LEXBASE
l'information juridique

Revues

Lexbase Hebdo édition affaires n°292 du 12 avril 2012

[Internet] Evénement

Promesses du *Cloud Computing* et protection des données à caractère personnel : la remise en question du cadre juridique français et européen

N° Lexbase: N1331BTH

ADIJ

par *Béatrice Delmas-Linel, Avocate associée, de Gaulle Fleurance & Associés, en collaboration avec Bruno Sabaila et Florent Lizzit, Membre de la "Section jeunes" de l'ADIJ*

Le 14 février 2012, l'Association pour le Développement de l'Informatique Juridique (ADIJ) a souhaité réunir sur un même panel les animateurs de deux de ses ateliers, l'un sur les données personnelles, l'autre sur le "*Cloud Computing*" ("informatique dans les nuages"), afin d'évoquer la problématique précise de la protection des données personnelles dans les solutions de *Cloud Computing*, à l'heure où le cadre réglementaire de cette protection est amené à évoluer en Europe, ainsi qu'en atteste le projet de Règlement européen 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, publié par la Commission européenne le 25 janvier 2012. Etaient donc présents autour de la table Nathalie Métallinos, avocate du cabinet Bird & Bird et co-responsable de l'atelier ADIJ sur la Protection des Données Personnelles, les trois co-animateurs de l'atelier *Cloud Computing*, Béatrice Delmas-Linel, avocate associée de la société de Gaulle Fleurance & Associés, Helle Jul-Hansen, Directrice juridique EMEA de la société VMware et David Feldman, consultant en gestion et redressement de projets informatiques chez David Feldman Consulting, ainsi que leur invité, Jean Gonié, *Director of Privacy* au sein de la société Microsoft EMEA, venu de Bruxelles, pour son éclairage sur la dimension européenne du sujet. Nous vous proposons donc un compte-rendu des différentes interventions et discussions qui ont eu lieu au cours de cet événement.

Tout d'abord, les intervenants ont présenté une synthèse des travaux de l'atelier ADIJ sur le *Cloud Computing*, qui se sont déroulés entre septembre 2010 et novembre 2011. Cette synthèse a permis de partager le constat que le *Cloud Computing*, qui est techniquement un assemblage de technologies préexistantes, ne pose pas de problématiques juridiques entièrement nouvelles, mais vient mettre en lumière de manière différente de nombreuses problématiques juridiques classiques en matière de contrats informatiques et d'infogérance pour lesquelles des réponses juridiques, plus ou moins adaptées, existent.

L'atelier de l'ADIJ, qui a bénéficié de la participation de représentants d'entreprises variées, prestataires ou utilisatrices de solutions de *Cloud Computing*, ainsi que de la CNIL, a été l'occasion de faire l'inventaire de ces problématiques juridiques les plus spécifiques, au titre desquelles on retrouve : la sécurité et la nécessité d'assurer la confidentialité et la disponibilité des données sur des serveurs mutualisés ; la perte de maîtrise technique directe sur

les serveurs et systèmes d'information, à compenser par l'encadrement contractuel des obligations du prestataire et de son client ; une réversibilité et une interopérabilité à assurer afin de pouvoir sortir du nuage (*Cloud*) ou changer de prestataire ; la place des normes techniques et juridiques -en particulier un effort de normalisation qui doit être mis en œuvre par les prestataires— ; la question des assurances et du besoin de polices d'indemnisation adaptées et efficaces en cas de pertes de données ; la nécessité de clarifier les responsabilités respectives du client et du prestataire, en particulier en cas de maîtrise des moyens de traitement des données par le prestataire.

En conclusion de ces travaux, il est apparu rapidement que la question de la protection des données à caractère personnel tenait une place centrale dans toute discussion concernant le *Cloud Computing*, au point d'en devenir aussi bien un enjeu qu'un frein ralentissant l'émergence des solutions de *Cloud Computing* en Europe. Il est donc particulièrement pertinent de se focaliser sur cet aspect.

