ARTICLE

FAUT-IL AVOIR PEUR DU CLOUD ACT ?

Immobilier et Construction Droit européen Droit public et commande publique | 25/06/18 | Emmanuelle Mignon

Le *Clarifying Lawful Overseas Use of Data Act* (ci-après, le « ***Cloud Act*** ») a été promulgué par le Président des Etats-Unis le 23 mars 2018. Adopté sans réel débat à l'issue des complexes discussions relatives à la loi sur les dépenses pour 2018, il ne cesse de susciter, aux Etats-Unis et en Europe, les critiques des associations de protection des droits fondamentaux et celles des contempteurs de l'extraterritorialité, pas toujours bien comprise, des lois américaines. Non sans une bonne dose d'approximations.

L'ambition du présent flash est d'exposer concrètement ce qu'est le *Cloud Act*, préciser ce qu'il faut en retenir et explorer ce que pourrait/devrait être la réaction des autorités françaises et européennes.

1- Du warrant case au C*loud Act*

Le Titre 18 du *United States Code* constitue l'équivalent de notre code pénal et de notre code de procédure pénale réunis. Il comprend un chapitre 121 connu sous le nom de *Stored Communications Act* (ci-après, le « ***SCA*** ») introduit dans la législation américaine en 1986. Ce texte fixe un principe de confidentialité et de protection des données de communication (contenu et informations sur l'utilisateur et ses communications) traitées ou stockées par les fournisseurs de services de communication, traitement et stockage électroniques de données.

Classiquement, ce texte prévoit également un certain nombre d'exceptions au principe ainsi édicté, telles que les divulgations nécessaires à la fourniture du service, les divulgations à la demande de l'utilisateur, ainsi que la possibilité pour les autorités américaines, sous certaines conditions de forme et de fond, de requérir des fournisseurs de ces services la communication de données concernant leurs clients pour les besoins de procédures répressives. Il n'est pas indifférent de noter que le *Stored Communications Act* a été adopté dans le but de soumettre expressément la divulgation de certaines données de communication par des tiers (les fournisseurs de services) dans le cadre d'investigations criminelles au Quatrième amendement à la Constitution des Etats-Unis (protection contre les perquisitions et les saisies non ordonnées par l'autorité judiciaire et non fondées sur une présomption sérieuse que la personne concernée a commis ou est sur le point de commettre une infraction pénale et que les lieux, objets ou informations visés par le mandat sont utiles à l'enquête).

Dans ce cadre, et à l'occasion d'une affaire de trafic de stupéfiants, les autorités américaines ont demandé en 2013 à la société Microsoft Corporation de lui communiquer des données de communication concernant un ressortissant non américain. Microsoft Corporation a refusé au motif que les données étaient stockées en Irlande et que, par respect pour la souveraineté de ce pays, une telle demande de communication devait emprunter le circuit de l'entraide judiciaire internationale (c'est-à-dire soit une procédure prévue par un *Mutual Legal Assistance Treaty*, les fameux MLAT, soit une commission rogatoire internationale). Microsoft soutenait, d'une part, qu'il aurait été impossible pour les autorités américaines de venir forcer elles-mêmes les portes d'une armoire physique située en Irlande dans laquelle les mêmes données auraient été stockées sous format papier et qu'il n'y avait donc aucune raison de le permettre pour une armoire virtuelle ; d'autre part, Microsoft faisait valoir qu'une telle demande risquait de la placer dans une situation de conflits de lois dans l'hypothèse où une loi irlandaise ferait obstacle à la communication des données. Ce faisant, Microsoft anticipait sur l'entrée en vigueur du RGPD.

Comme on le sait, la cour d'appel du 2nd circuit de New-York a donné raison à Microsoft. Le ministère américain de la justice a alors porté l'affaire devant la Cour suprême des Etats-Unis, qui a décidé de l'instruire. Toutefois, peut-être dans la crainte du résultat de cette instance, le gouvernement américain a préféré, avant que la décision de la Cour suprême ne soit rendue, faire adopter le *Cloud Act* par le Congrès, réglant ainsi la question directement par la loi. En conséquence, la Cour suprême n'a pas statué sur le *warrant case*.

