Les principales questions juridiques posées par l'informatique en nuage

Nguyen Nhu Ha

***Résumé*—Les implications juridiques de l'utilisation de solutions de Cloud computing sont largement similaires à celles de tout contrat d'externalisation avec une tierce partie. Une différence majeure en utilisant un fournisseur de Cloud découle de la souplesse du mouvement des données entre les serveurs qui peuvent être situés dans diverses parties du monde. Il est donc difficile de déterminer quelle loi s'applique à un moment donné pour les données, notamment parce que les données peuvent également avoir été fragmentées en fonction notamment de la disponibilité ou de la capacité du service Cloud. Cet article recense les principales questions juridiques posées par l'informatique en nuage afin de déterminer l'ordre juridique qui assure une protection adéquate.**

***Mots clés*—L'informatique en nuage, Cloud computing et droit; Propriété intellectuelle; Vie privée; Informations personnelles.**

1. INTRODUCTION

COMME nous le savons, l'informatique en nuage (ou le Cloud computing) n'est pas une technologie nouvelle. Les principales économies du monde ont toutes mis au point leur propre politique ou stratégie de technologie de communication de l'information nationale afin de cultiver et d'orienter le développement de l'industrie de Cloud computing émergent et d'équilibrer les avantages des différentes parties prenantes dans le nouvel environnement de l'informatique en nuage. Il existe diverses ramifications juridiques pour fournir des services Cloud dans le contexte de l'utilisation de dispositifs intelligents dans l'UE, les États-Unis et l'APEC, etc.

Received: 10-7-2018, Accepted: 10-11-2018, Published: 24-11-2018.

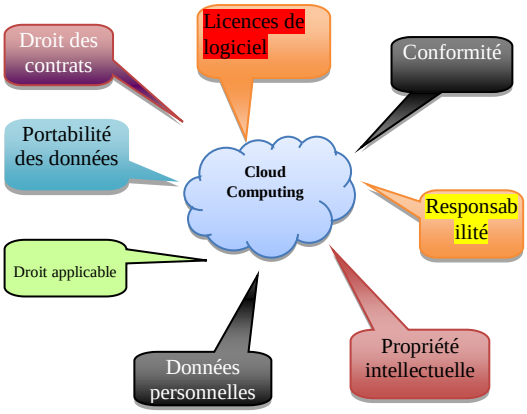
Nguyen Nhu Ha, Vietnam National University, Hanoi - School of Law (e-mail: nhuha.nguyen@hotmail.fr).

La stratégie de l'informatique en nuage du gouvernement fédéral américain fournit une stratégie globale qui comporte de multiples niveaux de gouvernance [1]. Un élément essentiel de la stratégie est la politique du « *nuage d'abord* ». Il met en place une « *exigence de haut en bas* » pour toutes les instances exécutives de transition active informatiques existantes pour le « *Cloud Computing* » pour une période de 18 mois [2]… ; La Commission européenne a également annoncé son engagement pour le Cloud Computing et un plan à long terme pour l'établissement d'un ensemble commun de règles pour proposer une structure de marché cohérente entre les États membres de l'UE pour les fournisseurs de services de l'informatique en nuage [2]. Plus précisément, la politique de l'UE mettra l'accent sur l'activation du Cloud en vue de faciliter une adoption plus rapide du Cloud Computing dans tous les secteurs de l'économie qui peuvent diminuer le coût des TIC, et lorsqu'il est combiné avec de nouvelles pratiques d'affaires numériques, peut accroître la productivité, la croissance et l'emploi [2] …

Bien qu'un certain nombre de grandes économies aient élaboré leurs propres stratégies nationales, des réglementations ou des politiques visant à promouvoir l'application à large échelle des nouveaux modèles de technologie de l'informatique en nuage et la croissance rapide des industries de Cloud computing, une question importante est de savoir si ces nouveaux choix techniques sont en fait légaux. Effectivement, les questions juridiques engendrées par l'informatique en nuage sont extrêmement diverses. Elles concernent : la sécurité, la date, la répartition des risques, les problèmes de rétention de limitations contractuelles des tiers, la conformité aux réglementations, le contrôle sur l'emplacement physique des données, la violation de la sécurité, la protection des secrets commerciaux, le hacking du fournisseur de services de Cloud, la responsabilité financière du Cloud et une cour compétente, du

vendeur de droits, le droit de propriété intellectuelle, et les questions relatives aux accords de Cloud computing, etc.

