA interdisait catégoriquement aux sociétés américaines de révéler des informations, telles que celles contenues dans des emails, aux autorités étrangères. Elles exigeaient donc que ces autorités utilisent les traités d'assistance judiciaire mutuelle et autres instruments pertinents. Si une autorité étrangère avait émis une ordonnance enjoignant à Microsoft de révéler le contenu d'emails d'une personne de droit américain, cette société aurait pu être confrontée à un choix cornélien : enfreindre la loi américaine ou enfreindre la loi étrangère. En pratique, les autorités étrangères transmettaient généralement les requêtes au gouvernement américain au moyen d'un traité d'assistance judiciaire mutuelle ou d'une commission rogatoire, de manière à ce que les autorités américaines puissent saisir des données pour le compte des autorités étrangères.

Bien que les procédures des commissions rogatoires et traités d'assistance judiciaire mutuelle soient généralement efficaces, les délais peuvent être longs, quand bien même les requêtes seraient urgentes. Afin d'encourager la coopération internationale et, se faisant, étendre la portée de l'autorité américaine, le CLOUD Act institue un système alternatif pour les demandes de données aux fins d'application des lois étrangères.

Il permet ainsi à certains gouvernements étrangers de conclure des accords bilatéraux (*executive agreements*) avec les Etats-Unis, afin d'être reconnus comme des Etats étrangers coopératifs (QFC). Ces Etats étrangers sont alors autorisés à signifier directement des requêtes, pour l'obtention d'information en vue de l'application de lois étrangères, directement aux entités américaines, plutôt que de passer par l'intermédiaire du gouvernement des Etats-Unis.

Le CLOUD Act supprime expressément les interdictions prévues dans le SCA en ce qui concerne les révélations directes à la demande des Etats étrangers coopératifs. Il permet – mais n'oblige pas – les sociétés américaines auxquelles sont signifiées des ordonnances

émises par des autorités étrangères de transmettre leurs données à ces Etats étrangers coopératifs sans crainte de sanctions.

Afin d'être reconnu comme coopératif, un gouvernement étranger doit, en application du CLOUD Act, conclure un accord bilatéral. Pour ce faire, l'Avocat général du Département de la justice américaine (*Attorney General*) doit, avec le concours du Ministre des affaires étrangères américain (*Secretary of State*), déclarer au Congrès que le gouvernement étranger remplit un certain nombre de critères, par exemple qu'il *"apporte de protections procédurales solides et substantielles pour la vie privée et les libertés publiques"* et que des procédures *"adéquates"* garantissent la protection des données relatives aux sujets de droit américain s'agissant de la rétention, de l'acquisition, et de la diffusion de ces données.

Le CLOUD Act prévoit une procédure accélérée d'une durée de 180 jours au cours desquels le Congrès américain peut empêcher un accord bilatéral d'être conclu. Les certifications doivent être renouvelées tous les cinq ans, et le Congrès peut, de nouveau, à chaque certification, empêcher le renouvellement de l'accord en votant une résolution (*joint resolution*) le dénonçant.

Les dérogations qui permettent aux autorités étrangères de signifier des ordonnances directement aux entités américaines sont limitées aux ordonnances sur des infractions graves, dont le terrorisme ; celles qui ciblent une personne en particulier, un compte, ou un autre identifiant objet de l'ordonnance ; celles qui sont motivées par *"des faits clairs et crédibles, en particulier la légalité et la gravité du comportement faisant l'objet de l'enquête"* ; et, dans le cas de l'interception de communications télégraphiques et électroniques, celles qui sont assorties d'une durée déterminée et limitée à ce qui est raisonnablement nécessaire, et sont émises uniquement si les informations ne peuvent être obtenues par un moyen moins intrusif.

Aussi, l'ordonnance d'un Etat étranger coopératif doit être conforme au droit interne étranger, ne peut porter atteinte à la liberté d'expression, ou viser une personne de droit américain.

Sans surprise, compte tenu de la rapidité avec laquelle le CLOUD Act a été rédigé, celui-ci ne traite pas de manière exhaustive le fonctionnement pratique des accords exécutifs. Par exemple, le CLOUD Act ne prévoit aucune procédure de contestation des ordonnances signifiées par les Etats étrangers coopératifs (QFG) devant les tribunaux américains. Cela peut paraître surprenant, dans la mesure où le CLOUD Act limite expressément les situations dans lesquelles un Etat étranger coopératif peut directement notifier une ordonnance à une entité américaine. Un mécanisme interne permettant de garantir que le respect des conditions légales serait judicieux.