2- Que prévoit le *Cloud Act* ?

Bien qu'il fasse plus d'une dizaine de pages, le *Cloud Act* contient essentiellement deux dispositions :

- il prévoit d'abord que toute société américaine au sens du droit américain, c'est-à-dire u**ne société incorporée aux Etats-Unis ainsi que les sociétés contrôlées par elle, doit communiquer aux autorités américaines, sur leur demande, les données de communication placées sous son contrôle sans considération du lieu où ces données se trouvent stockées.** *Exit* donc la souveraineté juridique des autres pays à raison du lieu de stockage des données ;

- il prévoit ensuite (et c'est la partie de loin la plus longue du texte) **la possibilité pour le gouvernement des Etats-Unis de signer avec des gouvernements étrangers des accords internationaux permettant aux autorités respectives de chaque pays de demander directement aux fournisseurs de services de communication, traitement et stockage électroniques de données relevant de la juridiction de l'autre la divulgation des données de communication les intéressant, sans avoir à passer par les procédures beaucoup plus longues des MLAT ou des commissions rogatoires internationales.**

Concrètement, si les Etats-Unis signaient un tel accord avec un pays imaginaire appelé de manière fort originale la Syldavie, les autorités de Klow pourraient demander directement aux fournisseurs de services relevant de la juridiction des Etats-Unis la communication des données placées sous leur contrôle et intéressant leurs enquêtes, à l'exception toutefois de données concernant des *US persons* (ressortissants américains, résidents permanents, sociétés immatriculées aux Etats-Unis principalement), sans avoir à passer par le département américain de la justice ; réciproquement, les autorités américaines pourraient s'adresser directement aux fournisseurs syldaves de services de communication, traitement et stockage électroniques de données (les très fameux «clouds souverains» syldaves) pour obtenir la divulgation de données de communication placées sous le contrôle de ces sociétés sans passer par les autorités gouvernementales et/ou judiciaires du Royaume du pélican noir. Le texte ne le dit pas, mais la logique de réciprocité voudrait naturellement que de telles demandes formulées par les autorités américaines ne puissent pas concerner des données concernant des ressortissants ou entreprises syldaves, ni des données concernant des ressortissants ou entreprises relevant de la juridiction des autres pays avec lesquels la Syldavie forme une « *Union sans cesse plus étroite* ».

Les accords internationaux dont il s'agit prendront la forme d'*executive agreements*, c'est-à-dire des accords qui ne supposent ni l'accord du Sénat à la majorité des deux tiers, ni l'adoption d'une loi par les deux chambres du Congrès. Pour entrer en vigueur, il suffira que les deux chambres ne s'y opposent pas par une résolution conjointe dans les 90 jours de leur signature. En contrepartie, de tels accords ne peuvent être signés qu'avec des pays respectueux des droits fondamentaux et des principaux standards démocratiques. Et le *Cloud Act* précise expressément que les demandes de communication de données concernées par ces accords ne peuvent viser que les infractions les plus graves (« *serious crime* »).

En réalité, le *Cloud Act* organise à l'échelle de la relation transatlantique ce que le projet de réglement E-evidence essaie d'organiser à l'échelle européenne : la possibilité pour les autorités de poursuite d'obtenir la divulgation des données de communication les intéressant dans le cadre de leurs investigations en s'adressant directement aux sociétés traitant ou conservant ces données, c'est-à-dire de manière beaucoup plus rapide que dans le cadre classique de la coopération judiciaire internationale. L'objectif affiché est de rapprocher le temps de l'investigation criminelle de celui de la criminalité.

Tous les observateurs s'accordent à dire que le *Cloud Act* ne permet pas de déterminer avec certitude si un tel *executive agreement* pourrait être signé avec l'Union européenne plutôt qu'avec les Etats membres. Peut-être dans un souci d'affichage politique, il semble que les autorités américaines aient voulu se réserver la possibilité de ne pas signer de tels accords avec des pays de l'Union européenne considérés, du point de vue de la protection des droits, comme moins fréquentables que d'autres, d'où la notion d'accords signés avec uniquement des *qualifying foreign governements*.

