cigref

Réseau de Grandes Entreprises

La réalité du Cloud dans les grandes entreprises

SYNTHESE

Un certain nombre d'évolutions des modèles, des organisations et des technologies liés aux systèmes d'information sont actuellement des vecteurs de transformation des entreprises. Parmi celles-ci le *Cloud Computing* occupe une place prééminente.

Il suffit pour s'en convaincre de recenser les entreprises ayant au moins un projet de *Cloud* en cours, souvent en phase très avancée, voire déjà opérationnel. Certaines d'entre elles, pour être parties très tôt dans l'expérimentation, en sont à exploiter leur troisième génération de *Cloud*.

On peut affirmer que le degré de maturité des grandes entreprises dans la compréhension de l'apport du *Cloud* est à présent élevé. Un changement d'état d'esprit s'y est produit, dans les équipes de la fonction SI aussi bien que dans les directions métiers au sein desquelles l'image de la fonction SI est d'ailleurs en forte évolution.

3 ans après avoir analysé les « fondamentaux du *Cloud Computing* » et la question de « la protection des données dans le *Cloud* », le CIGREF a interrogé ses adhérents sur les raisons de leur passage au *Cloud*. Il en ressort principalement que

- la pression des directions métiers,
- le *Cloud* comme vecteur d'innovation et d'agilité,
- la pression des fournisseurs,
- la simplification des infrastructures,
- la réduction des coûts,

se révèlent comme les principaux moteurs d'adoption de solutions de *Cloud*.

Pour autant, l'introduction du *Cloud* comporte aussi sa part d'ombre et de difficultés dans sa mise en œuvre ; l'étude s'est donc aussi intéressée :

- à la gouvernance à mettre en place,
- aux problématiques de mise en œuvre,
- à la difficulté d'évaluer le niveau de sécurité et d'assurer la conformité à la réglementation d'une offre *Cloud*,
- aux difficultés de contractualisation avec les fournisseurs,
- aux problèmes d'adaptation de la réglementation à cette innovation que représente le *Cloud*.

Pour éclairer ce dernier point, le rapport dresse un état des lieux de la réglementation et des réflexions menées sur son évolution, en France comme en Europe. L'objectif étant de contribuer à cette évolution et en proposant quelques pistes d'action.

Le CIGREF, réseau de Grandes Entreprises, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...). Le CIGREF a pour mission de promouvoir la culture numérique comme source d'innovation et de performance.

TITRE DU RAPPORT : LA REALITE DU *CLOUD* DANS LES GRANDES ENTREPRISES

EQUIPE DU CIGREF :

Jean-François PÉPIN – Délégué général
Sophie BOUTEILLER – Directrice de mission
Anne-Sophie BOISARD – Directrice de mission
Josette WATRINEL – Secrétaire de direction
Flora FISCHER – Chargée de programme de recherche
Frédéric LAU – Directeur de mission
Matthieu BOUTIN – Chargé de mission
Marie-Pierre LACROIX – Chef de projet
Josette LEMAN – Assistante de direction

REMERCIEMENTS :

Nos remerciements vont à Jean-Claude LAROCHE, Directeur des systèmes d'information Groupe EDF, qui a piloté cette réflexion, ainsi qu'à ceux qui ont activement contribué à l'élaboration de ce rapport : Eric ROBERT – EDF, Olivier LIGNEUL - EDF, Cyril BARTOLO - LAGARDÈRE.

Nous remercions également les personnes qui ont participé à la réflexion :

