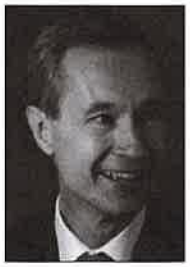

Par Gilles Kolifrath, avocat,

et Eric David, avocat, Kramer Levin

Quelques propos de démystification sur le Cloud Act

Qu'on ne s'y méprenne pas, le Cloud Act, adopté par le Sénat américain le 6 février 2018, n'a pas vocation à réglementer les activités de cloud. Cet acronyme trompeur devient davantage compréhensible lorsque l'on sait qu'il s'agit du Clarifying Lawful Overseas Use of Data Act. Reste que sa portée n'a rien à voir par exemple avec le programme Echelon[1]. Le Cloud Act amende le titre 18 du US Code consacré aux règles fédérales en matière pénale et de procédure pénale et plus particulièrement le chapitre 21 de ce titre consacré à l'accès aux données communiquées ou stockées par des prestataires IT, accès en principe interdit aux tiers. Le Cloud Act a donc pour objet de renforcer l'accès aux données électroniques détenues par les prestataires IT en dehors des Etats-Unis (on retrouve ici un lien avec le cloud...), lorsqu'il s'agit de lutter, et donc de poursuivre, les crimes. Si le Cloud Act vise expressément le terrorisme, il ne s'agit pas de la seule forme de criminalité visée.

D'ailleurs, le Cloud Act a été adopté suite à un arrêt d'une cour d'appel de New York faisant droit aux demandes de Microsoft visant à l'autoriser à refuser de communiquer aux autorités de poursuites des données stockées en Irlande concernant un ressortissant non américain poursuivi pour une affaire de stupéfiants. Nul doute que les infractions des cols blancs sont également concernées. Au regard des grandes affaires de corruption ou de sanctions financières internationales qui opposent parfois les Etats-Unis et l'UE, on comprend les interventions multiples, et en dernier lieu celle du ministre de l'Economie devant l'Assemblée nationale le 15 janvier 2019, déclarant que «Nous sommes en train, avec le Premier ministre, de travailler à un dispositif de protection des données stratégiques de nos entreprises pour qu'elles ne puissent pas être récupérées par l'administration américaine ou par la justice américaine sans qu'elles soient averties». Il s'agit donc d'empêcher que les autorités des Etats-Unis puissent, à l'occasion de la lutte contre les infractions économiques et financières commises par les entreprises, accéder à des données stratégiques, voire d'ériger un obstacle à l'application extraterritoriale du droit américain (comme par exemple s'agissant des sanctions mises en place par les Etats-Unis à l'encontre des investisseurs en Iran).

Un nouvel article (§ 2713) permet d'accéder aux données lorsqu'elles sont stockées dans un Etat qui a conclu un executive agreement avec les Etats-Unis ou dont la législation permet un tel accès.

Ces craintes affichées sont-elles pour autant justifiées?

Le Cloud Act rappelle qu'il est avant tout une réponse aux problèmes rencontrés dans les investigations internationales. En

effet, la coopération internationale se traduit par la mise en œuvre de traités internationaux (MLAT pour Multi Legal Assistance Treaty) qui prévoient des mécanismes de coopération contraignants. Mais une réponse unilatérale, comme le Cloud Act, à l'insuffisante coopération internationale est délicate, spécialement lorsqu'elle vient des Etats-Unis, taxée d'impérialisme. La plupart des Etats adoptent cependant des législations dites «à portée extraterritoriale», comme le devoir de vigilance ou le RGPD.

Le Cloud Act dresse donc le constat que le Chapitre 21 susvisé peut empêcher la communication de données nécessaires à des investigations pénales à l'étranger et inversement. Pour répondre à cette difficulté, le Congrès a décidé d'autoriser un accès aux données dans le cadre d'enquêtes criminelles. Cet accès est conditionné et soumis au contrôle du juge américain (1). Cet accès s'insère cependant essentiellement dans un cadre de coopération internationale puisqu'il suppose le plus souvent la signature préalable d'un executive agreement avec l'Etat tiers dont le cadre juridique a été précisément déterminé (2).

1. Un accès aux données sous conditions et sous contrôle du juge

Un nouvel article (§ 2713) a été introduit dans le Titre 18. Il permet d'accéder aux données lorsqu'elles sont stockées dans un Etat qui a conclu un executive agreement avec les Etats-Unis ou dont la législation permet un tel accès. Le prestataire IT peut cependant saisir un juge afin d'être autorisé à refuser un tel accès. Il convient donc de noter que seul ce prestataire peut s'opposer et non pas la personne faisant l'objet d'investigations (dont elle peut d'ailleurs ignorer l'existence) ou le client du prestataire IT dont les données vont être rendues accessibles. Ainsi, ces personnes ne pourront aucunement s'opposer à l'accès ou engager la responsabilité du prestataire IT, ni contester la légalité de l'accès aux données, si le prestataire IT décide de faire droit à la demande de communication des autorités de poursuite.