Si le Royaume-Uni a commencé à négocier de son côté un *executive agreement* avec les Etats Unis, la position majoritaire des Etats membres de l'Union européenne est plutôt, à ce stade, de rechercher un accord global entre l'Union et les Etats-Unis.

3- Le C*loud Act* permet-il aux autorités américaines d'accéder sans contrainte à l'ensemble des données européennes traitées ou stockées par les fournisseurs de services placés sous la juridiction ds Etats-Unis ?

On a entendu sur ce point beaucoup d'approximations, sinon de bêtises.

Il est certain que le *Cloud Act* s'applique à toute société placée sous la juridiction des Etats-Unis qui contrôle les données informatiques que lui ont confiées ses clients quels que soient la nationalité de ceux-ci et le lieu physique où ces données ont été émises ou sont stockées. Les GAFAM sont des sociétés placées sous la juridiction des Etats-Unis ainsi que leurs filiales. C'est en ce sens que le ***Cloud Act* n'est pas une loi extraterritoriale, mais seulement une loi qui s'applique à toute société placée sous la juridiction des Etats-Unis au sens, il est vrai extensif, du droit américain.**

Pour autant, le *Cloud Act* ne change rien aux conditions légales dans lesquelles de telles demandes de communication peuvent être formulées par les autorités américaines.

Concrètement :

- sur le fondement du *SCA*, les autorités américaines ne peuvent requérir la communication de données de la part de fournisseurs de services de communication, traitement et stockage électroniques de données placés sous leur juridiction que dans le cadre de procédures judiciaires et si elles disposent en ce sens d'un mandat (*warrant*), c'est-à-dire d'un titre délivré par une juridiction et placé sous la protection du Quatrième amendement à la Constitution des Etats-Unis (présomption sérieuse que la personne concernée a commis ou est sur le point de commettre une infraction pénale et que les lieux, objets ou informations visés par le mandat sont utiles à l'enquête). Sous cet angle, le droit américain est plus protecteur que le droit français, lequel permet au Parquet de formuler des réquisitions comparables. Or, comme ne cesse de le dire la Cour européenne des droits de l'homme, le Parquet n'est pas un « tribunal indépendant et impartial », non pas en raison des conditions de nomination de ses membres (faux débat), mais parce qu'il est l'autorité de poursuite ;

- le *SCA* autorise également les entités gouvernementales américaines à requérir la communication de données ou métadonnées de communications sur le fondement de *court orders.* Ces demandes sont donc elles aussi formulées avec l'autorisation d'une juridiction et doivent, comme pour les *warrants*, être justifiées par les nécessités d'une procédure pénale ;

- la possibilité, prévue par le texte, pour les entités gouvernementales américaines d'obtenir la communication de données de contenu par le biais d'*administrative, grand jury ou trial subpoenas* a été censurée par un arrêt du 14 décembre 2010 de la cour d'appel du sixième circuit de Cincinnati (*United States v. Warshak*) au motif que de telles demandes n'étaient pas placées sous la protection du Quatrième amendement. Cette jurisprudence n'a été ni confirmée, ni infirmée par la Cour suprême des Etats-Unis, mais elle est considérée comme incontestable par l'ensemble des acteurs et, de fait, les GAFAM ne transmettent pas de données de contenu aux autorités américaines sur le fondement de simple *subpoenas*. Mieux encore, par un arrêt extrêmement récent (22 juin 2018 *Carpenter v. United States*), la Cour suprême des Etats-Unis a jugé que la demande de communication de données de géolocalisation émises par un téléphone portable, adressée par les autorités américaines à un fournisseur de services de communication, devait bénéficier de la protection du Quatrième amendement et être formulée par l'intermédiaire d'un *warrant* : une décision qui va totalement dans le sens de l'arrêt *United States v. Warshak* ;

- enfin, il est toujours possible pour le fournisseur requis de contester devant une juridiction de première instance ou d'appel, par voie d'action ou par voie d'exception (cf. infra), l'ordre qui lui a été remis de divulguer aux autorités américaines les données de communication qui lui ont été confiées.