De plus, le CLOUD Act prévoit que *"le Gouvernement des Etats-Unis se réserve le droit de rendre* [un accord bilatéral] *inapplicable à toute ordonnance dès lors* [qu'il] *considère que l'accord ne peut pas être invoqué à bon droit*". Bien que cela autorise le pouvoir exécutif à intervenir dans les affaires des autorités judiciaires à chaque fois qu'il considère une requête d'un Etat étranger coopératif comme abusive, le CLOUD Act ne précise pas les effets d'une telle intervention.

Les réactions au CLOUD Act sont ambivalentes. Elles vont du soutien le plus enthousiaste à la critique la plus sévère. Les autorités judiciaires soutiennent que le CLOUD Act a résolu les problèmes soulevés par la Cour d'appel du deuxième Circuit dans l'affaire *Microsoft*. Les sociétés de services espèrent que les accords exécutifs du CLOUD Act limiteront les situations dans lesquelles elles sont contraintes de choisir entre enfreindre le droit américain et enfreindre le droit étranger. Autorités et entreprises pensent que le processus de transfert de données prévu par le CLOUD Act est plus simple que le précédent système des traités d'assistance judiciaire mutuelle, et que les procédures du CLOUD Act permettant aux Etat étrangers coopératifs d'obtenir des informations directement auprès des sociétés permettra de contourner les lois qui contraignent à localiser les données au sein d'une juridiction donnée et sont par conséquent attentatoires à la vie privée.

Par ailleurs, certains défenseurs de la vie privée tels que le syndicat américaine *American Civil Liberties Union* et la fondation américaine *Electronic Frontier Foundation* ont manifesté leurs préoccupations quant au fait que le CLOUD Act ne protège pas convenablement la vie privée des personnes physique. En effet, il permet notamment le transfert de données sur la base d'un critère peu exigeant et dont la portée semble plus large que le simple motif suffisant (*probable cause*). Certains auteurs ont toutefois suggéré que le choix du nouveau critère a été motivé par la volonté d'inclure des critères appliqués dans des juridictions étrangères, dont les formulations peuvent varier. En effet, la procédure de certification permet d'assurer que les critères appliqués sont adaptés.

Aussi, des organisations telles que le *Human Rights Watch* ont fait part de leur inquiétude quant au fait que des pays présentant de faibles garanties en matière de droits de l'homme puissent néanmoins être reconnus comme coopératifs et ainsi avoir largement accès à des données individuelles.

L'avenir ?

Plus généralement, le CLOUD Act représente une première étape dans ce qui pourrait être un changement de paradigme en matière de régulation de l'accès aux données digitales. Les décisions *Microsoft* reposent sur le postulat que les données sont localisées en des lieux spécifiques, et que ces lieux sont pertinents pour déterminer si un gouvernement a le pouvoir d'ordonner leur révélation. Microsoft et l'Irlande ont affirmé

que l'Irlande avait un intérêt à protéger la vie privée des citoyens irlandais et, dans la mesure où les données étaient en l'espèce localisées sur le territoire, ont comparé la production forcée de données informatiques à une invasion du territoire irlandais.

Les arguments du Département de la justice américaine concernaient tout autant la localisation des données, bien qu'il soutenait que le lieu de révélation - au sein des Etats-Unis - et non du stockage des données - en Irlande - devait permettre de déterminer si Microsoft pouvait être contraint de les produire, en l'absence d'application extraterritoriale du SCA.

En permettant expressément l'application extraterritoriale du SCA, le CLOUD Act nie la pertinence du lieu de stockage des données informatiques et, en revanche, s'intéresse à *l'accès* à ces données. Un prestataire de services soumis à la juridiction des Etats-Unis peut désormais être contraint de transférer les données qui sont en sa "*possession, garde ou contrôle*", indépendamment du lieu de stockage de ces données.

Toutefois, le CLOUD Act n'a pas tout à fait anticipé la nature évolutive du stockage et de la protection des données. Des questions quant à son application pratique restent sans réponses.

La nouvelle loi semble répondre à la problématique du stockage dynamique des données, c'est-à-dire le fait que les serveurs sur lequel les données sont stockées changent de manière quasi constante, tel que dans l'affaire *Google*. Ces données n'étant pas localisées en un lieu fixe, l'applicabilité des procédures du SCA demeurait incertaine. Désormais, de telles données peuvent faire l'objet de mandat (*warrants*) et assignations (*subpoenas*) des autorités américaines à condition qu'elles soient accessibles depuis les Etats-Unis.

Le stockage dynamique des données complique toutefois le système de reconnaissance juridique mutuel accordées aux Etats étrangers coopératifs (QFG) ayant conclus des accords en application en CLOUD Act. Il a été expliqué qu'un prestataire de services américain qui se verrait signifier une ordonnance par une autorité étrangère pourrait introduire une requête en annulation ou réformation si, entre autres, les lois nationales de l'Etat étranger coopératif (QFG) sont concernées. Mais il convient alors de déterminer si les lois de l'Etat étranger s'appliquent bien aux données, ce qui pourrait ne pas être le cas si seul un "fragment" de donnée informatique a été stocké dans le pays étranger, ou si les données n'ont été stockées en ce lieu que pendant un temps très bref, avant d'être déplacées.

