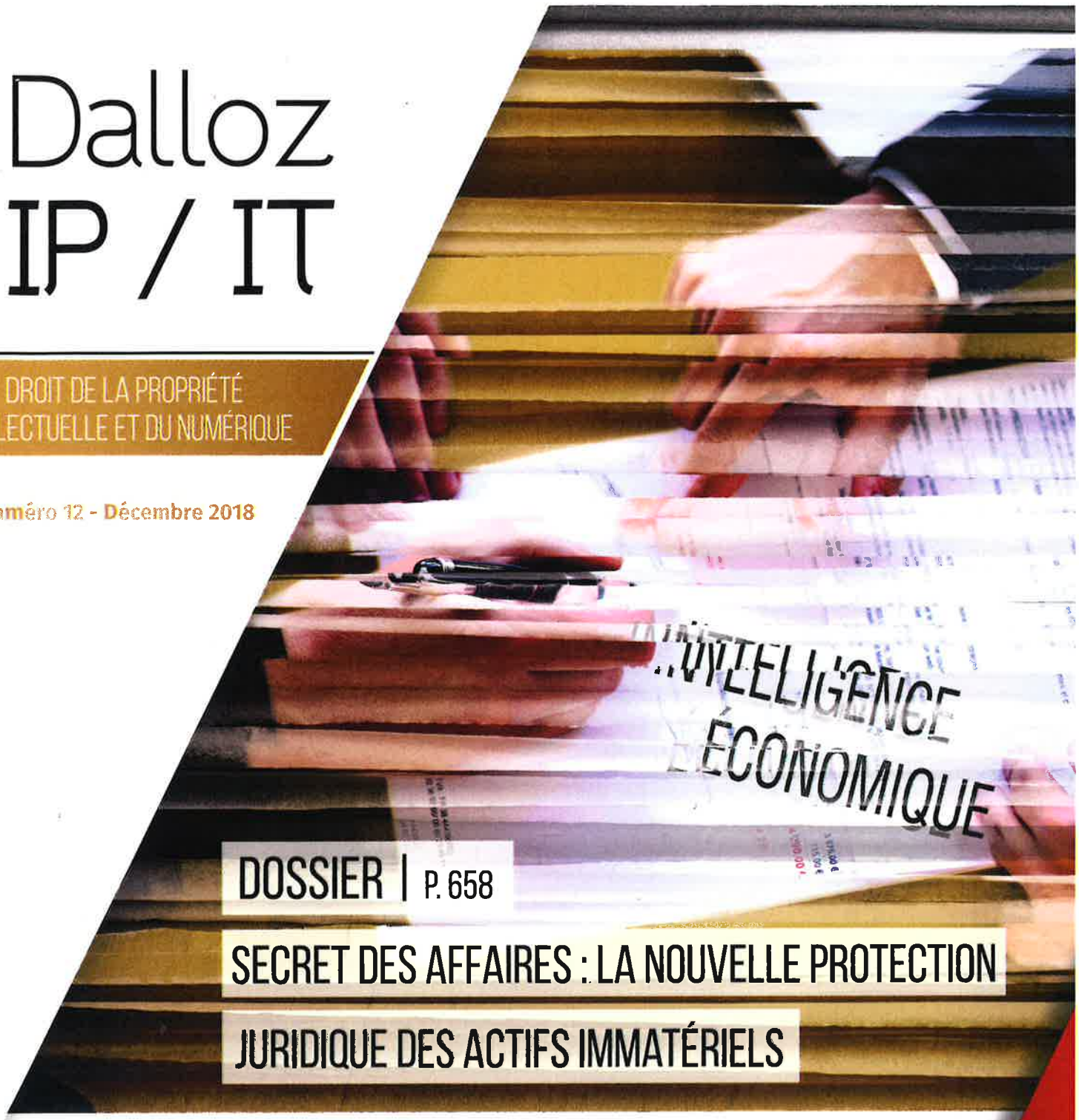
Dalloz IP / IT

DROIT DE LA PROPRIÉTÉ INTELLECTUELLE ET DU NUMÉRIQUE

Numéro 12 - Décembre 2018

9 782997 518126



DOSSIER | P. 658

SECRET DES AFFAIRES : LA NOUVELLE PROTECTION JURIDIQUE DES ACTIFS IMMATÉRIELS

PRATIQUES

Cloud Act : des inquiétudes légitimes

Flora Plénacoste et Emmanuel Daoud

TEXTES ET DÉCISIONS

Renonciation tacite au droit de paternité dans le domaine des arts appliqués : une cour d'appel franchit le pas

