**Le cloud computing : à qui sont les données ?**

*Conférence organisée par le Master 2 Droit du Commerce Électronique et de l’Économie Numérique*

5 juin 2013

Intervenants :

* **Guillaume Jahan**, Directeur juridique de Numergy
* **Jérémie Zimmerman**, Co-fondateur et porte-parole de la Quadrature du

net

* **Cédric Manara**, Professeur associé à l'EDHEC, chargé d’enseignement

dans le Master 2 «Droit du commerce électronique et de l'économie

numérique »

* **Romain Perray**, Avocat, Cabinet andCo Avocats, chargé d’enseignements dans le

Master 2 « Droit du commerce électronique et de l'économie numérique »

Introduction

Nous avons choisi le sujet du cloud computing compte tenu de l'importance du phénomène. En effet, si l'on en croit les derniers chiffres publiés par Markess International, il résulte que depuis 2009, le cloud à destination des entreprises connaît une forte croissance (une augmentation de près de 30% depuis 2009).

Parallèlement à cette croissance, le cloud reste un phénomène mal connu. A titre d'exemple, une étude réalisée aux USA a mis en évidence le fait que parmi les Américains répondant à cette enquête, près de la moitié n'avait aucune idée de ce qu'était le cloud. Certains croyaient même que c'était un phénomène météorologique et que les services de cloud computing pouvaient être influencés par une tempête...

Le cloud est également dans tous les esprits : cloud privé, public, hybride, services SAAS, IAAS, PAAS... autant de notions qui sont inconnues pour des novices comme nous et qui nous invitent à nous demander comment définir plus précisément le cloud computing, si cela s’avère possible. Peut-on parler de cloud ou faudrait-il parler des clouds ?

Une proposition de règlement sur la protection des données à caractère personnel est actuellement en discussion au niveau européen. Ces nouvelles dispositions pourraient avoir un impact sur le cloud computing, notamment au regard de la responsabilité des différents acteurs impliqués et des droits des personnes concernées sur les données stockées.

***Le cloud computing est au centre des discussions et l’expression connaît de multiples déclinaisons : Cloud public, Cloud privé, SaaS, Iaas. Le cloud est donc multiple et n’est pourtant toujours pas défini par le législateur. Quelle définition retenir en conséquence : peut-on adopter une définition unitaire ou doit-on aller vers des définitions multiples ?***

**Guillaume Jahan :** en France, le cloud est un phénomène qui n’a pas de définition juridique. Il est communément entendu comme l’informatique à distance fournie grâce aux connexions internet et permettant l’accès à une capacité de calcul et de stockage qui se trouve chez un prestataire et non dans la société.

Il existe différentes catégories de cloud:

* IAAS (Infrastructure as a Service) qui fournit l’infrastructure informatique virtualisée pour utiliser des serveurs qui vont permettre le traitement, le stockage… à distance avec un système d’exploitation au choix.
* PAAS (Platform as a Service) qui en plus de l’infrastructure fournit des outils de programmation pour offrir un environnement de développement et de test aux développeurs.
* SAAS (Software as a Service) qui met à disposition des utilisateurs des applications et usages, par exemple un service de messagerie électronique.

De nouvelles catégories de « aaS » (as a Service) apparaissent chaque jour selon les nouvelles fonctionnalités proposées dans le cloud.

Aux Etats-Unis, le National Institute of Standards and Technology a fixé une définition communément acceptée en fonction d’un certain nombre de critères :

* un service à la demande,
* des ressources mutualisées : le prestataire met à disposition un data center où les serveurs sont partagés avec d’autres clients mais les espaces créés pour chaque client informatiquement cloisonnés,
* un accès permanent à ce service.

L’Europe s’intéresse au cloud : elle souhaite développer ce type de service et réfléchit à des outils juridiques et pratiques pour rendre le cloud plus accessible aux européens. Pour structurer le marché, elle préfère les recommandations à la réglementation. Le marché du cloud est en train de se structurer.