Pour répondre à cette question, les tribunaux devraient appliquer le droit de l'Etat étranger coopératif (QFG), qui pourrait apporter une solution claire au problème. Le droit européen, par exemple, est relativement univoque. Conformément au RGPD, les données collectées au sein de l'Union Européenne sont considérées comme étant des

données européennes indépendamment du lieu de stockage. Il reste cependant à voir si les lois de tous les Etats qui concluent des accords avec les Etats-Unis en application du CLOUD Act permettront d'apporter de telles solutions.

Par ailleurs, certains prestataires de services pourraient chercher à échapper à la portée du SCA pour obtenir un avantage concurrentiel auprès des consommateurs, soucieux de la protection de leur vie privée. Ils pourraient pour cela éviter toute présence aux Etats-Unis ou avoir recours à des technologies visant à empêcher le gouvernement américain de pouvoir accéder aux données relatives à leur clientèle.

Par exemple, certaines sociétés proposent des technologies de cryptage intégral grâce auxquelles personne – pas même le prestataire de services – ne peut accéder aux données sans la clef de déchiffrage conservée par le client. La compatibilité du cryptage et la crainte que les autorités de contrôle refusent de communiquer sur cette question du fait de la facilité d'accès à ces technologies, soulèvent encore d'autres problèmes.

Dans une récente affaire, qui ne concernait pas l'application du SCA, le FBI a ordonné à Apple de décrypter l'iPhone d'un suspect dans le cadre d'une enquête en matière de terrorisme. Apple a refusé de s'exécuter, soutenant qu'elle n'avait pas la clef permettant de déverrouiller le téléphone. Le FBI a alors ordonné à Apple de développer un programme qui permettrait de dépasser cette barrière technologique. Finalement, le FBI ayant accédé aux données du téléphone par d'autres moyens, l'affaire est devenue sans objet.

Les pays étrangers peuvent aussi prendre des mesures pour protéger les données collectées sur leur territoire ou réputées avoir un intérêt pour les citoyens. Certains pays envisagent d'adopter une obligation de stockage national des données, selon laquelle toute donnée relative à un service offert au sein du pays doit être stockée à l'intérieur de ce même pays.

Une autre option consisterait à rendre obligatoire l'utilisation d'intermédiaires de confiance (*data trusts*), pour lesquels le droit local national pourrait prévoir que les données informatiques relatives aux services de communication à destination des citoyens d'un pays ne sont pas stockées par le prestataire de services, mais automatiquement transférées à un intermédiaire de confiance— qui répondrait du gouvernement — pour le stockage des données sur des serveurs indépendants. Dans cette relation, si le prestataire de services est visé par une procédure prévue par le SCA aux fins de révélation de certaines données, il pourrait probablement soutenir n'avoir ni la possession, ni la garde, ni le contrôle des données, mais que l'intermédiaire de confiance les aurait, et que, conformément au droit national local, ce dernier peut en refuser tout accès qui ne serait pas conformes aux lois et procédures locales.

Au niveau international, les réactions au CLOUD Act sont mitigées. Le gouvernement britannique a exprimé son soutien. Etant donné que 90% des suspects visés par les autorités britanniques utilisent des services de communication américains, le CLOUD Act pourrait considérablement simplifier les enquêtes menées par ces mêmes autorités.

A l'inverse, au cours de l'affaire *Microsoft*, des représentants de l'Union Européenne ont déposé un mémoire en tant qu'*amicus*, affirmant que l'application extraterritoriale du SCA par les autorités américaines, sans prendre en compte les lois étrangères, porterait atteinte à leur souveraineté. Les représentants de l'Union ont aussi soutenu que les dispositions du SCA relatives aux révélations forcées pourraient contrevenir à l'Article 48 du RGPD. En effet, le RGPD pose une interdiction de principe de transférer des données européennes à l'extérieur de l'Union, et prévoit des exceptions (ou "dérogations") autorisant certains transferts. Ces dispositions du RGPD renforcent les protections accordées aux consommateurs et pourraient compliquer la conclusion par les Etats membres de l'Union avec les Etats-Unis d'accords bilatéraux prévus par le CLOUD Act.

Bien que certaines des dérogations à l'Article 48 puissent peut-être permettre à un prestataire de services de répondre aux demandes des autorités américaines sans enfreindre le RGPD, l'application de ces dérogations aux requêtes prévues par le CLOUD Act est incertaine. Notamment, un Etat étranger coopératif (QFG) qui conclut un accord bilatéral doit reconnaître aux Etats-Unis des *"droits réciproques d'accès aux données"*. Il peut en être déduit que, de la même manière, que l'Etat étranger serait autorisé à adresser directement des requêtes aux sociétés américaines conformément au CLOUD Act. Les autorités américaines pourraient alors directement adresser des ordonnances aux sociétés soumises à la juridiction de cet Etat étranger.