Pour s'opposer, le prestataire IT doit saisir le juge dans les 14 jours de la demande d'accès. Ce droit d'opposition n'est cependant ouvert que dans l'hypothèse de l'application d'un executive agreement. Après avoir pris connaissance des observations des autorités de poursuite, le juge rejette ou modifie la demande si les trois conditions cumulatives suivantes sont satisfaites :

- l'accès viole la loi de l'Etat tiers ;
- les circonstances de l'espèce conduisent à conclure que les «intérêts de la justice» imposent le rejet ou la modification de la demande d'accès, et
- la personne (physique ou morale) ayant recours aux services du prestataire IT n'est pas résident ou citoyen des Etats-Unis ou une société de droit américain (et ses filiales étrangères).

L'accès aux données est donc conditionné à ce que l'Etat tiers ait conclu un executive agreement avec les Etats-Unis ou dispose d'une législation autorisant un tel accès.

Les «intérêts de la justice» doivent être appréciés au regard des intérêts des Etats-Unis (notamment s'agissant de l'investigation), des intérêts de l'Etat tiers (notamment s'agissant de l'opposition à la demande d'accès), du risque de sanction (et sa gravité) pour le prestataire IT si l'accès conduit à ce qu'il viole la loi de l'Etat tiers, du domicile ou de la nationalité du client du prestataire IT, des liens du prestataire IT avec les Etats-Unis (notamment présence d'un établissement sur le sol américain ou non), de l'importance de l'accès aux données pour le succès des investigations, de la possibilité de procéder à un accès moins impactant pour les parties concernées et, lorsque les autorités américaines agissent sur demande de l'Etat tiers, de l'intérêt pour cet Etat. Cette grille d'analyse n'est pas sans rappeler la rule of reason et reprend notamment la première condition dont l'importance est donc relativisée. Le pouvoir discrétionnaire du juge américain est dès lors très important et nul doute que la cour suprême sera amenée à se prononcer sur le test opéré par les juges.

La troisième condition pour que le juge s'oppose à l'accès aux données tel que demandé est donc liée à la nationalité du client du prestataire IT. Ce client doit être américain. Cela signifie néanmoins que des poursuites pourraient être mises en œuvre à l'encontre d'une personne (physique ou morale) non américaine dès lors que des communications ont eu lieu avec une personne résidant ou citoyenne des Etats-Unis et que les données sont stockées par un prestataire IT ayant un lien avec les Etats-Unis. Ainsi, une société non américaine dont le droit n'interdirait pas l'application du Cloud Act et qui est en contact avec une personne des Etats-Unis a intérêt à conclure des stipulations contractuelles interdisant à cette dernière de stocker des données chez un prestataire IT ayant un lien avec les Etats-Unis, sous peine de s'exposer à une demande fondée sur le Cloud Act dans le cadre d'une investigation américaine. Le Cloud Act peut donc, par exemple, avoir pour effet de porter atteinte à l'activité économique de Google Cloud qui peut apparaître, pour cette raison, moins attractive.

Une société non américaine dont le droit n'interdirait pas l'application du Cloud Act et qui est en contact avec une personne des Etats-Unis a intérêt à conclure des stipulations contractuelles interdisant à cette dernière de stocker des données chez un prestataire IT ayant un lien avec les Etats-Unis.

Durant la procédure d'examen par le juge, le prestataire IT peut refuser, à titre provisoire, de faire droit à la demande d'accès sauf si le juge considère qu'il y a un risque :

- pour l'intégrité physique d'une personne physique,
- de fuite de la personne visée par l'enquête,
- de destruction ou d'altération de preuves,
- d'intimidation d'un témoin potentiel, ou
- d'obstacle ou de retard indu de la procédure.

La probabilité que l'un de ces risques soit considéré comme

avéré est donc très élevée. Le juge devrait dès lors contraindre le prestataire IT à se soumettre à la demande d'accès à titre provisoire, quitte à annuler les opérations d'accès par la suite s'il juge que le Cloud Act s'oppose à l'accès aux données opéré.