Danielle BILLARD - ORANGE / DSI
Xavier BOILEAU - AXA GROUP SOLUTIONS
Christophe BOUCHER - HARMONIE MUTUELLE
Christophe BREGERAS - FONDATION DE FRANCE
Philippe BRON - SGMAP
Jérôme CAEL - ESSILOR
Antoine CAO - SGMAP
Olivier CATELIN - GIP MDS
Hervé CICCHELERO - MINISTERE DE LA DEFENSE
Jean-Marc DANTY - MINISTERE DE LA DEFENSE
Gilles DAUSSY - LVMH
Olivier DE BERNARDI - SOCIÉTÉ GÉNÉRALE
Eric DEWILDE - CREDIT AGRICOLE SA
Rédouane EL BENNANE - NEOPOST
Dominique FACE - FRANCE TELEVISIONS
Robert FOUQUES - MACIF
Jean-Louis GHIGLIONE - RENAULT
Pierre GODELAINE - SOLVAY
Mathias HALLOSSERIE - GEODIS
Benoît HERMENT - ELIOR
Frédéric HUEBER - AIR FRANCE KLM
Renaud JAHAN - SAINT-GOBAIN
Laurent LE BLAY - MINISTÈRE DE L'INTÉRIEUR
Emmanuelle LEMIERE - CLUB MÉDITERRANÉE
François MARSOLLIER - RENAULT
Alain MECCHI - MINISTÈRE DE L'INTÉRIEUR
Alain MERLE - SGMAP
Vincent NIEBEL - MINISTÈRE DE L'INTÉRIEUR
Marc NOEL - AXA GROUP
Florence PATROUILLER - CREDIT AGRICOLE SA
Maximiliano PELUSO - AXA FRANCE SERVICES
Luc PIERRE-DIT-MERY - SGMAP
Jean-Luc RAFFAËLLI - LA POSTE
Sasun SAUGY - MINISTÈRE DE L'ÉCONOMIE, DE L'INDUSTRIE ET DU NUMÉRIQUE
Lucien VIEIRA - LVMH
Konstantinos VOYIATZIS - EDENRED
Michèle WALTER - AIR FRANCE KLM

Ce document a été rédigé par Frédéric LAU (CIGREF) et par les contributeurs d'EDF.

POUR TOUT RENSEIGNEMENT CONCERNANT CE RAPPORT, VOUS POUVEZ CONTACTER LE CIGREF AUX COORDONNEES CI-DESSOUS :

CIGREF, Réseau de Grandes entreprises
21, avenue de Messine 75008 Paris
Tél. : + 33.1.56.59.70.00
Courriel : contact@cigref.fr

Sites internet :
http://www.cigref.fr/
http://entreprise2020.fr/
http://www.fondation-cigref.org/
http://www.histoire-cigref.org/
http://www.questionner-le-numerique.org
http://www.entreprises-et-cultures-numeriques.org

SOMMAIRE

1. Préambule 1
2. Introduction 3
3. Le *Cloud* : des attentes… une réalité 6
3.1. Pourquoi passer au Cloud ? Quatre raisons prioritaires… 7
3.1.1. Des raisons stratégiques 7
3.1.2. La pression des métiers 8
3.1.3. Un vecteur d'innovation 9
3.1.4. La pression des fournisseurs 9
3.2. … Et des promesses moins vérifiées 10
3.2.1. La simplification et l'harmonisation 10
3.2.2. La réduction des coûts 11
4. Mise en œuvre du *Cloud* : des facteurs clés de succès 13
4.1. La gouvernance 13
4.2. La contractualisation 14
4.3. La mise en œuvre 15
4.3.1. Intégration 16
4.3.2. Infrastructure réseau 17
5. *Cloud* et réglementation 18
5.1. Contexte 18
5.2. Rééquilibrer les responsabilités 18
5.3. Faire connaître la réglementation applicable 20
5.4. Bâtir quelques solutions de type « Certifications » 21
5.5. Participer à la réflexion 22
6. En résumé 25

FIGURES

Figure 1 : Points d'attention dans une négociation Cloud et qui contribueraient à plus de confiance dans le Cloud 24

1. PREAMBULE

Les membres du groupe de travail constitué pour la réalisation du présent rapport indiquent au préalable que celui-ci n'a pas vocation à représenter toute la diversité des entreprises, qu'il s'appuie sur les échanges intervenus au sein du groupe de travail et qu'il n'engage que le point de vue des participants à ce groupe.

❖

D'un point de vue économique, le marché grand public est devenu depuis quelques années le moteur de l'innovation numérique qui transforme profondément l'usage des technologies. Dans les entreprises, la demande des directions métiers évolue constamment en lien avec l'apparition de nouveaux modèles d'affaires. La notion de service se transforme et se renforce en réponse à la prééminence de l'expérience client. La donnée accroît sa suprématie et représente un véritable minerai pour les entreprises et l'agilité business devient une exigence dans un marché globalisé.

