Compte - rendu de la confcall de l'AFCDP sur le CLOUD Act

Ceci est le compte-rendu de la confcall du 28 juin 2018 de l'AFCDP : « CLOUD Act : une confcall pour essayer de comprendre... » avec Me Olivier Iteanu et Me François Coupez, Avocats à la Cour, et animée par Pascale Gelly, Vice-présidente de l'AFCDP en charge des relations internationales.

Pascale Gelly : Bonjour à tous et bienvenue dans cette Confcall de l'AFCDP. Aujourd'hui, François Coupez et Olivier Iteanu, Avocats à la Cour, vont nous apporter leurs éclairages sur le *Clarifying Lawful Overseas Use of Data Act*, le « CLOUD Act ».
Cette conférence est enregistrée et ré-écoutable pendant 3 mois [jusqu'au 28 septembre 2018]. Il ne sera pas possible de poser des questions lors de la conférence, mais cela pourrait être fait ultérieurement sur notre forum, Agora.

Rentrons dans le vif du sujet : de quoi s'agit-il ? Et que change ce texte par rapport à la situation actuelle ?

Olivier Iteanu : Pour commencer, pourquoi « *Clarifying* » ? Jusqu'à présent, les effets extra-territoriaux de la loi américaine étaient contestés par certains acteurs, je pense en particulier à Microsoft qui refusait le rapatriement de courriel stocké sur des serveurs irlandais, dans une affaire de droit commun. Le CLOUD Act met fin à ce genre de litige en clarifiant les conditions d'application de l'extra-territorialité.

Ce Cloud Act ajoute à l'US Code, dans une section dans laquelle on retrouve des dispositions issues de l'USA Patriot Act (devenu depuis Freedom Act, suite à un « coup marketing » sous l'administration Obama), une disposition très claire : « *A provider of electronic communication services* [« fournisseur de services de communication électroniques », i.e. les opérateurs de communications électroniques plus un certains nombres d'autres acteurs qui peuvent fournir des accès à un service de communication, comme un WiFi public] *or remote computing service* [le cloud computing, les fournisseurs de service informatique à distance] *shall comply with the obligations of this chapter to preserve, backup, or disclose the contents* [donc pas uniquement les métadonnées, mais aussi les contenus] *of a wire or electronic communication and any record pertaining to a customer or subscriber within such provider's possession regardless of whether such communication, record, or other information is located within or outside of the Unites States* » . Voilà ce que clarifie ce texte : quel que soit le lieu de stockage de ces « records » ou « contents », les acteurs concernés doivent communiquer l'ensemble de ces données.

François Coupez : Le CLOUD Act clarifie effectivement les éléments. Le texte a bien un effet extra-territorial mais cet effet est limité lorsqu'on examine la possibilité pour le prestataire de s'opposer à une telle demande - qui prend la forme d'une assignation, d'un mandat ou d'une ordonnance. Ainsi, le caractère impératif du texte s'impose pour la communication des informations sous réserve de l'existence de deux critères cumulatifs dont l'un est que les personnes concernées soient américaines et résidentes sur le sol américain. Cependant, il est utile pour bien comprendre le contexte du CLOUD Act de connaître le projet européen de règlement relatif aux « *injonctions européennes de production et de conservation de preuves électroniques en matière pénale* », paru le 17 avril 2018, et qui est très similaire au CLOUD Act. En fait, si l'on regarde les déclarations du Commissaire à la Justice de l'Union européenne ou les déclarations du premier Vice-Président de la Commission européenne, ils ne reprochent pas au CLOUD Act d'exister, mais ils reprochent aux

américains d'avoir « tiré les premiers ». Il faut garder ceci en tête pour replacer les choses en perspective. Le projet européen reprend l'élément d'extra-territorialité puisqu'il s'applique aux européens qui ne se trouvent pas dans l'Union européenne, dès lors que le service fourni est rendu dans l'Union européenne. Ce projet européen est par ailleurs soutenu tant par la Commission européenne que par les Etats membres.