Avant d'aborder de manière plus approfondie cette discussion il est apparu utile de décrire, ou de rappeler, ce que recouvre ce concept de *Cloud Computing*.

I — Le "*Cloud Computing*" en quête de repères : une réalité multiple et un cadre juridique applicable méconnu

Il existe aujourd'hui de nombreuses définitions du *Cloud Computing*, comme par exemple celle du NIST (*National Institute of Standards and Technology*) aux Etats-Unis et, en France, celle de la commission de terminologie et de l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

La commission de terminologie a défini l'informatique en nuage comme le "*mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire*". Elle constitue "*une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients*" (JORF du 6 juin 2010).

Les observateurs et spécialistes s'entendent généralement sur le fait que plusieurs critères alternatifs caractérisent une solution ou une prestation de *Cloud Computing*, dont deux, au moins, doivent être réunis. Cette solution doit, en effet, offrir :

— une flexibilité immédiate en fonction des besoins de l'utilisateur (pour couvrir pics et baisses d'activité) ;

— une virtualisation des systèmes, permettant de faire fonctionner plusieurs systèmes d'exploitation ou programmes sur un même serveur ;

- une mutualisation des ressources au sein d'un *datacenter* (ferme de données), permettant de partager les ressources d'un même serveur entre plusieurs serveurs virtuels et plusieurs clients ;

- un usage à la demande ;

- une accessibilité par le biais d'un réseau depuis n'importe quel point géographique ;

un paiement à l'usage (*pay per use*).

Quatre modèles de déploiement existent :

— le *Cloud* public, dans lequel l'infrastructure hébergée par le prestataire est virtualisée et dont les ressources sont mutualisées et partagées entre plusieurs clients ;

— le *Cloud* privé, dans lequel l'infrastructure hébergée par le prestataire est exploitée par un unique client, sans mutualisation ;

— le *Cloud* hybride, permettant par exemple à un client disposant d'un *Cloud* privé de recourir à des ressources d'un *Cloud* public en cas d'utilisation de l'ensemble de ses ressources réservées ;

— et le *Cloud* communautaire, dans lequel l'infrastructure est mutualisée et partagée entre plusieurs organisations ou entités ayant choisi cette formule entre elles compte tenu de leurs intérêts communs, ce qui leur permet de bénéficier des avantages d'un *cloud* privé avec celui d'un certain degré de mutualisation. Des applications pratiques concernent, par exemple, les entreprises du secteur public ou de secteurs hautement réglementés comme le secteur bancaire ou celui de la santé.

Enfin, plusieurs modes d'utilisation et types de services de *Cloud Computing* cohabitent :

— "*Software as a Service*" ou "SaaS", consistant en la mise à disposition d'une application, comme par exemple la sauvegarde à distance ou les boites de messagerie de courriels ;

— "*Platform as a Service*" ou "PaaS", consistant en la mise à disposition de l'utilisateur d'un environnement de développement, permettant par exemple à une DSI de développer ses applications ;

— "*Infrastructure as a Service*" ou "IaaS", consistant en la mise à disposition de l'utilisateur d'une infrastructure à distance avec des capacités de traitement à géométrie variable, permettant à une DSI de ne pas avoir à anticiper ses besoins plusieurs mois à l'avance, étant donné les délais de livraison d'un serveur, ou de compenser des pics de consommation de ressources.

Le *Cloud Computing* est donc protéiforme et ses avantages, en particulier pour les entreprises, sont nombreux : une diminution des investissements, la possibilité de bénéficier facilement des dernières technologies, une facilité d'utilisation et une flexibilité permettant de répondre à toute évolution des besoins.