Or le *Cloud Computing* a été très tôt intimement lié à tous ces éléments aussi bien sur un plan conceptuel que technologique. Il induit pour les entreprises une nouvelle manière d'acheter, de consommer et d'offrir des services liés aux SI dans le monde ; il s'appuie essentiellement sur le réseau Internet et il impacte fortement les métiers de l'entreprise et l'organisation des systèmes d'information car il les fait entrer dans un mode de service récurrent.

Tout d'abord, les métiers n'utilisent plus un produit figé par des spécifications mais demandent un service qui évolue en permanence et met en œuvre de nouvelles fonctionnalités souvent innovantes, générant elles-mêmes de nouveaux usages.

A cet effet, on observe que les équipes de la DSI glissent d'un mode traditionnel de prestations de type « *service pack* » vers un mode de mise à disposition d'applications mises à jour automatiquement et en continu, ce qui induit des réorganisations internes pour pouvoir accompagner le cycle de vie des applications métiers, car penser service et non plus application implique une relation au client interne plus forte, le recours à de nouvelles compétences et à une organisation et une gestion des coûts adaptés.

Le *Cloud Computing* s'appuie ensuite sur des technologies qui permettent de bénéficier pleinement de la valeur de la donnée en la rendant accessible partout et à tous, sans limitation de lieu, de moyen et de stockage et ceci quel que soit le terminal[1].

[1] Terminal : *device* (ordinateur portable, smartphone, tablette…)

Il se positionne au cœur de la transformation numérique des entreprises parce qu'il rend possible :

- le décloisonnement des organisations par un accès plus large aux données,
- la mobilité par sa compatibilité avec les différents terminaux et son indifférence à leur localisation géographique,
- l'affranchissement du temps par la possibilité de travailler n'importe quand du fait de la permanence du service rendu (même si ce point ne constitue pas un avantage exclusif du *Cloud*),
- le « *Time to Market* » par la prise en compte immédiate des nouvelles fonctionnalités.

Cependant, tout en permettant l'apparition, dans et hors de l'entreprise, de nouveaux services sans cesse innovants, le *Cloud Computing* génère un domaine nouveau de questionnements dont la donnée est le centre : Il s'agit de savoir notamment comment la protéger, la catégoriser, l'utiliser, la maîtriser et la valoriser. Si les entreprises peuvent prétendre jusqu'à présent plus ou moins bien gérer le risque « donnée » en leur sein, le *Cloud Computing* étend désormais le périmètre de ce risque à tout leur environnement, voire à l'ensemble du monde.

En conséquence, pour la première fois au CES 2015 (*Consumer Electronic Show)* de Las Vegas, la question de la « sécurité de la donnée dans le *Cloud* » a été mise en avant, sans doute en lien avec les affaires de fuite ou d'espionnage qui défraient la chronique. Les éditeurs ne semblent pas encore, dans leur majorité, avoir intégré dans leurs offres les contraintes et les besoins des entreprises sur la protection de leur patrimoine numérique, notamment des données à caractère personnel. Pourtant, la résolution des questions de sécurité relatives au *Cloud* apparaît comme un prérequis pour l'instauration de la confiance, préalable indispensable avant tout transfert de la gestion de ces données à des infrastructures et/ou des applications en mode *Cloud* et toute proposition de services associés.

2. INTRODUCTION

Un certain nombre d'évolutions des modèles, des organisations et des technologies liés aux systèmes d'information sont actuellement des vecteurs de transformation des entreprises. Parmi celles-ci le *Cloud Computing* occupe une place prééminente.

Cette transformation concerne d'abord les métiers avec le développement de nouveaux modèles de services mais elle impacte également les infrastructures car elle est rendue possible par la virtualisation des systèmes et des applications.

Le CIGREF s'intéresse au *Cloud* depuis 2010. A l'époque, l'offre commençait à faire partie du paysage des solutions et des services liés aux systèmes d'information, mais le marché était en cours de structuration et l'offre ne répondait que partiellement aux besoins fonctionnels des DSIs. Néanmoins les entreprises entrevoyaient déjà que le *Cloud* serait source d'innovation en termes de services, d'efficacité, de *sourcing* et d'architecture.