Rennes, 18 septembre 2018

Noémie Enser

TEXTES ET DÉCISIONS

Échec de demandes de restrictions judiciaires à l'accessibilité en ligne à des informations relatives à une affaire pénale ancienne

CEDH 28 juin 2018

Emmanuel Derieux

DALLOZ

CLOUD ACT : DES INQUIÉTUDES LÉGITIMES

Flora Plénacoste
Avocat au barreau de Paris - Cabinet Vigo - membre du réseau GESICA

Emmanuel Daoud
Avocat au barreau de Paris - Cabinet Vigo - Membre du réseau GESICA

« Pompe à data », « Permis officiel d'espionnage industriel », « Arme commerciale », « Système de lutte contre l'intelligence économique » ... L'adoption du *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*) ou, en français, la « loi clarifiant l'usage légal des données hébergées à l'étranger » a provoqué la parution de nombreux articles aux titres alarmistes.

Accusée d'avoir été votée en catimini par le Congrès américain et sans le moindre débat parlementaire, la loi a suscité des critiques dès sa promulgation par le Président Donald Trump, le 23 mars 2018.

Sur le fond, et en résumé, le *Cloud Act* permet aux autorités américaines d'obtenir de toute société « de droit américain » détenant des *data centers* en dehors des États-Unis la divulgation de données, dans le cadre d'investigations criminelles, en s'adressant directement aux sociétés traitant ou conservant ces données. Concrètement, la police, la justice et l'administration américaines pourront avoir accès à des données sans considération du lieu où se trouvent celles-ci, dès lors que la société qui les conserve est « de droit américain » (une filiale européenne de société américaine par exemple), sans en informer la personne concernée. Les sociétés concernées sont Microsoft, Google, IBM, AWS, Salesforce, Oracle, etc.

Naturellement, les organismes de défense des droits fondamentaux s'insurgent. Les critiques pleuvent : ingérence numérique et juridique, hégémonie américaine, atteinte à la vie privée, loi liberticide...

De même, les entreprises ayant recours à des prestataires « de droit américain » pour héberger leurs données s'inquiètent de leur perte de contrôle sur les données de leurs clients, mais aussi de la confidentialité de leurs secrets d'affaires ainsi que d'une possible divulgation de leurs actifs incorporels.

Les partisans du *Cloud Act* arguent que le texte n'organise pas un droit d'accès absolu aux données et qu'il prévoit un contrôle systématique par un juge du bien-fondé de ces demandes de transmission de données. Ils invoquent également la possibilité pour les sociétés « de droit américain » de mettre en œuvre des mécanismes juridiques permettant de s'opposer à ces demandes de transmission des données, dans le cas où le *Cloud Act* contreviendrait à la réglementation du pays dans lequel elles se trouvent.

Cependant, les garanties mises en place pour contrôler son application sont-elles suffisantes ? Quels risques réels génère ce texte pour les entreprises françaises

confiant leurs données à des prestataires « de droit américain » ? Quelle est la nature de ces risques ? Quelles précautions ces entreprises peuvent-elles prendre ?

I - POURQUOI UN *CLOUD ACT* ?

En 2013, les autorités américaines ont demandé à *Microsoft Ireland* la communication de données relatives à un citoyen américain hébergées en Irlande, sur le fondement d'une loi américaine, le *Stored Communication Act* (ci-après SCA).

Le SCA permet en effet aux autorités américaines de requérir les données et les communications d'un utilisateur auprès des fournisseurs de services de traitement électronique, pour les besoins de procédures répressives. Cette disposition constitue une exception au principe posé par le même texte garantissant la confidentialité des données de l'utilisateur et de ses communications stockées par les fournisseurs.