Contrairement à ce qui a pu être écrit à de nombreuses reprises, le *Stored Communications Act* tel que modifié par le *Cloud Act* **ne donne donc pas carte blanche aux autorités américaines pour accéder sans aucune condition, ni aucun contrôle à l'ensemble des données confiées aux fournisseurs de services de communication, traitement et stockage électroniques de données placés sous la juridiction des Etats-Unis.**

Par ailleurs, le *Cloud Act* prévoit explicitement que le fournisseur de services auquel les données sont demandées a toujours la possibilité de s'y opposer au motif que la demande, si elle devait être satisfaite, **le conduirait à méconnaître la législation d'un pays étranger et l'exposerait à des sanctions (situation de conflits de lois).**

Les conditions d'opposition sont différentes selon qu'il existe ou non un *executive agreement* avec le pays dont la loi est susceptible d'être méconnue :

- en cas d'*executive agreement* entre les Etats-Unis et le pays en cause, la demande d'opposition, qui vient donc en plus des autres cas éventuels d'opposition tenant à la légalité ou au bien-fondé de la réquisition, doit être formée dans un délai de 14 jours. Pour apprécier s'il y a lieu d'annuler ou modifier la demande de communication, la cour doit prendre en compte le caractère sérieux du risque de sanction auquel est exposé le fournisseur dans l'autre pays et l'intérêt qui s'attache, pour la justice, à la modification ou à l'annulation de la demande. L'intérêt de la justice est apprécié en fonction des critères suivants : l'intérêt des Etats-Unis, notamment celui de l'entité cherchant à obtenir communication des informations litigieuses ; l'intérêt du *qualifying foreign government* à empêcher la communication, illégale selon sa législation, des informations litigieuses ; la localisation et la nationalité du client et la nature des connections de ce client avec les Etats-Unis ; la nature des liens du fournisseur avec les Etats-Unis ; l'importance des investigations menées et des informations dont la communication est demandée pour ces investigations ; les possibilités qu'a l'entité gouvernementale d'obtenir de manière tout aussi acceptable les informations demandées par des moyens présentant moins de conséquences négatives.

  Cette procédure d'opposition, dénommée c*omity analysis* (ou analyse de courtoisie), n'est pas applicable lorsque les données dont la communication est demandée concerne une *United States person*, c'est-à-dire un citoyen des Etats-Unis, une personne admise à la résidence permanente, une association non enregistrée dont un nombre important de membres sont des citoyens américains ou des personnes admises à la résidence permanente, ou toute société enregistrée aux Etats-Unis ;

- en l'absence d'*executive agreement*, le fournisseur requis peut également refuser de communiquer les données sollicitées sur le fondement des *common law principles of comity*, c'est-à-dire sur le fondement du principe de courtoisie internationale reconnu par les juridictions américaines selon lequel, pour l'application du droit des Etats-Unis, il convient de tenir compte des intérêts importants des autres pays et, le cas échéant, ne pas appliquer ou appliquer de manière nuancée la législation américaine. A la différence de la procédure précédente, les critères que le juge devra utiliser pour se prononcer sur le bien-fondé d'une telle opposition ne sont pas précisés par la loi (ils résultent de la jurisprudence). Par ailleurs, lorsque la procédure repose sur un *warrant*, l'opposition n'est pas directe. Elle prend la forme d'un argument en défense contre la demande de condamnation de la société requise pour *contempt of court*.

Il n'est pas très facile de comprendre les différences, ni surtout la raison d'être de cette double procédure d'opposition en cas de conflit de lois, selon que le pays étranger dont la loi risque d'être méconnue a signé ou non un *executive agreement*. L'objectif des Etats-Unis semble avoir été d'encourager la signature d'*executive agreements* par l'élaboration d'une procédure directe et claire d'opposition alors que le principe de courtoisie internationale tel qu'il résulte de la seule jurisprudence de droit commun des juridictions américaines est parfois critiqué comme insuffisamment précis et prévisible.

4- Existe-t-il des lois françaises ou européennes susceptibles de faire obstacle aux réquisitions des autorités américaines sur les données conservées en Europe ?

Il en existe au moins trois.

La première est la loi n°68-678 du 26 juillet 1968 *relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères*, dite « loi de blocage française » (par opposition au règlement européen de blocage n°2271/96 du Conseil du 22 novembre 1996 *portant protection contre les effets de l'application extraterritoriale d'une législation adoptée par un pays tiers, ainsi que des actions fondées sur elle ou en découlant*, qui s'efforce, pour sa part, de contrer l'effet de certaines sanctions américaines contre les entreprises européennes ayant des activités avec des pays soumis à des embargos américains).