La Fonction SI se préparait alors à un rôle d'intégrateur, dans les processus métiers, entre les solutions *Cloud* et les autres solutions constituant le patrimoine applicatif de l'entreprise étendue. Les questions réglementaires liées à la protection du patrimoine numérique et à la sécurité numérique des entreprises, en relation notamment avec la localisation de l'information et des données, n'étaient qu'émergentes.

« *Faire différent, plus vite, moins cher, en optimisant les ressources* » tel était alors le message des dirigeants. Ce qui impliquait pour l'entreprise performance, innovation, agilité et rapidité dans la conception, réalisation et distribution de nouveaux produits et services.

En 2013, le développement des offres de *Cloud Computing* est progressivement devenu une opportunité incontournable pour les organisations. A cette date cependant, l'ensemble des acteurs du marché (fournisseurs comme clients) manquaient encore de maturité et une certaine confusion régnait entre les modèles de services (XaaS[2]) et la technologie associée au *Cloud*. Commençait également à se répandre un discours critique sur les problématiques de sécurité liées au *Cloud*.

Afin de répondre aux difficultés de compréhension de ce que représentaient les modèles de service (XaaS) et le *Cloud Computing*, le CIGREF a alors publié un rapport intitulé « Les fondamentaux du *Cloud Computing* : le point de vue des grandes entreprises ». Ce document

[2] XaaS : Terme générique désignant l'ensemble des modèles « *As a Service* »

a proposé une définition claire des concepts associés au *Cloud*, en fonction de leur mise en œuvre dans les entreprises et non à partir des offres du marché, très disparates à l'époque :

« *Un Cloud est un espace virtuel contenant des informations fragmentées, dont chaque fragment est dupliqué et réparti (ou distribué) dans cet espace virtuel, lequel peut être sur un ou plusieurs supports physiques. Un Cloud possède toujours un programme unique qui permet de reconstituer l'information à partir des fragments éparpillés dans cet espace virtuel* »[3].

Le rapport du CIGREF a mis en évidence que le *Cloud* sert très souvent d'appui à des modèles de services de type IaaS (*Infrastructure as a Service* : mise à disposition de Machines Virtuelles pour du stockage à la demande, ou du service réseau à la demande) ou SaaS (*Software as a Service* : applications mises à disposition sous forme de services le plus souvent utilisés directement par les métiers) ou enfin PaaS[4] (*Platform as a Service*).

En plus d'une définition et des modèles de services, le CIGREF a identifié quatre types de *Cloud* dont la combinatoire permet de décrire l'ensemble des *Clouds* existant aujourd'hui :

- *Cloud* géré en interne à l'entreprise par des équipes de l'entreprise ou des prestataires, à usage privé pour l'entreprise ;
- *Cloud* géré en interne à l'entreprise par des équipes de l'entreprise ou des prestataires, à usage ouvert aux partenaires, clients ou publics ;
- *Cloud* géré en externe, par un opérateur, à usage privé pour l'entreprise ;
- *Cloud* géré en externe, par un opérateur, à usage ouvert aux partenaires, clients ou publics.

Pour aborder et comprendre les problématiques de sécurité, le CIGREF a aussi publié en 2013, en partenariat avec l'AFAI et l'IFACI, un guide pratique[5] à destination des directions générales et des directions Métiers des entreprises. Ce document vise à les sensibiliser sur les risques liés au *Cloud* et sur les pratiques à mettre en œuvre lors de la souscription d'une offre *Cloud*. Ces dernières portent notamment sur le choix d'une offre adaptée en fonction

[3] Rapport CIGREF – 2012-2013 – Fondamentaux du *Cloud Computing* - le point de vue des grandes entreprises : http://www.cigref.fr/*Cloud*-computing-si-entreprise-2012

[4] A l'heure actuelle, le PaaS est moins mis en œuvre par les entreprises qui trouvent cette technologie moins mature et pointent notamment une ligne de partage de responsabilité floue entre les exploitants et les développeurs. Certaines entreprises s'intéressent également au CaaS (*Container as a Service*), concept en émergence, qui pourrait apporter des facilités de mise en œuvre des PaaS.