Selon mon observation, en général, les principaux domaines juridiques à envisager avec l'informatique en nuage sont : la sécurité des données et la conformité à la protection des données ; la compétence ; la confidentialité ; la liberté d'information ; la propriété intellectuelle ; le droit des contrats (y compris l'exécution de contrat). En d'autres termes, les principales questions juridiques dans l'informatique en nuage naviguent entre droit applicable, les droits de propriété intellectuelle (le droit d'auteur, le droit *sui generis*, les brevets), le droit des contrats, les licences de logiciel, la protection des données personnelles, la portabilité des données, la conformité et la responsabilité. Le schéma suivant représente une vue d'ensemble de celui-ci :



2. DROIT APPLICABLE

Un premier défi juridique se rapporte à la définition de la législation applicable[1] sur le nuage quant aux relations essentielles pour l'attribution des responsabilités, des obligations et des recours légaux. En l'absence d'une entente contractuelle « *entre le fournisseur de Cloud et le consommateur, une variété de lois, qu'elles soient ou non contradictoires, peuvent s'appliquer*» [3]. En effet, il n'est pas toujours clair de savoir où le fournisseur de l'informatique en nuage a ses établissements ou ses points de service et quelle entité juridique « *effectue les services : la partie de la prestation de services pourra être effectuée par des filiales des fournisseurs de Cloud computing dans différents endroits ou même par des sous-traitants*[2] » [4]. En outre, différents services peuvent être fournis, y compris le traitement de renseignements personnels ainsi que des données non personnelles et diverses exigences légales des régimes de droits applicables peuvent être abordées.

La directive 2000/31/CE « *complète le droit communautaire applicable aux services de la société de l'information sans préjudice du niveau de protection, notamment en matière de santé publique et des intérêts des consommateurs, établi par les instruments communautaires et la législation nationale les mettant en œuvre dans la mesure où cela ne restreint pas la libre prestation de services de la société de l'information* » [5]. À mon avis, la Directive 2000/31/EC sur le commerce électronique pour les services de la société de l'information n'aborde pas la question de façon appropriée. Son application est discutable, car l'emplacement géographique est le critère essentiel et la directive ne s'applique pas sur les relations à l'extérieur de l'UE.

D'autre part, je pense que, l'insécurité décrite peut être facilement résolue contractuellement pour déterminer la loi applicable, qui est actuellement la pratique standard. Dans la pratique cependant, des discussions peuvent survenir sur quelle loi choisir, puisque la plupart du temps, les fournisseurs de Cloud ont tendance à imposer la loi de leur établissement. En tant que tels, des négociations sont souvent nécessaires pour arriver à un accord, résultant parfois même dans l'application de la loi d'un pays tiers afin d'assurer la « *neutralité* ». Une façon d'éviter cela est déjà de prendre en compte le droit applicable en tant que condition requise à l'appel d'offres, de sorte que les fournisseurs de Cloud sont au courant qu'il s'agit d'un élément clé.

[1] L'expression « *loi applicable* » est une notion propre au droit international privé (le droit international privé, entendu ici au sens large, désigne l'ensemble des règles juridiques régissant les relations internationales entre personnes privées). Voir plus sur le glossaire de la Commission européenne sur le site : http://ec.europa.eu/ : Elle indique la loi nationale qui régit une question de droit déterminée présentant un caractère international. Il faut savoir qu'un juge, lorsqu'il est saisi d'un litige, n'applique pas nécessairement sa loi nationale pour résoudre ce litige. On détermine la loi applicable en utilisant le mécanisme des règles de solution des conflits de lois.

[2] Si un fournisseur de Cloud fonctionne avec un sous-traitant établi aux États-Unis, par exemple, de l'US Patriot Act peut être applicables, même lorsque ce nuage prestataire est établi en Europe.

3. PROPRIÉTÉ INTELLECTUELLE

Les droits de propriété intellectuelle (DPI) sont, généralement, les droits accordés aux créateurs et propriétaires des œuvres qui sont le résultat de la créativité intellectuelle. Ces œuvres peuvent être dans les domaines industriels, scientifiques, littéraires ou domaines artistiques. Les types de DPI considérés ici sont le droit d'auteur, le droit des bases de données, et les brevets.

Un brevet protège les caractéristiques et processus qui permettent le fonctionnement des choses, permettant aux inventeurs de tirer profit de leurs inventions. Il donne au titulaire du brevet le droit d'empêcher quiconque de fabriquer, d'utiliser, d'importer ou de vendre l'invention sans permission.