Sous réserve de traités ou accords internationaux, **la loi de blocage française interdit à toute personne de nationalité française ou y résidant habituellement ou à toute personne morale y ayant son siège ou un établissement, de communiquer à des autorités publiques étrangères des documents ou des renseignements d'ordre économique, commercial, industriel, financier ou technique de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public (article 1), interdit à toute personne de demander, de rechercher ou de communiquer des informations 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 (article 1 bis), instaure une obligation pour les personnes qui se trouveraient saisies de telles demandes d'en informer sans délai le Ministre des affaires étrangères (article 2 dont la méconnaissance n'est pas sanctionnée) et prévoit une sanction pénale de six mois d'emprisonnement et 18 000 euros d'amende (90 000 euros pour une personne morale) en cas de méconnaissance des interdictions instituées par les deux premiers articles de la loi (article 3).**

Très clairement, les demandes de communication de données qui pourraient être formées auprès des GAFAM par les autorités américaines dans le cadre du *Cloud Act* pourraient entrer dans le champ d'application de l'article 1 et plus encore de l'article 1 bis de la loi française de blocage et exposer ces sociétés ainsi que leurs filiales françaises aux sanctions correspondantes. **Elles devraient donc pouvoir s'opposer à la communication de telles données en invoquant le principe de courtoisie internationale selon l'une ou l'autre des procédures mentionnées ci-dessus.**

Il est exact que les juridictions américaines ne portent que peu de considération à la loi de blocage française compte tenu du fait que les sanctions qu'elle prévoit ne sont, dans les faits, jamais infligées. Dans une décision tristement célèbre du 15 juin 1987 (*Société nationale industrielle aérospatiale v. U.S. District Court* No.85-1695), la Cour suprême des Etats-Unis a ainsi refusé de prendre en considération cette loi pour dégager une entreprise de ses obligations au regard du droit américain, excipant principalement du fait que les sociétés françaises qui communiquent des informations en méconnaissance des dispositions de la loi de blocage ne sont, dans les faits, pas sanctionnées.

On notera toutefois que, depuis l'intervention de cette décision, au moins une sanction pénale sur le fondement de la loi de blocage a été prononcée par une juridiction française et confirmée par la Cour de cassation (Cass. crim 12 décembre 2007 pourvoi n°07-83.228 *Christopher X*), et que, postérieurement à cet arrêt, la *Court of Chancery* de l'Etat du Delaware (21 février 2014 *Activision Blizzard Inc. Stockholder litigation* Cons. C.A. No.8885-VLC) a accepté, compte tenu de la loi de blocage française, de favoriser, pour la recherche de preuves dans une procédure juridictionnelle américaine, l'utilisation de procédures prévues par la Convention de La Haye de 1970 plutôt que la procédure américaine de *discovery* (mais en fixant des délais réduits pour les mettre en œuvre sous peine de faire primer les procédures américaines).

Les articles 44 et suivants du 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* (le fameux RGPD), règlementent pour leur part les conditions dans lesquelles des données à caractère personnel peuvent être transférées vers des pays tiers ou à des organisations internationales.

De manière générale, de tels transferts ne sont possibles que :

- lorsqu'ils sont fondés sur une décision d'adéquation : c'est-à-dire lorsque la Commission a constaté par voie de décision que le pays tiers en question assure un niveau adéquat de protection des données à caractère personnel (article 45 du RGPD) ; ou

- lorsque ces transferts s'accompagnent de garanties appropriées et que les personnes dont les données sont en cause disposent de droits opposables et de voies de droit effectives pour faire respecter leurs droits (article 46 du RGPD) ; ou

- lorsque l'autorité de contrôle compétente a approuvé des règles d'entreprise contraignantes (article 47 du RGPD) ; ou encore

- dans une série de cas particuliers (article 49 du RGPD).

L'article 48 du RGPD précise par ailleurs, pour que les choses soient tout à fait claires, que : « *Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un Etat membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre* ».