La substance de ces droits réciproques sera en définitive déterminée par chacun des accords bilatéraux, mais il pourrait être difficile pour les Etats membres de l'Union, pris individuellement, d'accorder de tels droits aux autorités américaines eu égard au RGPD. En effet, les Etats membres ne sont pas autorisés à garantir moins de protections que celles exigées par le RGPD. Cela rend difficile, pour un Etat membre, de garantir unilatéralement que les transferts de données réalisés au titre des accords bilatéraux du CLOUD Act soient permis par dérogations au RGPD.

Il est essentiel de noter qu'un accès si large aux données européennes par les autorités américaines pourrait simplement leur être refusé, étant donné les nécessités de protection européenne du droit à la vie privée des individus.

Ainsi, il reste à voir si le CLOUD Act renouvellera le modèle international pour les demandes d'information transfrontalières aux fins d'application du droit, ou bien si sa portée se limitera aux problèmes soulevés par l'affaire *Microsoft*.

Tout indique que le Royaume-Uni conclura avec les Etats-Unis, en application du CLOUD Act, un accord bilatéral peu après sa sortie de l'Union Européenne. L'impact du CLOUD Act en Europe continentale est, quant à lui, plus incertain ; alors que les Etats-Unis y sont devenus le premier acteur, et que l'approche américaine de la protection des données personnelles diffère radicalement de la vision européenne, il ne peut être considéré comme acquis que l'Union Européenne acceptera le CLOUD Act comme base d'un nouveau régime international protection des données.

En effet, l'Union Européenne envisage actuellement l'adoption du Règlement e-*Evidence*, similaire au CLOUD Act. Ce Règlement exigerait que les sociétés étrangères nomment un représentant légal au sein de l'Union Européenne, qui pourrait donner accès aux données stockées en dehors de l'Union dans un délai de dix jours suivant la requête, ou six heures en cas d'urgence. Le Règlement s'appliquerait aux sociétés — par exemple, Facebook et Google — qui offrent des services au sein de l'Union Européenne et qui ont un "lien substantiel" avec l'Union Européenne, c'est-à-dire des sociétés qui ont un établissement dans un pays de l'Union, ou qui fournissent des services à un large nombre d'utilisateurs dans un pays européen.

En pratique, cela étendrait l'autorité de l'Union Européenne, qui pourrait enjoindre de révéler des données détenues en dehors de l'Union Européenne, de manière similaire au CLOUD Act dans son application extraterritoriale.

Il reste aussi à observer comment le CLOUD Act et le RGPD évolueront et interagiront. L'Union Européenne a le pouvoir de négocier au nom de tous ses Etats membres. A ce stade, celui des deux modèles – RGPD ou Cloud Act – qui pourrait finir par s'imposer reste débattu.

Une chose est certaine : la situation est précaire et continuera à évoluer. Dans la vie des affaires comme dans la vie privée, les données informatiques sont essentielles. Celles-ci n'ont plus de lien évident ou intuitif avec un territoire identifiable, dont il serait attendu que les lois régulent l'accès, tout en protégeant les intérêts des personnes et des activités.

Au niveau national, il peut être attendu que les garanties constitutionnelles en matière de vie privée évolueront, dans une certaine mesure, avec la technologie. En juin 2018, la Cour Suprême des Etats-Unis, dans l'affaire Carpenter, a jugé pour la première fois que l'accès *ad hoc* du gouvernement, en application du SCA, aux métadonnées d'un téléphone portable - qui ne révèlent pas le contenu des communications, mais des faits objectifs tels que des lieux et identités - peut être soumis aux exigences du Quatrième Amendement, en dépit du fait que les données étaient en l'espèce détenues par un tiers.

Cependant, au niveau international le problème reste plus complexe. Au fur et à mesure où les données deviennent à la fois mondialisées et "déterritorialisées", la position de

chaque pays quant à la façon de répondre aux besoins des enquêteurs tout en protégeant la vie privée doit de plus en plus prendre en compte les lois et les intérêts des autres pays.

Le CLOUD Act le montre, la coopération internationale pour la régulation de l'accès aux données est la réponse au problème.

Antoine F. Kirry
+33 1 40 73 12 35
akirry@debevoise.com

Frederick T. Davis
+33 1 40 73 13 10
ftdavis@debevoise.com

Alexander Bisch
+33 1 40 73 13 37
abisch@debevoise.com

Anna R. Gressel
+1 212 909 6485
argressel@debevoise.com