Le droit d'auteur protège essentiellement les œuvres originales, cela comprendra des œuvres comme matériaux d'enseignement et de recherche et les blogs. Les logiciels (ou programmes informatiques) et bases de données peuvent être protégés comme des œuvres littéraires, en plus d'autres droits possibles tels que les droits des bases de données. Par exemple, une université ou un collège sera habituellement le propriétaire du droit d'auteur de l'œuvre créée par son personnel, sauf s'il existe un accord différent. Un titulaire de droit d'auteur a le droit de contrôler la reproduction, l'adaptation, l'édition de performance et de diffusion de l'œuvre, et dans quelles conditions cela peut être fait. En plus de la création de matériaux auxquels s'appliqueront le droit d'auteur, le personnel et les étudiants des collèges et des universités sont susceptibles d'utiliser les travaux qui appartiennent à autrui de façon intensive. La conformité avec la législation sur le droit d'auteur reste nécessaire dans la migration vers le Cloud.

En plus de toute la protection du droit d'auteur, le droit sur les bases de données peut protéger une base de données. Le droit de base de données s'applique dans l'UE et est destiné à protéger et récompenser l'investissement dans la création et l'arrangement de bases de données. Si une base de données est enregistrée sur un serveur dans un État membre de l'UE, alors il est clair que le droit sur les bases de données peut s'appliquer, à condition bien sûr que la base de données réponde aux critères énoncés ci-dessus pour la protection. Toutefois, la recherche a posé la question de savoir où la base de données est conçue ou où elle est enregistrée (ce sont des points clés pour résoudre les problèmes) et si ce sont des endroits différents conformément à la législation. Cela peut potentiellement affecter l'application du droit des bases de données ou non comme lorsqu'il n'y a pas de droits sur les bases de données, par exemple, aux États-Unis. Selon moi, comme il n'y a pas de décision de justice sur l'interprétation, il existe une certaine incertitude quant à savoir si une base de données enregistrée sur un serveur non-UE est protégée par le droit sur les bases de données.

4. DROIT DES CONTRATS

L'inclusion des indemnités pour les droits de propriété intellectuelle dans les contrats de l'informatique en nuage reste importante, parce que les clients ont à se fier à un fournisseur de services pour nous assurer que les problèmes de licence du logiciel ont été résolus de manière à fournir au client le droit d'utiliser le logiciel en tant que partie du service.

Visant à protéger les droits de propriété intellectuelle des fournisseurs pour leur propre logiciel et la mesure dans laquelle les clients peuvent profiter du savoir-faire acquis dans une relation contractuelle à court terme qui peut être résiliée à bref délai par un client. Les utilisateurs du Cloud computing doivent être conscients de la possibilité de violation de brevet grâce à l'utilisation d'arrangements de l'informatique en nuage. La protection par brevet est de plus en plus disponible pour les logiciels aux États-Unis et, dans une moindre mesure, dans l'UE. Les arrangements de l'informatique en nuage sont établis sur une base internationale, l'indemnité de droits de propriété intellectuelle doit être suffisamment large pour protéger les clients des services Cloud dans toutes les juridictions dans lequel le logiciel sera utilisé.

Pour atténuer les risques posés par l'incertitude sur les licences de logiciels, le client peut souhaiter demander une indemnité pour atteinte aux droits de propriété intellectuelle. L'indemnité peut aussi être demandée relativement à la possibilité de contrefaçon d'un brevet. Le client peut également demander une indemnité pour perte subie à la suite de matériel effacé ou interruption de service. La pratique du marché à ce niveau indique que des indemnités peuvent donc être très difficiles à négocier. Sur l'objet d'interruption de service en particulier, les clients peuvent plutôt se concentrer sur les accords de niveau de service relatifs à la disponibilité des services ; et bien entendu à faire

preuve de diligence raisonnable de manière approfondie sur les fournisseurs potentiels. Les intégrateurs peuvent aussi être plus disposés à accepter la responsabilité.

À mon avis, les indemnités de DPI devraient être négociées avec succès dans les contrats du Cloud, ils doivent être suffisamment larges pour protéger le bénéficiaire visé dans toutes les juridictions dans lesquelles le service sera utilisé/maintenu.