Cependant, le *Cloud Computing* a aussi des inconvénients : une perte de maîtrise directe par le client de son infrastructure et de ses données, une dépendance à l'égard du prestataire -comme pour tout contrat d'externalisation, une négociation difficile du contrat en cas de déséquilibre entre les parties-. Ce déséquilibre est aujourd'hui courant en raison de la domination du marché par de grands acteurs pour l'essentiel d'origine américaine.

Le *Cloud Computing* n'est pas un effet de mode, mais une tendance forte et incontournable qui permet une meilleure prise de conscience de sujets préexistants, liés en réalité à toute externalisation de systèmes d'information, tant par les professionnels que par les particuliers. En effet, comme pour toute externalisation de l'hébergement et de la conservation de données, il est important de mener en amont une étude de risque afin de définir le niveau de sécurité adapté pour chaque type de données, voire de déterminer si une donnée peut ou non être placée dans le nuage, tout en gardant à l'esprit le fait que la sécurité des données en interne n'est pas forcément meilleure et plus fiable que celle offerte par un prestataire de *Cloud Computing*.

S'il existe avec le *Cloud Computing* une perte du contrôle physique de son infrastructure et de ses données, celle-ci peut et doit être compensée par un contrôle contractuel, le contrat devenant le pivot de toute relation d'externalisation en permettant de définir les garanties et responsabilités de chacun. Dans le *Cloud Computing*, on constate une implication des juristes beaucoup plus en amont des projets, qu'il s'agisse de bâtir les offres standards des prestataires ou d'évaluer des réponses aux appels d'offres lancés par les sociétés intéressées par ces solutions mais soucieuses des risques, informatiques comme juridiques, encourus. En effet, le *Cloud Computing* recouvrant des types de services et des relations contractuelles extrêmement variés, il n'existe pas de modèle de contrat pour les différents types de services de *Cloud Computing* (SaaS, PaaS, IaaS), ce qui amène à se poser de nombreuses questions lors de l'élaboration d'un contrat, alors même que les prestataires tentent d'imposer leur contrat en en négociant le moins possible les termes et en les groupant au sein d'un contrat global incluant la licence, la prestation de services, l'hébergement et une chaîne contractuelle entre plusieurs prestataires.

Afin de combattre le caractère anxiogène du *Cloud Computing* et une peur parfois irrationnelle des clients, les contrats incluent quasi-systématiquement des garanties de niveaux de services minima (SLA) offertes par les prestataires, souvent très détaillées. Cela n'est pas nouveau dans les contrats d'externalisation. Ce qui change, c'est la perception accrue des risques du fait de l'amplification des possibilités d'externalisation promises par le *Cloud*, ouvertes à tous, particuliers, grandes et petites entreprises, collectivités locales. Tous les acteurs du marché estiment qu'il serait utile, pour simplifier les contrats, de pouvoir s'appuyer sur des normes professionnelles ainsi que des procédures de certification, notamment en matière de sécurité, qui permettraient de rationaliser les niveaux de garantie tout en rassurant les clients. Mais l'élaboration de telles normes prend du temps.

En conclusion sur le cadre juridique du *Cloud*, il n'existe pas de problématiques juridiques nouvelles qui n'aient déjà été envisagées dans le cadre des contrats informatiques classiques ou de la réglementation applicable. En revanche, il est clair que la problématique spécifique de la protection des données à caractère personnel dans le *Cloud Computing* et des responsabilités respectives du client et du prestataire à cet égard, très prégnante en Europe, constitue un frein au développement du *Cloud Computing* sur le "vieux continent", alors que les principaux prestataires sont aujourd'hui américains.

II — Les difficultés d'application de la règlementation "Informatiques et Libertés" et le positionnement des autorités de protection des données personnelles

Certains évoquent souvent les risques d'espionnage ou d'application de lois de police nationales pour lutter contre le terrorisme, tel le *US Patriot Act*, comme l'une des problématiques du *Cloud Computing*. Ces aspects ne font en réalité pas partie des problématiques liées à la réglementation des données personnelles, mais relèvent plutôt

des conventions internationales qui régissent les conditions de l'accès par les autorités de police et de défense du territoire d'une nation concernée aux données localisées sur ce territoire. Ils ne sont donc pas traités ici.