Craignant de perdre la confiance de ses clients, *Microsoft* a contesté l'application du SCA au motif que les données étaient localisées en Irlande, et demandé à ce que soit empruntée la voie de la coopération judiciaire internationale, et plus précisément une procédure prévue par le *Mutual Legal Assistance Treaty* (MLAT).

La cour d'appel du second circuit de New York ayant conforté l'analyse de Microsoft, le ministère américain a décidé de porter l'affaire devant la Cour suprême des États-Unis.

L'adoption du *Cloud Act* a eu lieu avant même que la Cour suprême ne se prononce.

La réaction de Microsoft est ambiguë. La société a dans un premier temps salué l'adoption du texte pour la clarification qu'il a apportée sur le cadre d'accès aux données des utilisateurs par les autorités. Puis, au mois de septembre 2018, la société a publié, sur un ton quelque peu craintif, un appel (« *call* ») à l'application, par les autorités américaines et étrangères, de six principes protecteurs de la vie privée des utilisateurs qui seront exposés ci-dessous.

II - QUE PRÉVOIT EXACTEMENT LE *CLOUD ACT* ?

Le *Cloud Act* prévoit essentiellement deux dispositions.

En premier lieu, toute société « de droit américain », quelle que soit sa situation géographique, est tenue, sous certaines conditions développées ci-après, de communiquer les données placées sous son contrôle sur demande des autorités américaines.

En second lieu, les gouvernements étrangers ont la possibilité de conclure des accords internationaux (« *executive agreements* ») avec les États-Unis, autorisant les autorités respectives de chacun des pays parties à demander la communication de données directement aux fournisseurs de services de stockage électronique situés sur le sol du pays étranger.

L'objectif affiché par le *Cloud Act* est celui du rapprochement du temps de l'investigation criminelle de celui de la criminalité.

III - DES GARDE-FOUS INSUFFISANTS

À première vue, le *Cloud Act* ne confère pas aux autorités américaines un droit d'accès absolu et illimité aux données des utilisateurs.

Tout d'abord, le *Cloud Act* ne s'applique qu'aux sociétés « de droit américain », c'est-à-dire aux sociétés constituées aux États-Unis, filiales européennes de sociétés américaines comprises.

De plus, le texte prévoit que les autorités américaines ne peuvent requérir la communication de données de la part des prestataires de services informatiques « de droit américain » que dans deux situations particulières.

La demande de communication peut, en premier lieu, être formulée lorsque les autorités américaines disposent d'un titre délivré par une juridiction : un mandat (ou « *warrant* »). Ce titre est délivré s'il existe une présomption sérieuse que la personne a commis ou est sur le point de commettre une infraction pénale et que les informations visées par le mandat sont utiles à l'enquête.

Les données peuvent également être transmises sur le fondement de *court orders*, autrement dit sur autorisation d'une juridiction. Pour l'obtenir, il doit être démontré que l'accès est nécessaire à l'évolution d'une procédure de nature pénale. Dans ce dernier cas, le fournisseur « de droit américain » peut contester l'ordre qui lui a été remis de divulguer aux autorités américaines les données de communication, devant une juridiction de première instance ou d'appel, par voie d'action ou d'exception.

Peut-on affirmer pour autant qu'un contrôle effectif, indépendant et impartial est garanti dans la mise en œuvre du *Cloud Act* ? Nous n'avons à notre sens pas assez de recul pour pouvoir l'affirmer de manière certaine. De même, nous pouvons imaginer que les juridictions américaines seront tentées par une vision « patriotique » des litiges qui leur seront soumis dans le cas où les intérêts fondamentaux des États-Unis entreraient en conflit avec ceux d'une entreprise étrangère.

Par ailleurs, dans chacune de ces situations, le *Cloud Act* prévoit que le fournisseur de services de traitement électronique « de droit américain » a également la possibilité de s'opposer, devant la juridiction américaine, à la transmission des données, au motif que celle-ci le placerait dans une situation de conflit de lois qui le conduirait à méconnaître la législation du pays dans lequel les données sont localisées, et à l'exposer à des sanctions.

En Europe, l'obstacle réglementaire principal à l'application du *Cloud Act* est le règlement européen (UE) 2016/679 sur la protection des données (RGPD) entré en application en mai 2018.