5. LICENCES DE LOGICIEL

Bien que les contrats de l'informatique en nuage se rapportent à la prestation de services plutôt qu'à la fourniture de logiciels à des clients, d'après moi, des licences logicielles appropriées doivent encore être accordées au client pour leur permettre d'utiliser légalement et correctement le logiciel nécessaire sans risquer de commettre une infraction au droit d'auteur. C'est parce que les licences de l'informatique en nuage sont habituellement très étroites et limitées à l'utilisation de l'application en ligne pour leurs propres fins commerciales. Les clients n'ont aucun droit de faire des copies ou modifications ou d'apporter des améliorations aux logiciels, et ils ne peuvent pas les distribuer ou les partager sous licence à des tiers.

De plus, le fournisseur de service ne saura pas toujours détenir les droits de propriété intellectuelle sur le logiciel qui fait l'objet de service grâce au Cloud computing. Lorsque cela est le cas, le prestataire de services devra prendre des dispositions pour que le droit de sous-licence du logiciel à ses clients, ou d'une licence directe, soit conclu entre les clients et le concédant de licence auprès du prestataire de services pour gérer les licences tierces. Toutefois, toutes les autres questions relatives à la fourniture du logiciel, telles que la livraison, l'installation et la configuration requise, devraient être traitées dans des accords distincts entre le client et le fournisseur de service.

Pour le cas de la restriction de licence : les licences de logiciel peuvent être propres à un lieu précis et nécessiteront un examen afin d'assurer une conformité continue lorsqu'on envisage un service d'infrastructure Cloud. Un établissement aura convenu contractuellement avec les éditeurs par le biais de l'actuelle ressource pédagogique des licences de sauvegarder les ressources. Le fournisseur de Cloud doit donner l'assurance que tous les efforts seront faits pour empêcher l'accès par des utilisateurs sans licence et pour empêcher toute utilisation non autorisée des ressources sous licence[3].

6. DONNÉES PERSONNELLES

Les lois sur la protection des données personnelles font partie intégrante du cadre du Cloud computing. Dans un environnement de Cloud, les données personnelles et non personnelles peuvent être traitées. Dans la mesure où des données personnelles sont traitées, la législation européenne de protection des données entre en jeu, ce qui apporte certains défis judiciaires relatifs au cadre législatif existant comme l'application de la législation sur la protection des données ; les données personnelles sensibles ; la qualification des différents acteurs dans un environnement de Cloud ; la loi applicable et la compétence ; le transfert de données vers des pays/non-EEE non-UE. Dans l'UE, ils sont actuellement régis par la Directive sur la protection des données [6] et, après un bon processus législatif, par le nouveau règlement relatif à la protection des données [7]. Ils veillent à ce que les données à caractère personnel, étant des données à partir desquelles une personne peut être identifiée, soient soumises à une protection supplémentaire et ne soient pas divulguées aux parties qui ne les exigent pas et ne sont pas en droit de recevoir ces informations.

De plus, je pense que l'informatique en nuage est sans conteste une des affaires fort attrayantes, offrant de tels avantages comme un court délai, un investissement minimal et la facilité d'utilisation pour tout projet d'entreprise ou opération qui requiert l'assistance informatique[4] [8]. Au milieu de l'attrait de la technologie de l'informatique en nuage, toutefois, il est important de garder à l'esprit les risques inhérents au fait que bon nombre de ses caractéristiques sont liées aux données personnelles. Les risques concernent

[3] L'accord de licence, peut indiquer que seules les personnes autorisées, par exemple le personnel et les étudiants, peuvent afficher la ressource numérique ou le stockage de documents numériques et peuvent être restreintes en vertu de la licence pour les serveurs locaux. Il y a une possibilité d'accès par une tierce partie (c.-à-d. le fournisseur de Cloud et leurs sous-traitants) et le nuage n'est intrinsèquement pas un emplacement spécifique. Des ententes contractuelles avec les fournisseurs de vos ressources, sur l'accès et l'emplacement, doivent être prises en compte dans le contrat avec le fournisseur de Cloud via des garanties.

[4] Gartner, leader dans le domaine de la recherche et de conseils indépendants, a estimé que le marché du Cloud passerait de 111 milliards de dollars US en 2012 à 244 milliards $ US en 2017.

principalement le manque apparent de contrôle et de surveillance de la protection de la vie privée de l'utilisateur des données conservées lorsqu'il confie des données personnelles à un tiers comme un fournisseur de l'informatique en nuage à des fins de traitement ou de stockage.