**Jérémie Zimmerman :** il faudrait préférer l’acception « *clown computing*» tellement l’on en parle ces derniers temps. On pourrait appeler le cloud l’informatique en fumée ou fumeuse. Les entreprises utilisent la complexité de la technologie pour faire barrage entre vous et vos données.

Le cloud regroupe en réalité deux concepts anciens :

* la virtualisation : dissociation de la machine et du software ;
* l’externalisation: on ne maitrise pas son infrastructure, on choisit de faire confiance à quelqu’un d’autre.

Le cloud soulève en conséquence deux questions fondamentales :

* celle de la confiance envers la personne qui stocke vos données et y accède potentiellement. Exemple de risque : fuite de données des comptes de Playstation Network de Sony qui ont fuité avec les mots de passe.
* celle du contrôle : qui contrôle les données ? votre informatique ?

**Romain Perray :** il existe des définitions variées du cloud computing.

La difficulté est de savoir si l’on peut réellement appréhender ces pratiques par le biais d’un instrument juridique unique comme la loi. Cela paraît peu envisageable et même manquer d’intérêt tant les pratiques sont justement très différentes les unes des autres et évoluent beaucoup alors que la loi est figée et ne constitue de ce fait pas nécessairement une bonne solution.

En tout état de cause, le cloud pose un problème à la fois de transparence et, par conséquent, également d’information.

Sur ce point, s’il n’y a certes pas de législation spécifique au cloud, il existe tout de même des dispositions qui s’appliquent indirectement, dont celle sur la protection des données à caractère personnel. La loi Informatique et libertés établit en effet des règles spéciales pour garantir l’information de la personne concernée. Ces règles sont certes prévues mais la vraie question est de savoir si elles sont appliquées, particulièrement par les sous-traitants dans le cas du cloud. Il existe donc déjà des dispositions qui peuvent s’appliquer indépendamment de la façon dont le cloud est organisé.

**Cédric Manara**: il y a certes « l’approche technique » du cloud computing, mais il ne faut pas oublier « l’approche usage » : le cloud permet à chacun de sauvegarder ses données et de pouvoir les récupérer. Il facilite et accompagne les usagers contemporains. Le cloud permet aussi le partage. Il permet aussi à des petites entreprises qui ont peu de moyens et qui veulent créer un nouveau modèle économique de rendre leur nouveau service disponible à une échelle mondiale via le cloud et de voir leur projet aboutir plus rapidement.

Le cloud accompagne nos usages et nous rend plus libres.

La notion de cloud est avant tout un concept marketing qui regroupe sous un même nom des pratiques très différentes. Se pose alors la question de la qualification juridique de ce phénomène. Mais faut-il vraiment le qualifier ? Internet, ou encore le site web sont aussi des notions qui ne sont pas qualifiées juridiquement et cela ne pose pas problème. En revanche il peut être utile de qualifier les différents services de cloud.

Les enjeux sont de deux ordres :

* Le cloud est une adjonction d’une couche technique et juridique entre l’utilisateur et ses données. Selon qui administre cette couche, des difficultés peuvent survenir. La différence entre le stockage chez soi et le stockage dans le cloud, c’est que dans ce dernier cas on introduit un tiers.
* La centralisation : internet est un réseau acentrique, mais avec le cloud, les ressources peuvent être concentrées chez un minimum d’acteurs français ou étrangers. On assiste à la déconstruction d’internet et au regroupement des données dans un nombre d’endroits très limités et chez des acteurs très limités. Les données de Wikileaks par exemple étaient situées sur le cloud d’Amazon. Le gouvernement américain a fait pression pour demander à Amazon de mettre fin au service.

***Pourquoi les entreprises se tournent-elles vers le cloud aujourd’hui, quels sont ses avantages ?***

**Guillaume Jahan**: le cloud demande de faire confiance à un prestataire. Avant, le stockage se faisait en interne ce qui impliquait des coûts de maintenance et d’expertise. L’avantage pour les PME qui ont peu de ressources matérielles et humaines, c’est qu’elles peuvent accéder à tous ces services à distance, comme si c’était de l’électricité. L’informatique devient du consommable, on paie ce que l’on consomme. On passe progressivement de dépenses d’investissements matériels à des dépenses de services consommés. Les entreprises n’ont plus à gérer les contraintes matérielles et logicielles (mises à jour, confidentialité, sécurité sont gérées par le prestataire). Les entreprises de cloud ont la capacité à grande échelle de développer ces services à moindre coût.