En ce qui concerne la réglementation sur la protection des données personnelles en matière de *Cloud Computing*, les autorités ne se sont pas concentrées sur les relations "B2C" (*business to consumer*), mais plutôt sur les relations "B2B" (*business to business*). En effet, le traitement des données des consommateurs relève toujours de la responsabilité du professionnel qui met en œuvre le traitement, en application de la loi n° 78-17 du 6 janvier 1978, dite "Informatique et Libertés" (N° Lexbase : L8794AGS). Dans le cadre d'une relation de *Cloud Computing* B2B, les règles actuelles, qui conduisent à faire peser sur le client toute la responsabilité du traitement des données personnelles, font l'objet de débats car elles peuvent apparaître inadaptées.

La loi "Informatique et Libertés" crée une dichotomie entre le responsable de traitement et le sous-traitant. Le responsable de traitement est, en principe, la personne qui définit les modalités et les finalités du traitement de données personnelles. Le sous-traitant est censé n'avoir aucun rôle dans la définition des finalités et moyens techniques. Or, en matière de *Cloud Computing*, le prestataire est en réalité celui qui a la maîtrise de l'organisation du traitement des données et de son emplacement, selon ses paramètres de sécurité, et de la répartition de la charge de ses serveurs, même s'il maintient un certain niveau de transparence à l'égard de son client. Le prestataire peut donc être amené à prendre des décisions en principe réservées au responsable de traitement, et cela sans lui en demander l'autorisation. La CNIL a ainsi posé la question dans sa consultation du mois d'octobre 2011 (CNIL, article du 17 octobre 2011) de savoir s'il ne fallait pas dans certaines situations reconnaître une responsabilité propre au sous-traitant, distincte et complémentaire de la responsabilité du responsable de traitement au sens de la loi "Informatique et Libertés". Par ailleurs, en matière de transfert de données personnelles dans le cadre d'une externalisation du système d'information, la réglementation actuelle a été conçue pour une externalisation entre le responsable du traitement, et un seul sous-traitant, peut-être deux. La réglementation a certes anticipé de nombreux scénarii, mais pas celui du *Cloud*, où de multiples acteurs peuvent être amenés à intervenir dans une chaîne de contrats plus ou moins clairement définie.

Par ailleurs, en application de la loi "Informatique et Libertés", le responsable de traitement a le devoir de prouver qu'il a effectivement pris toutes les précautions utiles au regard de la nature des données et des risques qui y sont liés. En effet, le responsable de traitement de données à caractère personnel doit préserver la sécurité de celles-ci et notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès (loi n° 78-17, art. 34). Ces dispositions ont été complétées par l'ordonnance du 24 août 2011 (ordonnance n° 2011-1012 du 24 août 2011 N° Lexbase : L0014IRX) applicable "*au traitement des données à caractère personnel mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, y compris ceux prenant en charge les dispositifs de collecte de données et d'identification*". Cette ordonnance transpose les Directives 2009/136 (N° Lexbase : L1208IGT) et 2009/140 (N° Lexbase : L1209IGU), relatives au secteur des communications électroniques, visant à renforcer la protection de la vie privée et des données personnelles.

Aux termes du nouvel article 34 bis de la loi "Informatique et Libertés", "*on entend par violation de données à caractère personnel toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques*". En cas de violation, le fournisseur de services de communications électroniques accessibles au public doit avertir sans délai la Commission nationale de l'informatique et des libertés (CNIL). En outre, lorsque la violation porte atteinte aux données à caractère personnel ou à la vie privée d'un abonné ou d'une autre personne physique, le fournisseur doit également avertir, sans délai, l'intéressé. Cette notification n'est cependant pas nécessaire si la CNIL a constaté (i) que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée et (ii) que ces mesures ont été appliquées aux données concernées par cette violation (ce qui recouvre par exemple des mesures de cryptage).