Pour rappel, le RGPD est applicable aux traitements des données à caractère personnel effectués par l'établissement d'un responsable du traitement ou d'un sous-traitant situé sur le territoire de l'Union européenne[1]. Ainsi, les fournisseurs de services de traitement électronique « de droit américain » situés sur le sol français ou européen sont soumis aux dispositions de ce règlement.

Concernant les demandes d'accès aux données par les autorités, l'article 48 du RGPD prévoit :

« 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 État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre ».

En application de cette disposition, une décision d'une juridiction américaine autorisant les autorités américaines à requérir des données auprès d'un prestataire « de droit américain » soumis au RGPD, ne suffit pas pour obtenir leur divulgation. Le transfert n'est autorisé par le RGPD que dans le cas où cette décision est fondée

[1] RGPD, art. 3.

sur un accord international, tel qu'un traité d'entraide judiciaire, conclu entre les États-Unis et un État membre.

Or, aucun accord de cette nature n'a à ce jour été conclu entre les États-Unis et l'Europe.

En conséquence un prestataire de services américain situé sur le sol européen faisant droit à une demande de transmission de données émanant d'une autorité américaine fondée sur le *Cloud Act* méconnaitrait les dispositions du RGPD. À l'inverse, le prestataire se soumettant aux dispositions du RGPD, et refusant donc de communiquer ces données, risquerait de se voir sanctionner au regard des dispositions du *Cloud Act*.

En application du principe de courtoisie internationale, l'on peut espérer que les juridictions américaines retiendront l'application de l'article 48 du RGPD qui fait obstacle, en principe, à l'application du *Cloud Act*, et renonceront ainsi à la demande de transmission des données. Cependant, la décision reviendra *in fine* à ces juridictions qui disposeront d'une totale liberté d'appréciation, compte tenu de l'absence de précédent jurisprudentiel dans l'application de ce principe[2]. Le *Cloud Act* prévoit enfin la possibilité de conclure un accord international (« *Executive Agreement* ») avec les États-Unis. Dans le cadre de ces accords, qui ne peuvent viser que les infractions les plus graves (« *serious crimes* »), les autorités de poursuite pourront obtenir la communication des données de communication qu'elles estiment être pertinentes dans le cadre de leurs investigations, en s'adressant directement aux sociétés traitant ou conservant ces données. La consultation d'un juge ne sera donc pas nécessaire dans ce cadre, ce qui est de toute évidence problématique.

C'est dans ce contexte que la société *Microsoft* a imaginé et publié six principes fondamentaux, dans l'espoir qu'ils soient repris par les législations nationales et les accords internationaux à venir. La société revendique ainsi notamment un droit universel pour chaque utilisateur d'être informé de la communication de ses données aux gouvernements, l'obligation d'obtenir une autorisation judiciaire avant toute transmission des données aux autorités, l'instauration d'une procédure claire et précise permettant la contestation de l'ordre de communiquer les données, ainsi que l'intégration d'un principe de transparence permettant au public de connaître précisément les règles applicables à la protection des données.

Nous ne pouvons que saluer cette initiative, tout en ayant conscience de l'intérêt économique et réputationnel qu'a *Microsoft* à tenter de rassurer ses utilisateurs.

IV - LES RISQUES SOULEVÉS PAR LE *CLOUD ACT*

À ce jour, nous ignorons si, quand et avec qui (Union européenne ou pays membres) un accord international sera conclu avec les États-Unis. En revanche, tout le monde s'accorde pour dire que la procédure de décision sera longue. Pour l'heure, il s'agit donc pour les prestataires français et européens ainsi que pour les utilisateurs de s'adapter à cette situation de grande insécurité juridique, et de prendre leurs décisions en considération des enjeux que cette problématique soulève.

Pour les sociétés « de droit américain », le premier enjeu est d'ordre réputationnel. D'un côté, une soumission aveugle de ces sociétés aux demandes des autorités américaines risquerait de mettre à mal la confiance de ses utilisateurs. D'un autre côté, une réticence risquerait de le rendre responsable des conséquences d'éventuels actes criminels, y compris en matière de terrorisme.