Le Groupe de l'article 29, institué par l'article 29 de la Directive relative à la protection des données 95/46/CE, est composé de représentants des autorités de protection des données (DPA) de chaque État membre de l'Union européenne, le contrôleur européen de la protection des données et la Commission européenne. Parmi ses objectifs sont d'informer la Commission européenne et de formuler des recommandations à l'Union européenne sur toutes les questions liées à la protection des données à caractère personnel. Il estime que l'absence de contrôle et le manque d'information sur les opérations sont deux risques majeurs associés à l'utilisation de l'informatique en nuage [9].

7. PORTABILITÉ DES DONNÉES

Une préoccupation majeure dans un environnement Cloud, est la portabilité des données : comment un consommateur de Cloud peut s'assurer, s'il souhaite migrer vers un autre fournisseur de l'informatique en nuage ou rapatrier le service localement, qu'il reçoit les données efficacement et que de traces ne pas sont laissées avec le nuage du fournisseur originel ? Comment peut-il, en d'autres termes, éviter un « *verrou fournisseur* » ? Je pense que, cette préoccupation en particulier n'est soulevée qu'à l'égard de la faillite ou de circonstances imprévues, de risquer un transfert correct de retour des données. Elle peut également concerner l'utilisateur final du Cloud : comment un utilisateur final Cloud, en cas d'incidents, peut obtenir ses données retour dans leur intégrité et dans un délai raisonnable ? Ce défi est particulièrement important dans un environnement Cloud du secteur public, depuis peut-être que des données plus sensible sont stockées dans le Cloud (données sur la santé, les données fiscales...) ou des actions immédiates doivent être prises pour des raisons de sécurité nationale[5]. La solution réside en stipulant clairement dans le contrat de Cloud, les diverses circonstances (faillite, cessation, etc.) et les modalités de transfert, avec une attention particulière pour les niveaux de service, les échanciers, les côts et l'aide. En outre, il peut être envisagé, depuis le début de la collaboration, de travailler avec un fournisseur de service de « *stand-by* » qui exécute (certains) services en parallèle et peut immédiatement prendre le relais en cas de besoin.

En Union européenne, le nouveau projet de Règlement sur la protection des données[6] fait des efforts en ce qui concerne la portabilité des données vers les propriétaires des données, ce qui est un signal positif. Conformément à l'article 15(2), la personne concernée a le droit — ce qui peut être considéré comme un droit spécifique d'Internet — d'obtenir du responsable du traitement, une copie des profils téléchargés sur des plates-formes Internet dans un format adapté pour un traitement ultérieur et une utilisation par lui ou d'elle-même. Ce profil ne peut pas contenir d'obstacles techniques ou autres de sorte qu'il peut être téléchargé sur la plate-forme Internet d'un autre fournisseur de service, donc en pratique permettant un transfert direct d'un contrôleur à un autre, à la demande de la personne concernée. Le cadre réglementaire de l'UE définit un service de « *communications électroniques* » [10] comme un service entièrement ou principalement composé d'acheminement des signaux sur les réseaux électroniques, y compris des services de télécommunications, mais exclut les services fournissant ou exerçant un contrôle rédactionnel ou un contenu transmis au moyen des réseaux de communications électroniques et de services [11].

Théoriquement, selon Jasper Sluijs [12], les services de l'informatique en nuage peuvent être rassemblés sous le terme de services électroniques si l'activité est axée sur la prestation de services sous forme d'envoi de signaux sur les réseaux des communications électroniques. La directive « *accès* » de l'UE [13] contient des exigences en

[5] Par exemple, en Belgique, l'article 14 de la Loi sur le registre des personnes physiques du 8 août 1983, prévoit l'inscription des personnes physiques doit être détruit en temps de guerre ou à l'invasion de l'ennemi, selon les conditions et modalités fixées par le roi.

[6] Le 15 décembre 2015, la Commission européenne, le Parlement européen et le Conseil des ministres sont parvenus à un accord sur la protection des données générales Règlement (GDPR), après des mois de « trilogue » des négociations.

maîtrise d'interconnexion avec des pouvoirs correspondants pour les organismes nationaux de réglementation : cependant, ces exigences ne concernent que des prestataires de services de communications électroniques. Par conséquent, en accord avec Sluijs, le cadre réglementaire semble de peu d'appui pour l'amélioration de la portabilité des données et l'interopérabilité des services en Cloud [14].