Les fournisseurs de services concernés sont ceux fournissant des "*prestations consistant entièrement ou principalement en la fourniture de communications électroniques. Ne sont pas visés les services consistant à éditer ou à distribuer des services de communication au public par voie électronique*". Cette définition ne permet pas d'identifier avec certitude les fournisseurs visés, mais il est prévu en tout état de cause que les obligations de l'article 34 bis en cas de faille de sécurité soient généralisées à tous les responsables de traitement de données à caractère personnel.

Les besoins de sécurité doivent donc être anticipés, et les mesures de sécurité mises en place doivent être documentées. Or, la mise en place de cette documentation fait encore défaut ou est mal/pas assez appréhendée aujourd'hui dans les entreprises. L'absence de documentation sera problématique en cas de besoin de notifica-

tion d'une faille de sécurité d'un système d'information. Ce qui s'avère simple lorsque le système d'information est localisé dans l'entreprise peut devenir très compliqué lorsque les données ont été exportées chez un prestataire de *Cloud Computing*. L'entreprise sera tenue de faire localiser et de corriger les failles de sécurité auprès de ses prestataires et d'identifier sans attendre les personnes devant recevoir une notification.

Les obligations du responsable de traitement se trouvent donc renforcées dans les scénarii de *Cloud*, alors même que l'on constate souvent soit une méconnaissance des problématiques liées à la protection des données personnelles au sein des entreprises, soit une difficulté quant à l'identification des situations dans lesquelles la loi "Informatique et Libertés" est susceptible de s'appliquer. Certaines entreprises souhaitent absolument transférer leurs données vers un système de *Cloud* sans en considérer les conséquences en matière de sécurité et confidentialité, et ne se posent la question de la conformité à la loi "Informatique et Libertés" qu'après coup. Très souvent, les entreprises n'ont pas un niveau suffisant d'expertise en sécurité informatique pour se poser les bonnes questions au bon moment, et ne sont pas en mesure de choisir parmi les offres de *Cloud Computing* en toute connaissance de cause. Il est donc indispensable de sensibiliser les entreprises au fait que cette problématique doit être identifiée, analysée et traitée dès l'élaboration d'un projet d'exportation des données vers un serveur de *Cloud*.

Enfin, il faut souligner l'inadaptation des règles de protection des données personnelles en matière de transferts internationaux de ces données. La réglementation française et européenne pose sur ce point précis le principe de l'interdiction de tout transfert de données personnelles en dehors de l'Union européenne et de l'Espace économique européen d'une liste limitée de pays qui ont été reconnus par la Commission européenne comme offrant un régime de protection adéquat.

Pour autant, les transferts vers des pays tiers peuvent être licites s'ils sont encadrés et que les données personnelles font ainsi l'objet d'une protection adéquate. Les outils ou procédures permettant d'encadrer ce type de transferts, développés au niveau européen ou national, sont les "Clauses Contractuelles Types" qui, approuvées par la Commission européenne, doivent être signées entre les deux entreprises concernées par le transfert, et les règles internes d'entreprise (BCR, *binding corporate rules*) qui peuvent être mises en place au sein d'un groupe international de sociétés pour permettre le transfert de données au sein du groupe. Par ailleurs, les transferts sont autorisés à destination des entreprises américaines ayant adhéré au régime du *Safe Harbor* dans le cadre de l'accord conclu entre l'UE et les Etats-Unis en 2001, même si la Commission européenne a récemment pu s'émouvoir de l'insuffisance, selon elle, des contrôles mis en œuvre aux Etats-Unis pour s'assurer du respect de conditions de protection adéquates par ces entreprises.