L'enjeu est également de nature financière. Le prestataire « de droit améri-

[2] F. G'sell, Faut-il redouter le *Cloud Act* ? La réponse est oui. Pour l'instant, https://bit.ly/2P0q4ww.

CE QU'IL FAUT RETENIR

Le *Cloud Act* va-t-il nous conduire à une « Data war » comme le prédisent certains commentateurs ?
Les termes employés sont forts ; nous pouvons cependant nous inquiéter que des secrets d'affaires soient dévoilés au préjudice des entreprises européennes ou françaises. Et comment ne pas craindre que des atteintes irréversibles à la vie privée ne soient portées à l'occasion de l'application du *Cloud Act* ?
Il est donc conseillé aux utilisateurs de prendre leurs précautions en privilégiant les solutions existantes, certes perfectibles : stipuler une clause contraignant le prestataire informatique à s'opposer au *Cloud Act* tant qu'un accord international n'a pas été signé entre l'Union européenne et les États-Unis, ou avoir recours à des prestataires informatiques souverains ou de droit européen.
Enfin, si la localisation géographique de nos données ne constitue plus une garantie certaine de confidentialité, peut-être la solution réside-t-elle, comme le propose la société Microsoft, dans l'élaboration de principes universels de protection des internautes.

cain » devra mener une comparaison entre les risques financiers encourus en cas de non-respect du *Cloud Act* et en cas de violation des dispositions du RGPD.

Pour les utilisateurs de services offerts par les sociétés « de droit américain », les risques diffèrent. Concernant les entreprises, nul ne peut affirmer avec certitude que le *Cloud Act* ne constitue pas un risque de voir leurs secrets d'affaires dévoilés ou la confidentialité de leurs actifs incorporels menée à mal.

Les personnes physiques s'exposent quant à elles à un fort risque d'atteinte à leur vie privée.

V - QUELLES PRÉCAUTIONS PRENDRE POUR ASSURER LA CONFIDENTIALITÉ DE SES DONNÉES ?

Diverses solutions peuvent être proposées pour préserver la confidentialité de ses données.

En premier lieu, la stratégie globale d'hébergement des données peut être redéfinie. Il s'agit de privilégier le stockage des données dans des *data centers* de droit européen. De manière plus radicale, les utilisateurs peuvent faire appel à des acteurs offrant des alternatives souveraines, c'est-à-dire implantés en France et de droit français. Il conviendra dans tous les cas de veiller à introduire une clause dans les contrats interdisant le recours à des sous-traitants « de droit américain ».

Toutefois, les sociétés françaises sont parfois contraintes, pour des raisons économiques ou techniques, de faire appel à des prestataires « de droit américain ».

Dans ce cas, une stratégie d'hébergement modulaire, par application, peut être mise en place. Les prestataires « de droit américain » conserveront les données les moins « sensibles » et l'utilisateur pourra avoir recours au *Cloud* souverain ou européen pour les données confidentielles. L'utilisateur optant pour cette solution doit toutefois être conscient des difficultés de mise en place et des coûts de gestion que cela implique.

Dans le cas où l'entreprise ne pourrait ou ne souhaiterait pas faire appel à une société française ou européenne pour le stockage de ses données pour des raisons économiques ou techniques, celle-ci pourra tenter d'exclure contractuellement l'application du *Cloud Act*. L'idée serait d'inclure une clause au contrat conclu avec le prestataire « de droit américain » énonçant expressément que le RGPD constitue un cas permettant au prestataire d'opposer l'exception de violation de la législation d'un pays étranger prévue au *Cloud Act* précédemment exposée. Les conditions dans lesquelles les prestataires « de droit américain » pourraient être amenés à donner accès aux données pourront également être définies, en prenant soin de les limiter le plus possible.

Cependant, il est évident que la marge de négociation contractuelle avec les sociétés américaines de grande envergure qui soumettent le plus souvent des contrats d'adhésion à leurs clients est quasi-nulle.

De plus, la responsabilité du prestataire américain pourra certes être engagée en cas de non-respect de ses engagements contractuels, mais la divulgation des données ne pourra aucunement être empêchée.