8. CONFORMITÉ

Dans la conformité[7], l'informatique en nuage a le potentiel d'offrir la possibilité de reconfigurer dynamiquement les ressources informatiques lorsque la demande de ressources informatiques augmente ou diminue. Selon moi, un fournisseur de services au client (FSC) doit être capable de répondre à cette demande. Dans les cas où un FSC ne parvient pas à fournir cette demande, le FSC pourrait être forcé d'impartir des données organisationnelles à un autre FSC, amplifiant le problème des questions liées à la confidentialit. Ainsi, l'incidence des règlements sur la protection des renseignements personnels est la plus frappante entre l'informatique Cloud externe et l'informatique traditionnelle. Je pense que les règlements sur la protection des renseignements personnels ne sont clairement pas adaptés pour résoudre toutes les questions de protection de la vie privée liées au Cloud Computing. Il est nécessaire de mûrir d'avantage la conscience nécessaire sur les thèmes et sur le règlement actuel pour devenir une bonne première étape pour remédier à cette situation.

Actuellement, il y a plusieurs autres lois et règlements des États-Unis relatifs à la conformité qui sont : la famille Droits éducatifs et Loi sur la protection des renseignements personnels (FERPA) ; Gramm-Leach-Biley Act (GLBA) ; Health Insurance Portability and Accountability Act (HIPAA) ; technologies de l'information sur la santé pour le développement économique et la santé clinique (HITECH) État Sarbanes Oxley Act ; lois et réglementations (pour les données) ; notification de violation de l'article 5 de la Loi sur la FTC. Dans le cas de l'UE, il ya des directives et règlement mentionné ci-dessus, sourtout, la Directive 95/46/CE protection des données qui aidera à harmoniser les lois sur la protection de la vie privée qui existent dans les différents États membres de l'Union européenne et fournira une norme de base sur la protection des données personnelles et de la vie privée.

Comme d'autres dispositions externalisées, un bon accord de niveau de service est essentiel. L'informatique en nuage « *n'est pas sans bouleverser les contrats « traditionnels » du droit d'Internet tels que le contrat de licence de logiciel*[8] *»* [15]. Ceci doit refléter les besoins de l'institution dans des domaines tels que la sécurité des données, la continuité de l'activité et la planification en cas de catastrophe. Il est essentiel que le fournisseur de Cloud[9] soit fiable et utilise la protection des données, et que la sensibilisation à la sécurité des données se reflète dans les termes du contrat. Des inquiétudes sur les données verrouillées pour un fournisseur de nuage ont été exprimées, en particulier à l'égard des fournisseurs et des institutions nouvellement créés qui doivent proposer un contrat de pré-diligence nécessaire pour évaluer les risques potentiels. Les risques en matière de restitution des données en cas d'insolvabilité ou dans une série de situations comme l'endroit où le fournisseur de Cloud a externalisé une partie de ses ressources par exemple le stockage des données, doivent être connus dès le départ.

[7] Une plus grande harmonisation des cadres juridiques et réglementaires pertinentes pour être mieux adaptées pour aider à assurer un niveau élevé de protection de la vie privée, la sécurité et la confiance dans les environnements de l'informatique en nuage. Par exemple : établir des règles plus efficaces pour la reddition de comptes et la transparence contribue à un niveau élevé de protection de la vie privée et de la sécurité dans les règles de protection des données et à l'expansion des régimes de notification de violation pour couvrir les fournisseurs de l'informatique en nuage.

[8] En effet, le Cloud permet aux entreprises de disposer de leurs applications via Internet, sans que le logiciel soit préalablement installé sur le poste de chacun des utilisateurs. Le développement rapide du Cloud (*de nombreux grands acteurs du logiciel comme Microsoft ou Oracle proposent déjà leurs logiciels en cloud*) est amené à faire évoluer profondément la gestion traditionnelle des licences.

[9] Une personne, organisation ou entité chargée de fournir un service aux parties intéressées. Le fournisseur peut être un grand fournisseur de Cloud public ou une PME (*petites et moyennes entreprises*), internationaux ou locaux. Un fournisseur de Cloud peut livrer SaaS, PaaS ou services IaaS. De grands centres du gouvernement peuvent, dans certaines circonstances, également agir comme fournisseurs de Cloud vers d'autres organisations publiques, par exemple où les données doivent être à un emplacement du gouvernement ou sont très sensibles.

9. RESPONSABILITÉ

Dans la responsabilité, selon Vincent Fauchoux et al, le client de l'informatique en nuage « *aura le plus grand intérêt à rappeler que le prestataire est responsable du traitement des données qui lui sont confiées. Le contrat peut également prévoir que le prestataire mette en place un système permettant de garantir la continuité du service via des procédures de sauvegarde et de réplication des données sur d'autres sites*[10] » [16].