[5] Guide CIGREF – IFACI- AFAI – 2012 - *Cloud* et protection des données : guide pratique à l'attention des directions opérationnelles et générales : http://www.cigref.fr/*Cloud*-protection-donnees-guide-pratique-direction-operationnelle-generale

de la typologie des données à transférer et sur la gouvernance et le contrôle de conformité à mettre en place.

Aujourd'hui, en 2015, avec pour certaines une expérience d'ores et déjà éprouvée, les entreprises ont bien compris les enjeux et la valeur ajoutée du *Cloud* pour leur métier.

Il devient donc nécessaire pour le CIGREF de refaire le point sur le sujet et en particulier, il s'agit de regarder comment le *Cloud Computing* est utilisé dans les grandes entreprises : quels sont les gains / freins et la valeur créée ? La promesse d'amélioration de la performance de l'entreprise s'est-elle vraiment réalisée ?

Il s'agit aussi d'évoquer les « *Clouds* Souverains » et « *Cloud* Confidence », ainsi que l'état de la réglementation française comme européenne, qui tente tant bien que mal d'encadrer les usages et le marché, notamment d'un point de vue de la sécurisation des données.

3. LE *CLOUD* : DES ATTENTES… UNE REALITE

Les participants au groupe de travail ont tous mentionné au moins un projet *Cloud* en cours, souvent très avancé, voire déjà opérationnel. Certaines entreprises parties très tôt en sont même à leur troisième génération de *Cloud* en exploitation.

On peut désormais affirmer que la maturité des grandes entreprises quant à la compréhension de l'apport du *Cloud* est significative. Elle se traduit souvent par un changement d'état d'esprit des équipes SI comme des directions métiers. Le *Cloud* apparaît de plus en plus comme incontournable, et c'est pourquoi il apparaît important d'associer tous les collaborateurs et toutes les équipes dans la démarche de passage au *Cloud*. Certaines entreprises déconseillent même de mettre en place une « cellule *Cloud* » qui créerait une spécialisation au sein de la DSI.

Avec le *Cloud*, l'image du SI change auprès des directions métiers. Cela se traduit par une évolution des échanges avec la DSI sur :

- la valeur ajoutée du *Cloud* pour l'entreprise ainsi que sa mesure,
- les évolutions business à venir auxquelles les solutions *Cloud* pourront être associées,
- les possibilités offertes par les nouvelles architectures d'entreprise grâce au *Cloud*,
- le niveau de contractualisation sur les choix techniques fondamentaux liés aux solutions *Cloud*.

Les applications et services mis en œuvre sur des *Clouds* sont désormais nombreux. Ceux pour lesquels le recours à ces solutions *Cloud* (en mode SaaS en l'occurrence) est le plus souvent mis en avant par les membres du groupe de travail sont la messagerie, le stockage et le partage de documents.

Mais on trouve aussi d'autres usages comme par exemple la synchronisation des données entre ordinateurs et outils mobiles, la signature digitale, les réseaux sociaux d'entreprise, les suites bureautiques, les outils de CRM, etc…

Pour toutes ces applications, les entreprises entrevoient un intérêt aux solutions *Cloud* :

- D'un point de vue opérationnel du fait de :
  - l'existence d'un catalogue de services,
  - la facilité de mise en œuvre, surtout dans le cas de *Clouds* externes.
- D'un point de vue de la qualité de service de l'infrastructure en raison :
  - du taux de disponibilité des infrastructures (7/7 24/24), en particulier pour les *Clouds* externes
  - de l'adaptation aisée des infrastructures aux pics d'activité.
- D'un point de vue de la réponse au besoin de *Time to Market* court en raison de l'agilité de ces solutions et de la rapidité de leurs mises à jour.

Il semble toutefois, pour le moment, qu'une partie du SI historique ne migrera jamais dans le *Cloud* en raison :

- du coût de la transformation à opérer qui dépend de la complexité des architectures et des applications déjà en place,
- du risque de cette transformation dû à la complexité de migration sans rupture du service.