2. Une facilitation de la coopération internationale

Le Cloud Act dispose qu'un prestataire IT est habilité à exécuter une injonction d'octroyer l'accès aux données d'un Etat ayant conclu un executive agreement avec les Etats-Unis. Il ne s'agit donc plus d'une infraction au chapitre 21 susvisé.

Un nouvel article (§ 2523) est introduit au chapitre 119 du Titre 18 afin d'encadrer les conditions de signature d'un executive agreement. Ainsi, l'Attorney General et le Secretary of State doivent faire approuver par le Congrès tout executive agreement. A cette fin, l'exécutif américain doit démontrer que le système juridique de l'Etat tiers offre toutes les garanties de fond et de procédure quant à la vie privée et les libertés civiles. Le Congrès a tenu à préciser que cette démonstration doit s'appuyer sur des éléments pertinents et étayés. Plus précisément, l'Etat tiers doit disposer d'un arsenal juridique de fond et de procédure :

- contre la cybercriminalité et contenant des dispositions relatives aux preuves électroniques, notamment en ayant ratifié la Convention sur la cybercriminalité de Budapest en date du 23 novembre 2001 ou, à tout le moins, en respectant les règles définies aux chapitres I et II de cette convention (mesures à prendre au niveau national) ;
- garantissant l'Etat de droit et le principe de non-discrimination ;
- garantissant le respect des droits de l'homme tels que : la protection contre l'arbitraire et le respect de la vie privée ; le droit à un procès équitable ; la liberté d'expression ; l'interdiction des arrestations et détentions arbitraires ; l'interdiction de la torture et des traitements dégradants ; l'existence de règles déterminant précisément les conditions d'accès aux données, notamment la transparence de l'accès du gouvernement national aux données ; la liberté d'Internet.

L'Etat tiers doit avoir adopté des règles limitant l'accès aux données des ressortissants des Etats-Unis. De même, ces derniers ne doivent pas être visés par les investigations. Cette discrimination s'explique par la volonté des Etats-Unis de préserver leur juridiction sur leurs ressortissants. Mais cette restriction pourrait être contournée, notamment en engageant des poursuites à l'encontre d'une société des Etats-Unis à l'issue d'une procédure à l'encontre d'une société non américaine dont la responsabilité aurait été établie grâce au Cloud Act. L'Etat étranger pourrait alors poursuivre l'entreprise américaine dont la responsabilité serait également engagée, par exemple, en qualité de co-auteur ou de complice.

Seules les infractions les plus graves (notamment le terrorisme) doivent permettre le recours à un executive agreement. En outre, la demande d'accès doit viser limitativement une (des) personne(s), un compte, une adresse, etc. Elle doit également être limitée dans le temps et, plus généralement, être strictement proportionnée.

La demande d'accès doit pouvoir faire l'objet d'un contrôle juridictionnel. En outre, les éléments obtenus par le gouvernement étranger doivent être conservés sur un système sécurisé et communiqués aux seules personnes en charge ou en lien avec les investigations. Le gouvernement étranger doit également donner l'accès aux données au gouvernement américain si elles sont relatives à des infractions commises au préjudice des Etats-Unis ou d'une personne américaine et ce, afin de permettre l'exercice de la souveraineté américaine. L'absence de consécration d'une portée universelle au principe ne bis in idem ne protège cependant pas l'auteur de l'infraction de multiples poursuites.

Le Cloud Act dispose qu'un prestataire IT est habilité à exécuter une injonction d'octroyer l'accès aux données d'un Etat ayant conclu un executive agreement avec les Etats-Unis.

On le voit, les mythes entourant le Cloud Act sont nombreux. Loin d'être l'expression d'un imperium américain, la réponse des Etats-Unis à la question de l'accès aux preuves électroniques des infractions les plus graves n'est en réalité pas unilatérale (ce qu'elle ne pouvait d'ailleurs pas être). Cette nécessaire prise en compte des Etats tiers se confirme au regard de la loi de blocage française de 1968 ou, plus récemment, de l'article 48 du Règlement général sur la protection des données (RGPD)[2]. Cet article prévoit qu'un prestataire IT soumis au RGPD ne peut être contraint à permettre l'accès aux données qu'il traite pour le compte de ses clients/utilisateurs qu'en présence d'un accord international, c'est-à-dire d'un executive agreement au sens du Cloud Act. On suivra donc attentivement l'évolution des négociations entre les Etats-Unis et l'Union européenne à cet égard. ■

1. «Echelon est un nom de code utilisé pendant de nombreuses années par les services de renseignements des Etats-Unis pour désigner une base d'interception des satellites de télécommunications commerciaux» (Wikipedia).
2. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JOUE, n° L119 du 4 mai 2016, p. 1.