D'après mon observation, lors de la négociation d'un contrat de service avec un fournisseur de l'informatique en nuage, il y a une foule de questions liées à la responsabilité qu'un utilisateur devrait envisager. Dans une relation de Cloud, la responsabilité et la recevabilité sont essentielles. Les consommateurs de Cloud, qu'il s'agisse d'une institution gouvernementale ou d'utilisateurs finaux, devraient disposer des moyens à leur disposition pour demander et obtenir réparation contre leur fournisseur en cas d'incidents. Cela est d'autant plus le cas pour le gouvernement public, souvent considéré comme contrôleur de données, qui sera responsable de la conformité avec la législation relative à la protection des données. Selon Neil Robinson et al, cela suppose toutefois que la responsabilité du fournisseur de l'informatique en nuage puisse être définie, ce qui est souvent un défi dans un environnement Cloud (multinational), dans lequel les fournisseurs de Cloud peuvent avoir une partie des services effectués par des filiales dans d'autres pays ou même par des sous-traitants situés dans ou en dehors de l'UE/EEE [17]. À mon avis, je pense que les fournisseurs de Cloud ne disposent généralement pas d'un système de gestion de données interne systématique de sorte qu'il sera plus difficile de retracer l'information. On peut dire la même chose du côté des consommateurs : dans la mesure où il y a plus d'une filiale ou dans le cas d'une mise en place de Cloud dans le secteur public, les administrations régionales participantes il se peut également qu'il ne soit pas évident pour le fournisseur de l'informatique en nuage de savoir où s'adresser pour traiter des demandes de données spécifiques.

10. CONCLUSION

Les avantages potentiels de la technologie Cloud computing ont également bien reconnus par un nombre croissant de gouvernements, partout dans le monde. Toutefois, en raison de la nature souvent complexe et globale des services, les défis juridiques existants peuvent être amplifiés. C'est particulièrement le cas avec la propriété intellectuelle ó les commentateurs ont longtemps suggéré que la politique de propriété intellectuelle ne parviendrait pas à suivre le rythme des évolutions technologiques [18].

L'informatique en nuage étant basé sur « l'utilisation de multiples serveurs situés en divers points de la planète, les difficultés quant à la détermination du droit applicable sont évidentes. […] La flexibilité et la fluidité des transferts de données rendent potentiellement applicables autant de lois que de pays dans lesquels se trouvent des serveurs traitant les données [11] » [19]. Effectivement, la flexibilité et la fluidité des transferts de données « rendent potentiellement applicables autant de lois que de pays dans lesquels se trouvent des serveurs traitant les données » [20]. C'est pourtant important « d'identifier la loi applicable, afin notamment de déterminer quelles obligations pèsent sur le responsable de traitement » [2]. Le point clé est d'examiner les implications juridiques de l'utilisation du nuage d'emblée lors de la planification du réseau dans le Cloud, visant à s'assurer que l'utilisateur a considéré les risques et leur gestion et leur atténuation à un niveau satisfaisant pour lui./.

REFERENCES

[1] Urs Gasser, David R. O'Brien, *Governments and Cloud Computing : Roles, Approaches, and Policy Considerations*, No. 2013/23, 2013, p. 3-6, [Consulté le 16 juin 2018], disponible sur l'adress : https://dash.harvard.edu/handle/1/16460373

[2] *Ibid ;* COM (2012) 529 final, *Exploiter le potentiel de l'informatique en nuage en Europe*, Bruxelles, le 27.9.2012, [Consulté le 11 juin 2018], disponible à

[10] D'usage, le prestataire garantit qu'il dispose de l'ensemble des droits et autorisations nécessaires à la prestation. Notamment, il garantit qu'il dispose de tous les droits relatifs à son service, et garantit le client contre tous les recours, réclamations, règlements, actions et procédures judiciaires qui pourraient être engagés. Le prestataire garantit également que les précautions prises pour assurer la sécurité de son progiciel et de l'infrastructure mise à la disposition du client sont conformes à l'état de l'art en la matière. Le client devra veiller à ce que la garantie de son prestataire ne se cantonne pas au contrat principal mais s'étende également aux sous-contrats que ce dernier est susceptible de conclure avec des sous-traitants. En effet, il devra être convenu que le prestataire demeure seul responsable de l'exécution du contrat par ses sous-traitants.