Pascale Gelly : Concrètement, comment vont se passer les demandes des autorités américaines pour nous, européens ?

François Coupez : Les demandes vont prendre la forme d'une assignation, d'un mandat ou d'une ordonnance. L'argumentaire du texte américain (semblable à celui du projet européen) est que le texte doit permettre d'agir plus vite et de remplacer le système qui jusqu'à présent nécessitait, via un accord international, de passer par l'Etat étranger avant de « redescendre » vers les juges. Sur la base de l'assignation, du mandat ou de l'ordonnance, les autorités américaines peuvent maintenant prendre contact directement avec le prestataire pour lui demander la communication des informations. Le prestataire a la possibilité de s'y opposer sur deux critères : la demande ne concerne pas un Américain résidant aux Etats-Unis et le prestataire appartient à un pays qualifié de « *qualifying foreign government* ». La qualification tend à ce qu'un accord (*executive agreement*) soit conclu entre les U.S.A. et les différents pays pour que les opérateurs de ces pays puissent s'opposer à la communication des informations qui ne concernent pas les citoyens américains résidents aux USA.

Olivier Iteanu : C'est dans le reste l'US Code que l'on trouve les précisions sur l'accès aux données par les autorités. C'est assez complexe mais il faut retenir qu'il y a des cas où il y a possibilité pour les autorités américaines d'accéder à des informations sans passer par un mandat du juge. Le directeur du FBI, par exemple, peut faire un certain nombre de demandes sans passer par le juge. Cependant, en règle générale, il y a un mandat (*warrant*) pris par le juge, qui ne précise pas les motifs, car pour l'efficacité de l'enquête il est nécessaire de révéler certaines informations au moins de personnes possibles. Le champ de la criminalité visée est en fait très large : pas seulement le terrorisme mais également le trafic de drogues, ainsi que le « *tele-marketing fraud* » (spam et autres).

Dans ces demandes d'accès, de captation et d'interception de données, les « personnes concernées » (comme les appellent le droit européen) n'en sont jamais mises au courant, et *a fortiori* n'ont de recours.

Le texte clarifie ce qui est possible non seulement pour le gouvernement, mais aussi pour les prestataires, qui ont pris des engagements contractuels auprès de leurs clients en termes de confidentialité qui vont à l'encontre du CLOUD Act.

Pascale Gelly : Quels peuvent-être les gardes-fous pour que les libertés soient correctement protégées ? Et est-ce qu'il va s'agir de communication massive de données ou, à l'inverse, d'une surveillance très ciblée ?

Olivier Iteanu : Le texte vient simplement ajouter un dispositif de plus, et ne change pas ce qui précédait, c'est-à-dire les demandes massives.

En termes de recours, il y a une possibilité de la part du prestataire dans les 14 jours suivant la réception de la demande. Le texte du CLOUD Act n'est pas si long que ça - une petite dizaine de page - mais il passe beaucoup de temps sur la notion de « qualifying foreign government ». C'est la seconde possibilité pour contester une demande. En effet, le prestataire peut s'opposer au transfert des données vers les États-Unis si l'État duquel il devrait rapatrier les données est un « *qualifying foreign government* ». Il y a un grand nombre de critères qui explique ce qui est qualifié ou pas.

Tout d'abord, qui qualifie? C'est un haut fonctionnaire du Département de la Justice, l'Attorney General. Celui-ci va évaluer les droits des Etats étrangers, par exemple s'ils sont démocratiques ou s'ils respectent les droits de l'homme. Un grand nombre de critères sont posés par le texte pour déterminer si un pays est un *qualifying foreign govermnemt*. Cette liste n'est pas encore établie, à ma connaissance. L'Attorney General ne répond de cette liste que devant le Congrès américain, il n'y a pas de recours possible.