L’externalisation n’est pas forcément adaptée pour tous les services de l’entreprise. Cela suppose de se poser la question du type de données qui peuvent être confiées.

**Jérémie Zimmerman**: les entreprises utilisent le cloud souvent par incompétence.

ITunes, par exemple, fait des mises à jour automatiques : c’est lui qui nous contrôle. Apple ne nous demande pas notre avis et il n’y a pas moyen de refuser ces mises à jours.

Dans les Spyfiles de Wikileaks figuraient des vidéos montrant comment la société FinFisher diffuse des logiciels espions qui prennent le contrôle de l’ordinateur et qui s’installent grâce au bug dans le système de mise à jour automatique d’Apple.

Avec le cloud, on renonce au contrôle de son infrastructure par manque de connaissance des technologies.

La loi FISA aux Etats-Unis a été amendée il y 1 an et aujourd’hui il y a un vide juridique : l’amendement dit que quand les données de citoyens non-américains sont stockées sur un cloud américain, les juges américains peuvent accéder aux données sans aucune autorisation.

La question est de savoir comment utiliser intelligemment le cloud ou quelle alternative existe t-il ?

* Alternative juridique : aller vers un prestataire français afin que la juridiction française soit compétente ; c’est plus simple et la protection des données personnelles sera mieux assurée.
* Alternative technique : avoir la maitrise de son système d’information, ou stocker les données, mais chiffrées (attention, un chiffrement point que l’on maîtrise, et non pas un chiffrement vendu par un prestataire extérieur.)

**Romain Perray :** l’avantage est clair : l’argent. Avoir recours au cloud permet aux entreprises de faire des économies. Il ne faut pas considérer le cloud seulement au travers de l’exemple de Google : selon les pratiques, le curseur de la protection et des problématiques évolue notamment en terme de protection des données.

Avec l’externalisation, on a un prestataire qui centralise les données, mais cela n’a rien de très nouveau. Le souci vient du fait que ce qui était une concentration devient décentralisée. Cette décentralisation pose la question de la propriété sur les données et de l’impression d’en avoir le contrôle. La loi Informatique et Libertés permet d’envisager un certain nombre de droits et les prestataires de cloud en tiennent parfois compte. Cependant, la décentralisation et l’atomisation des données sont en même temps une garantie de la sécurité de la donnée. Si la donnée est atomisée, les risques sont moindres dans la mesure où il faudrait un logiciel pour tout recentraliser et unifier.

Le cloud offre un avantage financier incontestable mais des inconvénients en terme de protection et sur le fait de savoir, au delà des droits que l’on peut exercer sur ses données, comment leur sécurité est garantie.

***Question du public :***

Le cloud souverain (dont les données sont hébergées en France) peut-il être une alternative ?

**Guillaume Jahan**: Numergy est un prestataire de services « BtoB » dont tous les serveurs sont localisés en France. Elle met en avant la notion de proximité, par opposition à Amazon dont les serveurs sont surtout aux Etats-Unis et dont les données circulent d’un endroit à l’autre, d’un pays à l’autre selon l’espace disponible dans un Datacenter. Le cloud souverain peut être une réponse, notamment en terme de données à caractère personnel puisque les transferts de données hors de l’Union Européenne sont soumis à des contraintes.

En terme d’intelligence économique, le cloud souverain est d’autant plus une réponse que les principaux prestataires de cloud sont américains et que les 2/3 de leurs serveurs sont aux Etats-Unis régis par le Patriot Act (qui donne accès au gouvernement américain aux données situées sur les serveurs d’Amazon). C’est un échelon supplémentaire en terme de confiance.