[11] Le principe en la matière a été posé par l'article 5 de la loi du 6 janvier 1978 modifiée, au terme duquel la loi française s'applique si le responsable du traitement a son établissement sur le territoire français et a recours à des moyens de traitement situés sur le territoire français.

l'adress : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:FR:PDF

[3] Rapport d'information déposé par la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique M. Christian Paul, co-président Mme Christiane Féral-Schuhl, co-présidente, disponible sur : http://www2.assemblee-nationale.fr/documents/notice/14/rapports/r3119/ [consulté le 8 juin 2018].

[4] CNIL, *Consultation relative au Cloud Computing Observations et commentaires de l'AFDIT et de l'ITECHLAW*, le 17 novembre 2011.

[5] L'article 3 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« Directive sur le commerce électronique »).

[6] La Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995.

[7] COM/2012/11 final, Proposition de règlement du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement relatif à la protection des données générales).

[8] Forecast : Public Cloud Services, Worldwide, 2011-2017, 4Q13 Update, (Gartner, 26 décembre 2013), disponible à l'adresse : https ://www.gartner.com/doc/2642020/forecast-public-cloud, [Consulté le 3 juin 2018].

[9] Groupe de travail article 29, « Avis 5/2012 sur le Cloud Computing » (WP 196, 1er juillet 2012).

[10] Vivant Michel *et al.*, *Lamy droit du numérique*, 2013, n° 1425, 1444 et s. ; n° 1835 et s.

[11] La directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (Framework Directive).

[12] Jasper P. Sluijs, Pierre Larouch et Wolf Sauter, *Cloud Computing in the EU Policy Sphere*, 2012, p. 23. Disponible à l'adresse : https://www.jipitec.eu/issues/jipitec-3-1-2012/3320/sluijs.pdf, [Consulté le 27 mai 2018].

[13] La directive 2002/19/CE du Parlement européen et du Conseil du 7 mars 2002 sur l'accès à, et l'interconnexion des réseaux de communications électroniques et aux installations associées (Directive « accès »).

[14] Jasper P. Sluijs, Pierre Larouch et Wolf Sauter, 2012, *op. cit.*, p. 23.

[15] Fauchoux Vincent, Deprez Pierre F., Bruguière Jean – Michel, *Le droit de l'Internet - Loi, contrats et usages*, 2013, p. 133-134, n° 164.

[16] Ibid., p. 137-138, n° 172.

[17] Neil Robinson, Lorenzo Valeri, Jonathan Cave, Tony Starkey, Hans Graux, Sadie Creese, Paul Hopkins, *The Cloud Understanding the Security, Privacy and Trust Challenges*, 2011, p. 59-60.

[18] Frayssinet Jean, *Droit, Droits et Nouvelles technologies*, Rapport présenté au 30e Congrès de l'Institut International de Droit d'Expression et d'Inspiration Françaises Le Caire, 2006, p. 3-5.

[19] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (version consolidée au 15 mai 2018). [Consulté le 02 juin 2018], Disponible à l'adresse : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20180515

[20] CNIL, *Consultation relative au Cloud Computing*, 2011, p. 4-5.

Những vấn đề pháp lý cơ bản trong môi trường điện toán đám mây

Nguyễn Như Hà
Khoa Luật, Đại học quốc gia Hà Nội
Tác giả liên hệ: e-mail: nhuha.nguyen@hotmail.fr

Ngày nhận bản thảo: 10-7-2018; Ngày chấp nhận đăng: 20-11-2018; Ngày đăng: 24-11-2018.

***Tóm tắt*—Những vấn đề pháp lý phát sinh trong quá trình sử dụng các giải pháp điện toán đám mây đa phần tương tự như bất kỳ hợp đồng outsourcing (hợp đồng thuê ngoài) nào với bên thứ ba. Tính linh hoạt của việc di chuyển dữ liệu giữa các máy chủ được đặt ở khắp mọi nơi trên thế giới dẫn tới việc khó xác định cơ chế pháp luật nào sẽ được áp dụng tại một thời điểm nhất định cho dữ liệu. Khi dữ liệu bị phân tán tùy thuộc vào sự khả dụng hoặc dung lượng của dịch vụ đám mây, việc xác định luật áp dụng lại càng trở nên phức tạp và khó khăn hơn. Bài viết trình bày những vấn đề pháp lý cơ bản trong môi trường điện toán đám mây, qua đó giúp cho việc xác định luật áp dụng để có thể bảo đảm cho việc bảo hộ được đầy đủ và hiệu quả nhất.**

***Từ khóa*—Điện toán đám mây; Pháp lý đám mây; Sở hữu trí tuệ; Quyền riêng tư; Thông tin cá nhân.**