En l'espèce, aucune décision d'adéquation générale n'a été adoptée par la Commission pour les transferts de données vers des autorités publiques américaines. Le mécanisme prévu par les accords du *Privacy shield* ne couvre que des transferts vers des sociétés américaines qui se sont auto-certifiées comme adhérant sans réserve aux principes contenus dans cet accord et non des entités gouvernementales. Les engagements unilatéraux, au demeurant assez flous, pris par les autorités publiques américaines dans le cadre du *Privacy shield* ne valent pas reconnaissance par la Commission que le transfert de données à ces autorités assurerait un niveau adéquat de protection des données à caractère personnel et serait donc possible sur le fondement de l'article 45 du RGPD.

De même, en l'absence d'un accord avec les Etats-Unis, un tel transfert ne peut trouver sa justification dans l'article 46 faute de mécanisme *ad hoc* permettant aux ressortissants européens concernés de disposer de garanties et de voies de droit comparables à celles résultant du RGPD.

Enfin, un tel transfert ne rentre dans aucune des exceptions de l'article 49, en particulier pas dans celle prévue par l'article 49 paragraphe 1 point d) du règlement (« *transfert nécessaire pour des motifs importants d'intérêt public* »). Cette exception ne vise en effet que les intérêts publics d'un Etat membre de l'Union ou de l'Union elle-même comme vient de l'indiquer fort opportunément le Comité européen de la protection des données (qui a remplacé le G29) dans ses *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679* publiées le 25 mai 2018. Ainsi, ce n'est pas parce que la lutte contre le terrorisme est un objectif partagé par tous les Etats, dont évidemment les Etats-Unis, et reconnu par leur législation respective que cet objectif justifie le transfert de données personnelles vers des pays tiers, dont les Etats-Unis, ou des organisations internationales, quand bien même ces données seraient demandées par des autorités administratives ou judiciaires. Toute autre interprétation de l'article 49 1 d) aurait d'ailleurs été incompatible avec l'article 48.

En revanche, toujours selon ces lignes directrices, le principe de réciprocité dans les relations internationales constitue un intérêt public. Dans ces conditions, l'existence d'un accord international de coopération policière ou judiciaire internationale pourrait permettre le transfert de données personnelles aux autorités d'un Etat tiers sur le fondement de l'article 49 1 d) (qui s'ajouterait alors, de manière superfétatoire, à l'article 48).

Ainsi, le transfert de données à caractère personnel aux autorités américaines qui serait opéré par un GAFAM en application d'une demande fondée sur le seul *Cloud Act* et non sur un accord international de type MLAT ou la mise en œuvre d'une commission rogatoire internationale, ne serait pas conforme au RGPD. Or une telle violation des règles du RGPD peut faire l'objet d'une amende administrative pouvant s'élever à 20 000 000 d'euros ou, dans le cas d'une entreprise, à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent. Compte tenu de leur importance potentielle, il peut être espéré qu'en application du principe de courtoisie internationale, les juridictions américaines considèreront avec plus d'attention que pour la loi de blocage la délicate situation où, pour respecter ses obligations au titre du *Cloud Act*, une société devrait méconnaître le RGPD.

Enfin, l'Union européenne s'est dotée récemment d'une règlementation visant à protéger le secret des affaires, la directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 *sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites*, dont la transposition en droit français est imminente. Prochainement, un nouvel article L. 151-6 du code de commerce devrait disposer que « *le secret des affaires n'est pas opposable lorsque l'obtention, l'utilisation ou la divulgation du secret est requise ou autorisée par le droit de l'Union européenne, les traités ou accords internationaux en vigueur ou le droit national, notamment dans l'exercice des pouvoirs d'enquête, de contrôle, d'autorisation ou de sanction des autorités juridictionnelles ou administratives* ». *A contrario*, la communication de données couvertes par le secret des affaires aux autorités américaines, en dehors de tout accord international, c'est-à-dire sur le seul fondement d'une demande unilatérale formulée par l'administration américaine auprès d'un GAFAM en application du *Cloud Act*, est interdite et exposerait le fournisseur qui communiquerait de telles données à la mise en cause de sa responsabilité civile.