**Jérémie Zimmerman**: le chiffrement le plus sécurisé est le chiffrement RSA. C’est celui le plus répandu et il peut être utilisé en logiciel libre. L’algorithme le plus utilisé est donc public et peut être implémenté en logiciel libre. C’est une forme d’intelligence collective qui offre un niveau de protection suffisant.

On parle d’intelligence économique : certaines unités de l’armée chinoise qui cassent des systèmes d’information partout dans le monde pour en extraire des données.

L’Agence Nationale de la Sécurité des Systèmes d’Information a sorti un guide sur l’hygiène informatique dans laquelle manque la notion de logiciel libre et de souveraineté informationnelle sur ses propres systèmes et ses processus.

**Romain Perray**: le cloud souverain pose problème en terme de données à caractère personnel. La loi Informatique & Libertés a été adoptée en 1978 car l’Etat avait envisagé l’interconnexion d’un ensemble de fichiers à partir du numéro unique d’identification nationale : le numéro de sécurité sociale. Le risque lié au choix d’un cloud souverain qui stockerait les données des concitoyens est de basculer dans un régime autoritaire et fort. Le cloud souverain peut être un mécanisme incitatif mais s’il devenait un mécanisme d’Etat, cela poserait évidemment des problèmes en terme de démocratie.

**Guillaume Jahan**: l’Etat fournit 20% de ses fonds à Numergy par le biais de la Caisse des Dépôts et Consignation mais la société n’appartient pas à l’Etat. L’Etat français a fait le choix d’investir pas de contrôler ou diriger.

***Quels sont les droits de l’utilisateur sur ses données ?***

**Romain Perray :** du point de vue des données à caractère personnel, la loi Informatique et Libertés accorde un certain nombre de droits à la personne concernée :

* le droit d’opposition : il présente *a priori* peu d’intérêt en matière de cloud, sauf dans le cas où les données personnelles de salariés relevant exclusivement de leur vie privée seraient stockées dans un système de cloud mis à disposition par l’entreprise ;
* le droit d’accès ;
* le droit de modification ;
* le droit de suppression : mais malgré l’effacement, certains fournisseurs conservent parfois les informations ;
* le droit à l’information : en matière de cloud, les dispositifs impliquent souvent des transferts hors de l’Union Européenne, et sont donc soumis à des dispositions très détaillées. La réglementation française prévoit notamment des mentions supplémentaires à faire figurer sur la localisation des données transférées.

Il faut également noter au-delà de ces droits, la place importante que joue le consentement dans la protection des données personnelles. Pour autant, prévoir un e consentement explicite en toute circonstance n’est pas non plus la solution à tout et ne correspond pas, en tout état de cause, à la réalité économique, notamment en cas de clauses standardisées. Car, le consentement sur le traitement de données personnelles est souvent lié au consentement à conclure un contrat. Le consentement explicite n’est pas, à mon sens, le rempart ultime ni la seule solution pour assurer la protection des données à caractère personnel.

**Jérémie Zimmerman :** quels devraient être les droits des utilisateurs pour avoir une vague chance de reprendre le contrôle sur leurs données personnelles ?

Pour reprendre le contrôle sur nos données, il faut comprendre la technologie et repenser le rapport que nous avons chacun à la technologie. Sinon, on signe un contrat qu’on ne lit pas.

Ce que devraient être les droits de l’utilisateur (et qui est en train de se faire réduire par les géants de la Silicon Valley, banque, assurance, et gouvernement américain) :

* la notion de consentement explicite de l’utilisateur pour les traitements de données ;
* l’obligation de notification des fuites de données : aujourd’hui le prestataire se tait. S’il en avait l’obligation, il serait plus vigilent ;
* la question du profilage : doit-on accepter que l’on puisse autoriser ou interdire des décisions qui peuvent avoir un impact décisif sur la vie de quelqu’un ? Certaines banques refusent un crédit car les données sur Facebook ont montré que la personne était dépensière.