Une fois que cette liste est établie, l'État concerné est invité à passer un *Executive Agreement* (peut-être pourrait-on le traduire par « accord d'exécution ») avec le gouvernement des Etats-Unis. Cet accord va typiquement aussi inclure une responsabilité légale pour les prestataires américains de répondre aux demandes émanant des gouvernements des pays qualifiés.

Pascale Gelly : Mais le CLOUD Act est en application dès maintenant, alors que les accords n'ont pas été conclu ?

Olivier Iteanu : Effectivement. C'est problématique car certaines de ces données seront des données à caractère personnel au sens du RGPD. Dans notre règlement, nous avons une disposition qui autorise le transfert ou la divulgation à des pays qui sont hors de l'Union Européenne (article 48) dès l'instant où cela est fait dans le cadre d'un traité international ou d'un accord avec un pays tiers. De ce point de vue, la condition n'est pas remplie. Cependant, le problème posé est plus général: le gouvernement des États-Unis est en train de mettre en place un système, avec des ressources importantes. Mais *quid* des risques ? Le Sénat américain a très bien étudié, dans le cas du Patriot Act, les possibilités qui existaient de contourner le système pour prendre des informations et les donner à des tiers, totalement en infraction aux règles. Il peut y avoir aussi des interprétations très permissives du texte. Au moment où, avec le RGPD, nous sommes dans l'évaluation des risques, que penser de l'instauration d'un tel système ? Les risques dépassent le domaine du pur droit, et je pense qu'il est important d'en être conscient.

Pascale Gelly : Mais ne faut-il pas relativiser, puisque l'Union Européenne prépare un projet similaire ?

François Coupez : Effectivement il est important de reprendre le sujet dans son contexte général. Si l'on aborde le sujet sous l'angle juridique, à l'heure actuelle il n'y a pas de « *qualifying foreign government* », et le CLOUD Act est problématique vis-à-vis du RGPD notamment (article 48). Mais le Commissaire à la Justice de l'Union européenne ne dit pas « que le CLOUD Act est un danger pour les libertés », elle dit qu'il est dommage que le texte soit sorti trop vite ; obtenir des règles compatibles dans le cadre d'un projet de loi sur la preuve européenne était l'objectif. Selon le Premier Vice-Président de la Commission européenne « *Les propositions présentées visent non seulement à mettre en place des nouveaux instruments qui permettront aux autorités compétentes de recueillir des preuves électroniques rapidement et efficacement par-delà les frontières mais aussi à assurer des garanties solides pour les droits et libertés de toutes les personnes concernées*. »
Ces propos auraient pu émaner de l'administration américaine car l'on retrouve les mêmes fondements, les mêmes principes et le projet de texte européen est très proche du CLOUD Act. Sur certains points, il va même beaucoup plus loin que le texte américain.
Il convient de souligner que le mauvais réflexe serait de se dire « il faut boycotter les prestataires américains », soumis par hypothèse à ce texte. Le CLOUD Act s'applique aussi aux entreprises européennes : à partir du moment où celles-ci ont ouvert le marché pour proposer une offre aux États-Unis ou autres, elles sont concernées, même si elles pensent que ce texte ne leur est pas applicable. Le juge qui examinera les droits et libertés des personnes, au cœur de l'argumentation, pour déterminer s'il fait droit au mandat qui a été émis, tiendra compte du lien entre le prestataire qui a reçu la demande et les Etats-Unis (lien capitalistique, serveurs aux USA, etc.). Le réflexe naturel est de croire qu'avec ce texte, les relations avec les opérateurs américains vont être problématiques, mais cela le sera tout autant pour des prestataires d'autres pays. L'Union