Dans la pratique, ces outils sont difficiles à mettre en place en raison des formalités à accomplir auprès des différentes autorités nationales de protection des données personnelles. Ils sont également inadaptés à la réalité des offres du *Cloud Computing* pouvant faire intervenir plusieurs prestataires et sous-traitants et, comme on l'a vu, permettant la circulation des données d'un pays à l'autre. Au sein même de l'UE, la transposition de la Directive de 1995 (Directive 95/46/CE du 24 octobre 1995, 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 N° Lexbase : L8240AUQ) par les Etats membres comporte des divergences importantes, rendant difficile pour les entreprises la circulation des données.

Ces freins et ce manque d'harmonisation incitent les entreprises, responsables de traitement selon la loi, à la prudence et, pour éviter tout risque, à privilégier des offres de *Cloud Computing* n'entraînant pas le transfert des données personnelles dont elles sont responsables en dehors de l'Union Européenne. Ainsi, dans son guide "Externalisation et sécurité des systèmes d'information : maîtriser les risques", l'ANSSI (Agence nationale de sécurité des systèmes d'information) indique "*qu'en l'absence de cadre juridique international adapté à l'informatique en nuage, il est préférable de s'assurer que les données à caractère personnel restent localisées sur des serveurs exclusivement situés dans l'Union européenne -voire en France— et de prévoir les moyens de contrôle de cette obligation*".

III — Les perspectives d'évolution du cadre règlementaire au niveau européen et national

Deux mouvements parallèles sont en marche au niveau des instances européennes. Tout d'abord, la nécessaire révision de la Directive de 1995 sur la protection des données personnelles, afin de prendre en compte l'évolution du monde numérique et de tirer les conséquences du manque d'harmonisation des réglementations nationales relatives à la protection des données à caractère personnel, obligeant les sociétés tant européennes qu'étrangères à traiter avec les autorités de chacun des vingt-sept Etats membres, ce qui constitue un obstacle au marché unique européen. Ensuite, la Commission s'intéresse depuis 2009 au phénomène du *Cloud Computing*, tant au niveau des promesses économiques pour l'industrie européenne qu'en matière des risques qu'il présente eu égard à la sécurité des données, la fiabilité des systèmes, l'interopérabilité et la transportabilité permettant de changer de fournisseur de *Cloud*. Bien entendu, la question de la protection des données personnelles est au cœur de ces réflexions.

Ainsi, une consultation publique a été lancée par la Commission européenne en janvier 2011 à l'initiative de la commissaire Neelie Krœs pour alimenter la réflexion sur la stratégie européenne à adopter en matière de *Cloud Computing*, y compris pour parvenir à une réglementation mieux adaptée. Des centaines de réponses ont été adressées à la Commission européenne par les acteurs du marché. Néanmoins, c'est sans attendre les résultats de cette consultation que le nouveau projet de Règlement européen sur la protection des données personnelles a été publié le 25 janvier dernier. En effet, la commissaire Vivianne Reding a affiché la volonté d'aller vite, optant pour un Règlement plutôt qu'une nouvelle Directive, et de faire adopter ce règlement par les Etats membres avant la fin de l'année 2014. Il est important de noter que la Commission européenne s'est réservée sur près du tiers du texte la possibilité d'une seconde lecture sur laquelle elle aura le contrôle (par le biais de ce que l'on nomme les "actes délégués"). Si ce projet est adopté, il sera d'application directe et se substituera à la Directive 95/46/CE et aux législations nationales actuellement en vigueur dans les vingt-sept Etats membres. Les entreprises n'auront ainsi à se conformer qu'à une législation pan-européenne plutôt qu'à vingt-sept comme c'est le cas aujourd'hui, ce qui est plutôt une bonne nouvelle.