Attention à la notion de pseudonymisation : c’est une notion fumeuse car on peut très bien attribuer le pseudonyme à quelqu’un. Cela rendrait le règlement vide de sens. Il en va de même pour la notion d’intérêt légitime qui fait perdre de sa force au règlement.

Il faudrait connaître la valeur exacte de nos données. Aujourd’hui on fait des échanges économiques sans en connaître la valeur. On échange de l’or contre des patates. Si on connaissait la valeur exacte, on pourrait faire des choix éclairés : cela soulève la question de la souveraineté informationnelle.

**Cédric Manara :** les contrats sans garantie sur la sécurité existe depuis longtemps (chemin de fer, obligation de sécurité du transporteur…).

Il n’est pas certain que la solution se trouve au niveau de l’information de l’utilisateur. Elle se situe sans doute plutôt dans les contrats qu’il faudrait revoir (notamment les clauses abusives) plutôt que croire à la capacité de chacun à comprendre tout ce qu’il se passe. Il n’est pas si facile que ça pour tout un chacun de reprendre le contrôle technique.

Sur 12 millions d’utilisateurs de Facebook, un seul a attaqué la société et est parvenu à retoquer des clauses du contrat (*Cour d’appel de Pau, 1ère Chambre, 23 mars 2012*).

Il existe également des droits sur les fichiers qui ne sont pas des données personnelles : dans le cadre d’un conflit B2B,  le prestataire (Wizzgo) a par exemple été attaqué sur le fondement de la contrefaçon (*Cour d’appel de Paris, Pôle 5, Chambre 1, 14 décembre 2011*).

**Guillaume Jahan :** pour qu’une société comme Numergy soit compétitive, il faut qu’elle soit irréprochable en matière sécuritaire et pas seulement des prix attractifs ou la localisation des données en France, notamment face à Amazon qui a plus d’une dizaine d’année d’expérience dans le domaine et Google avec les moyens d’une multinationale.

***Compte tenu des inconvénients liés aux services de cloud computing et aux problématiques liées à la protection des données à caractère personnel, il ne faudrait pas revoir le partage des responsabilités entres les parties au contrat (d'autant plus lorsqu'il s'agit d'établir les responsabilités en cas de perte, vol et piratage des données) et agir directement au niveau contractuel ? A ce titre pouvez-vous nous parler davantage des parties qui sont amenées à collaborer dans un contrat de cloud?***

**Guillaume Jahan :** il y a deux dimensions :

* Dans le BtoB, les contrats ne sont pas du « sur-mesure » pour chacun des clients car cela serait compliqué et contre-productif. C’est en bâtissant une offre standardisée qu’il est possible à un prestataire informatique de proposer des prix compétitifs et l’élasticité des ressources. Numergy opte donc elle aussi pour un contrat standard mais qui se veut équilibré avec des adaptations possibles à la marge pour répondre à des demandes très particulières. Tout dépend de la relation que l’on a avec son prestataire : si le client est important, le prestataire n’a aucun pouvoir de négociation, et inversement. Numergy est dans une situation un peu différente de la plupart des prestataires cloud car ses offres sont distribuées pour et aux entreprises (BtoB) par des partenaires distributeurs, avec le bénéfice de leur valeur ajoutée (expertise métier, intégrateur, etc.). Un prestataire cloud qui n’est pas dans ce schéma acceptera de négocier un contrat différent selon la mesure du marché passé avec le client (coût global, durée…) ;
* Vis-à-vis des utilisateurs particuliers, donc pour le BtoC : le problème est plus flagrant car la souscription se passe en ligne et les conditions générales d’utilisation sont illisibles. Le problème majeur qui se pose alors, face à des services sur internet de dimension internationale, est celui de la loi applicable. Il s’agit de celle précisée dans le contrat.

La responsabilité peut se diluer car il y a souvent plusieurs sous-traitants. Le client a un seul interlocuteur mais, derrière, il y a plusieurs acteurs. Il faut être vigilent sur ce que l’on achète et sur ce que l’on signe.