5- Face au *Cloud Act*, que devraient faire les autorités françaises et européennes ?

La situation n'est pas très simple parce que les autorités européennes sont en réalité partagées entre le souci de protéger les données des entreprises et ressortissants européens et l'intérêt qui s'attache, pour les autorités répressives, à pouvoir récupérer rapidement les données de communication directement auprès des fournisseurs de services sans passer par les lourdes procédures de la coopération judiciaire internationale. Beaucoup de responsables européens approuvent le *Cloud Act*, comme ils approuvaient la position du département américain de la justice dans l'affaire du *warrant case*, et considèrent qu'au fond la nouvelle législation américaine va dans le même sens que le projet de règlement E-evidence dont ils ont été les pionniers. Ces acteurs poussent pour la négociation et la signature d'un *executive agreement* avec les Etats-Unis, qui présenterait, en principe, l'avantage d'ouvrir aux GAFAM la possibilité de s'opposer aux demandes de communication des autorités américaines concernant les données européennes dans le cadre de la nouvelle procédure d'opposition de *comity analysis,* en apparence plus sécurisante que l'application du seul principe jurisprudentiel de courtoisie internationale.

Encore faut-il savoir ce que l'on met derrière cette notion d'*executive agreement*. En effet, l'Union européenne et ses pays membres ne peuvent pas accepter de signer un ou des accords de cette nature aux termes desquels les Etats-Unis, en raison de l'importance des GAFAM dans l'économie numérique, auraient accès aux données mondiales, y compris les européennes, quel que soit leur lieu de stockage, tandis que les autorités européennes pourraient accéder à des données stockées aux Etats-Unis, mais ne concernant en aucun cas des *US persons.* La seule attitude possible pour l'Union européenne, celle qui témoignerait d'un réel souci de la réciprocité et d'un juste équilibre entre les nécessités de la lutte contre la criminalité et la protection des intérêts fondamentaux de l'Union, serait de négocier avec les Etats-Unis un accord par lequel les autorités de chaque pays auraient accès de manière fluide aux données nécessaires à la lutte

contre la criminalité, et à elles seules seulement, sans considération pour leur lieu de stockage et sans discrimination selon la nationalité des personnes ou des entreprises qu'elles concernent ; un tel accord devant être nécessairement adossé à des procédures de recours homogènes garantissant la protection des intérêts économiques et des droits fondamentaux des ressortissants de chaque partenaire.

Si un tel accord se révélait impossible, l'Union européenne devrait alors prendre les dispositions nécessaires pour rendre efficace le principe de courtoisie internationale devant les juridictions américaines.

A l'échelon français, il suffirait de décider d'appliquer la loi de blocage, après l'avoir le cas échéant renforcée, notamment en augmentant le niveau des sanctions pénales et en demandant au ministère public de mettre en route l'action publique. A l'échelon européen, il suffirait de se doter d'une réglementation équivalente faisant interdiction, sous peine de lourdes sanctions, à toute personne, ou société immatriculée sur le territoire de l'Union européenne, ou y ayant un établissement, de communiquer, en dehors de tout accord international, à des personnes privées ou à des autorités étrangères, des informations d'ordre économique, commercial, industriel, financier ou technique intéressant les entreprises européennes. L'Europe l'a fait pour les données personnelles, y compris donc potentiellement celles de dangereux criminels. On ne voit pas pourquoi elle ne le ferait pas pour ses entreprises.

On dit que les lois de blocage, quelles qu'elles soient, sont inefficaces en ce qu'elles placent les sociétés européennes entre un marteau (les sanctions susceptibles d'être infligées à leurs intérêts américains par les autorités américaines) et une enclume (les sanctions susceptibles d'être infligées à leurs intérêts européens par les autorités européennes). Le cas iranien est au cœur de cette problématique. Mais la situation est ici très différente. Car les entités susceptibles d'être placées dans l'étau ne sont pas des entreprises européennes, mais les filiales européennes d'entreprises américaines, ce qui est très différent.

En conclusion, ce n'est pas le *Cloud Act* qui est dangereux pour les entreprises européennes. C'est la manière dont l'Union européenne va réagir et les risques induits par les lenteurs de son processus de décision, quand ce n'est pas sa paralysie.