européenne va adopter ce type de schémas où les entités d'un pays peuvent accéder de manière extra territoriales à des informations qui sont stockées physiquement parlant dans un autre pays. Sur un plan tactique, il ne faudrait pas que le raisonnement très critique que nous pourrions avoir aujourd'hui nous soit opposé à l'identique demain, quand le texte européen sera publié et que le continent asiatique, par exemple, nous boycottera en arguant que les textes sont dévoyés. A ce titre, les projets de règlement et de directive européens avancent et la volonté politique de les adopter est très forte. Un accord interviendra selon toute vraisemblance dans un délai de 6 à 18 mois.
Il est probable qu'en attendant, les demandes fondées sur le CLOUD Act soient assez faibles car les États n'ont pas intérêt à mettre ce mécanisme en danger. Une fois l'accord passé, en revanche, il n'y aura plus de problèmes parce qu'une large partie des pays au sein de l'Union Européenne a besoin de ce type d'accord : la procédure de coopération actuelle paraît peu claire et trop lente aux yeux des Etats membres (alors que dans le projet de texte européen, les délais de fourniture peuvent être extrêmement rapides).

Tout comme pour le projet de texte américain, les textes européens envisagent de clarifier. Certes, les garanties ne sont pas toutes réunies, on n'est pas en totale conformité avec le RGPD pour l'heure. Cependant, toutes les entités politiques, américaines comme européennes, vont dans le sens d'un accord dont le contenu n'est pas remis en cause. Par ailleurs, le fait que de tels transferts de données puissent être rendus possible ne constitue pas une nouveauté : les clauses contractuelles type des responsables de traitement avec les sous-traitants prévoyait déjà cette possibilité, de façon spécifique, en 2010 (pour les cas où un sous-traitant, en vertu de sa loi locale, était obligé de transmettre des informations).

Olivier Iteanu : Je trouve que la Commission Européenne est bien discrète et bien clémente sur le sujet. Je rappellerais quand même le Safe Harbor, conclu par la Commission et finalement annulé par la Cour de Justice de l'Union Européenne : on voit que les positions de la Commission ne sont pas toujours suivies par le système judiciaire communautaire.

Je passerai rapidement sur le fait que les États-Unis aient opéré sur le *modus operandi* d'adopter d'abord des règles unilatérales avant d'aborder la discussion internationale…

Il n'est pas question de boycotter les prestataires américains, en effet. D'ailleurs, cela serait bien difficile aujourd'hui compte tenu l'état du marché européen. Mais il faut aussi avoir une approche circonstanciée : nous vivons dans un environnement concurrentiel mondial où il faut mesurer les risques que l'on prend quand on connaît les systèmes qui existent dans certains pays (aux États-Unis, en Chine, …). D'ailleurs, il n'est pas question que de données personnelles, mais également de données stratégiques ou commerciales. On se souviendra aussi qu'il y a le système et la manière dont il est utilisé. Le texte a au moins le mérite de clarifier les pratiques du gouvernement (alors que l'on m'a longtemps objecté qu'il n'y avait pas d'extra-territorialité du Patriot Act, ou qu'il ne concernait que les méta-données).

Pascale Gelly : Si je comprends bien , nous nous retrouvons, comme souvent en matière de protection des données personnelles, dans une phase d'incertitude qui ne sera pas levée avant quelques mois. Dans cet intervalle, que donneriez-vous comme conseil aux entreprises qui ont recours aux acteurs du cloud ? Pour ceux qui utilisent des acteurs du cloud américains, qui sont quand même assez incontournables, il faut signer des clauses types qui prévoient la situation ?

Olivier Iteanu : Non seulement les clauses types le prévoit mais déjà, la convention de Budapest, qui date de novembre 2001, quelques semaines après le Patriot Act, et qui donnait aux États un canevas de la surveillance électronique, posait les fondements de ce système. On sait très bien que les services de renseignement de chaque État ont également des activités pour la défense du patrimoine économique et industrielle de leur pays… Cela pose quand même certaines questions, sans même parler des risques accidentels ou de cyber-attaques. On ne sait pas comment ces données sont transmises, par qui elles sont conservées ou combien de temps.