Le projet de règlement européen envisage des obligations pour le sous-traitant et le sous-sous-traitant. Aujourd’hui la loi Informatique et Libertés envisage seulement le responsable de traitement et le sous-traitant. La transparence n’est pas toujours de mise pour l’ensemble des intervenants de la chaine. Numergy n’a pas de sous-traitant.

**Cédric Manara**: quel contrat de cloud ? Pour un contrat de base, la réponse est moins dans les clauses du contrat que dans le prestataire que l’on choisit. Par exemple, je vais chez Numergy car je sais que les données sont en France, peu importe les clauses du contrat qui nous lie.

Quels sont les moyens mis à disposition des personnes lésées par le contrat ? Quel est le pouvoir des internautes ? Faut-il rééquilibrer les pouvoirs ? Quels seront les moyens donnés aux autorités pour mettre en œuvre les nouveaux droits du projet de règlement ? Aujourd’hui les autorités compétentes ont peu de moyens.

**Romain Perray :** les responsables de traitement n’ont pas toujours conscience qu’ils le sont. La relation de sous-traitance pose des difficultés : la loi Informatique & Libertés, à la différence de la directive européenne, prévoit une obligation d’organiser les relations avec les sous-traitants en terme de sécurité et de confidentialité. Mais la loi ne se prononce pas sur les sous-traitants ultérieurs. Le projet de règlement européen prévoit, quant à lui, ou envisage de prévoir, que cette responsabilité ne soit pas autant diluée.

Le problème vient du fait que les sous-traitants peuvent exploiter au maximum la rédaction de la loi, dans la mesure où, selon le texte, ils ne doivent intervenir que sur demande du responsable de traitement. Donc s’ils n’ont pas reçu d’instruction, les sous-traitants peuvent échapper à leurs obligations.

Cette situation est d’autant plus difficile dans le cas où les utilisateurs de cloud sont des individus. Certes la personne concernée est placée au centre de la proposition de règlement européen : mais même si le consentement peut être un bon moyen, il n’est pas suffisant. La réglementation doit aussi protéger et ajouter d’autres principes qui viennent réguler cet aspect là, car même si le consentement est important, il ne permet pas à tout le monde de prendre librement des décisions qui le concernent lors de l’utilisation d’un service de cloud.

**Jérémie Zimmerman :** il n’est pas impossible que les gens comprennent les nouvelles technologies. C’est un choix politique. Ce qui est important, c’est la compréhension des technologies, qui sont faites pour être auto-apprises. C’est indispensable pour avoir conscience des choix que l’on fait, en toute liberté de conscience. Ce sont des choix politiques que l’Europe doit faire plutôt que renoncer.

Le rôle des pouvoirs publics sur les données personnelles est crucial. S’agissant de la proposition de règlement européen, pour le moment les Etats Membres seraient sur le point de tout céder à la Silicon Valley. Il faut attendre de voir alors quel va être le rôle des pouvoirs publics et si la France va céder ou non.

**Judith Rochfeld :** tous les droits s’appliquent pour le moment pour ceux qui ont les moyens de les faire valoir. Pour le consommateur lambda, le plus pénalisant, c’est le taux de litigiosité : il existe un seuil psychologique et financier en dessous duquel le consommateur ne poursuivra pas son action en justice.

***Question du public :***

Le prestataire garantit-il la sécurité des données ?

**Guillaume Jahan**: oui, le prestataire garantit un service (accessible par Internet) avec la sécurité et la confidentialité des données. En plus d’une liaison https et du chiffrement, un des moyens notamment est d’avoir obtenu la certification par un organisme indépendant qui vérifie l’application de standards dans le domaine (par exemple normes ISO). Cette procédure de certification, en plus du contrat, permet d’avoir l’attestation d’un tiers que la sécurité est effective. Le prestataire a intérêt à être certifié par les principaux organismes.

**Jérémie Zimmerman**: la sécurité ne se garantit pas. Il est impossible de vérifier au jour le jour que la sécurité sur nos données est bien garantie. La sécurité n’est pas un état mais un processus. Normalement pour vérifier la sécurité, il faudrait faire une analyse de risque.