En ce qui concerne le texte du projet de Règlement, il traite de toute la problématique de la protection des données personnelles, bien au-delà de la question spécifique du *Cloud* et du transfert des données personnelles en dehors de l'Union européenne. Le projet prévoit un renforcement des obligations pour les entreprises, en particulier en matière de procédures internes, et de lourdes sanctions en cas de défaut de conformité avec toutefois, en contrepartie en quelque sorte, un allègement des obligations de notification des traitements de données personnelles, prenant en compte le niveau de risque pour les personnes concernées, et une simplification des démarches et formalités à accomplir par les entreprises collectant des données personnelles puisqu'elles n'auraient plus qu'à traiter avec l'autorité du pays de leur établissement principal ("*one stop shop approach*"). Pour le transfert hors UE de données personnelles par les entreprises européennes responsables de traitement, lié à l'externalisation de leur système d'information, la règle de la protection adéquate accordée par la législation d'un pays étranger aux données à caractère personnel reste la même, et le projet de Règlement propose l'adoption par les entreprises de règles internes d'entreprise (BCR) -avec la question de savoir si ces BCR peuvent s'appliquer aux sous-traitants ou demeurent confinées aux relations intra-groupe— ou des "Clauses Contractuelles Types".

Il est à noter, en particulier, que les sanctions prévues dans le projet de règlement vont de 0,5 % à 2 % du chiffre d'affaires mondial des sociétés en infraction, dans une approche similaire à celle des sanctions applicables en cas de violation des règles de concurrence. Certes, le but est d'assurer le respect de la protection des données à caractère personnel, mais il est regrettable que le projet de Règlement mette au même niveau une violation volontaire des règles et une simple négligence.

Tous ces éléments feront à n'en pas douter l'objet de débats intenses avec les Etats membres, et nombreux sont ceux qui nécessitent d'être clarifiés dans le texte du projet de Règlement. Parmi les premières réactions de l'industrie figure l'identification du contraste entre l'approche européenne, fondée sur un principe d'autorisation des transferts de données à caractère personnel, et celle d'autres pays qui font place à une démarche volontaire de transparence et de responsabilité par les entreprises (référence au concept d'*accountability*, difficilement traduisible en français). Aux Etats-Unis et dans certains pays d'Asie, l'approche consiste à donner des règles aux entreprises tout en leur faisant confiance pour leur mise en place, sans besoin de respecter une procédure administrative préalable, un contrôle continu du respect et de la conformité aux règles pouvant cependant être exercé par les autorités responsables. Or, aujourd'hui en Europe, tout un ensemble de règles est mis en place, qui se traduit par de lourdes formalités qui sont un véritable fardeau pour les entreprises sans la moindre contrepartie. Il est à craindre que cette lourdeur administrative soit de nature à pénaliser les entreprises européennes et à porter atteinte plus généralement à l'attractivité du marché européen.

Il a été évoqué lors de la table ronde du 14 février 2012 qu'en tout état de cause, il semble fondamental pour les entreprises intervenant dans le contexte du *Cloud Computing* d'adhérer à un principe de transparence sans attendre la mise en œuvre de la nouvelle réglementation. Les entreprises doivent être transparentes quant aux traitements des données personnelles afin de créer la confiance indispensable de la part des clients, des consommateurs et des autorités. Sans cela, quelles que soient les règles et les sanctions en place, le système ne pourra pas fonctionner. Cette transparence peut par exemple être réalisée par les prestataires du *Cloud* en donnant à leurs clients un accès direct, à tout moment, à des sites sécurisés affichant à tout instant la localisation de leurs données.

En conclusion, il transparaît de cette remise en question du cadre réglementaire existant, tant au niveau national qu'européen, que l'ensemble des acteurs européens se rendent compte des enjeux économiques liés au *Cloud Computing* et du risque pour l'Europe de ne pas pouvoir offrir un environnement à même de permettre aux entreprises européennes utilisatrices de bénéficier des avantages du *Cloud Computing*, ni de permettre à des prestataires européens de développer des solutions et des offres de *Cloud Computing*. Les deux années à venir vont donc être très intéressantes de ce point de vue, et critiques pour l'Europe.