En Allemagne, les autorités allemandes ont demandé à ce que les data centers soient opérés par des opérateurs allemands ou en tout cas des opérateurs déclarés auprès de l'équivalent de l'ARCEP : c'est une solution qui permet de conserver une certaine souveraineté et confidentialité sur nos données.

Pascale Gelly : Que conseiller comme précautions à prendre ? Contacter leurs prestataires pour leur demander quelles procédures sont mises ne place pour réagir à des demandes de force de l'ordre ? Comment font-elles par exemple pour vérifier la nationalité et la résidence des personnes ciblées ?

Olivier Iteanu : le RGPD, dans son article 28 sur la sous-traitance, donne un certain nombre de pistes. Le dispositif mis en place pour répondre au RGPD doit apporter des garanties aux organisations qui recourent au service du cloud computing. Je pense qu'il faut regarder aussi la criticité des données que l'on va confier. Plus la donnée est critique, plus l'on doit disposer d'une prestation dont on considère que le risque qu'elle s'échappe hors de l'Union Européenne est moindre.

François Coupez : Je suis absolument d'accord avec Olivier pour cette approche par le risque. Il y a le juridique et ce que les services spéciaux des Etats, sortant du cadre juridique, sont capables de réaliser. Lorsque l'on pense aux grands contrats ainsi soufflés aux européens par des entreprises américaines du fait de l'ingérence de certains services de ce type, on ne peut qu'avoir ce réflexe d'analyse de risque et d'intelligence économique.
Maintenant, pour ce texte en particulier, je pense aussi qu'il faut être pragmatique et prendre acte de la situation actuelle, notamment du projet de texte européen grâce auquel on ne fait pas que subir le texte CLOUD Act : nous prévoyons la réciprocité ce qui s'avère un point positif pour la répression des crimes et délits.

Par ailleurs, si l'on se concentre sur la question de la localisation des données et de la souveraineté numérique des Etats en la matière, elle devient très faible au sein de l'UE : un autre projet de texte très prochainement adopté prévoit que l'on ne pourra plus exiger la localisation géographique des données dans un État membre en particulier (sauf certains cas très spécifiques) mais qu'à chaque fois le stockage devra pouvoir être possible dans l'ensemble de l'Union européenne. Politiquement, là encore, ça pose question…[1]

En pratique, pour les responsables de traitement, il faut se reposer sur l'article 28, mais également le dépasser en essayant d'apporter une garantie supplémentaire en imposant au prestataire, quand il est saisi d'une demande, de systématiquement la contester et, dès qu'il le peut, informer le responsable de traitement de celle-ci. S'il ne le peut pas, par exemple en vertu du CLOUD Act, il lui est toujours possible de prévenir l'État dans lequel il est implanté, où une pression politique peut faire en sorte que les choses s'arrangent. C'est un problème profondément politique, et pas simplement juridique.

D'un autre côté, il faut aussi voir le raisonnement et la légitimité de ces textes : sans ce type de coopération accentuée, il suffirait aux délinquants d'héberger leurs données dans un autre pays pour limiter ou réduire à néant l'efficacité des enquêtes, en pratique.

Un dernier point : nous avons beaucoup parlé du cloud, mais les textes américains et européens visent beaucoup plus largement tous les prestataires qui sont amenés à traiter des informations. Cela peut être les serveurs de messagerie, etc. L'appellation « CLOUD Act » est un peu trompeuse de ce point de vue, car le texte est d'application très large.

Pascale Gelly : Il ne me reste plus qu'à vous remercier pour cet échange passionnant qui nous aura permis de faire le tour de ce sujet important.

[1] Cf. le projet sur la libre circulation des données non personnelles http://europa.eu/rapid/press-release_IP-18-4227_en.htm, qui complète le RGPD prévoyant, quant à lui, la libre circulation des données personnelles.