La plupart du temps, l'opportunité de basculer sur le *Cloud* est liée soit à une refonte complète de l'application, soit à la mise en place de nouveaux services. Ce qui explique que les applications *front office* (en lien direct avec les métiers et les clients de l'entreprise) soient les premières à bénéficier des avantages du *Cloud* car elles requièrent une forte agilité pour répondre rapidement aux usages et besoins des clients et plus généralement pour être en phase avec l'évolution du marché de l'entreprise.

Nous examinons ci-dessous les principales raisons ou attentes qui conduisent les entreprises vers le *Cloud*.

3.1. Pourquoi passer au Cloud ? Quatre raisons prioritaires…

3.1.1. Des raisons stratégiques

Plus souvent qu'on ne le pense, la réduction du coût du SI n'est pas le moteur principal de la décision. Bien souvent la décision est issue d'un besoin conjoncturel ou d'une vision stratégique du business ou des dirigeants de l'entreprise.

Par exemple, à la suite de nombreuses acquisitions, une entreprise a préféré vouloir fédérer les fonctions et usages des applications métiers support (financier, RH, achats…) autour d'une application *Cloud* plutôt que de tenter de faire cohabiter ou de redévelopper les différents outils de chaque entité acquise. Dans une autre, c'est le Dirigeant qui cherche à tirer parti du la puissance du *Cloud* pour prendre un avantage compétitif sur ses concurrents.

Offrir de nouvelles solutions plus souples mais maîtrisées aux clients ou aux salariés peut aussi se révéler comme un critère de décision. Une hypothèse envisagée par certaines entreprises est d'autoriser leurs salariés à accéder à leur propre *Cloud* à partir des réseaux de l'entreprise, à l'image du BYOD[6] qui leur permet d'utiliser leur propre équipement (généralement smartphone) dans l'entreprise.

[6] « *Bring Your Own Device* »

3.1.2. La pression des métiers

Deuxième raison : la pression des métiers. De fait, celle-ci s'est toujours exercée sur la DSI. Elle porte sur la réponse aux besoins, les délais et les coûts.

La facilité apparente de consommation de services dans le *Cloud* l'accentue notablement : en effet la présentation des services offerts dans le *Cloud* peut faire croire aux métiers qu'il suffit de passer une simple commande pour les mettre en œuvre.

Les directions métiers ont très vite compris l'avantage qu'elles pourraient tirer d'applications dans le *Cloud*. D'une part, et comme indiqué précédemment, la mise en œuvre de *Clouds* publics tournés vers les clients leur permet d'être très agiles et réactives face au marché et aux besoins changeants des clients/utilisateurs.

D'autre part, le *Cloud* représente un espoir d'indépendance vis-à-vis de la DSI sur des projets qui nécessitent une expérimentation rapide ou qui ont une durée de vie courte. (Le groupe de travail ne cautionne d'ailleurs pas cet espoir d'indépendance, parce que l'accompagnement par les DSIs des métiers qui adoptent une solution *Cloud* reste une nécessité, pour les raisons d'intégration au SI de l'entreprise, de contractualisation et in-fine de maîtrise des coûts qui seront développées plus loin.)

Les directions métiers peuvent ainsi aujourd'hui choisir des services en ligne qui sont offerts sur un *Cloud* public et donc challenger implicitement la DSI sur leurs choix. Leurs besoins, tirés par la nécessité d'un *Time to Market* court, impliquent agilité et flexibilité de la part du SI et des solutions retenues. Les avantages promus par le *Cloud* et qui rejoignent leurs attentes sont les suivants :

- S'affranchir d'une infrastructure qui semble compliquée,
- Permettre la mise en œuvre de SIs temporaires que l'on monte rapidement (solutions intéressantes pour des événements ponctuels),
- Monter des solutions pour lesquelles on ne souhaite pas investir dans l'immédiat,
- Proposer des services non encore fournis par la DSI.

Cette pression des métiers conduit souvent la DSI à avoir un rôle de type « *Cloud Broker* » et à mettre en place une instance multipartite qui arbitre sur les choix métiers. Maîtriser ainsi les demandes du métier demeure nécessaire notamment pour freiner le *shadow-IT*[7], qui reste une source de difficultés et de surcoûts pour l'entreprise.

[7] *Shadow IT* (parfois *Rogue IT*) est un terme fréquemment utilisé pour désigner des systèmes d'information et de communication réalisés et mis en œuvre au sein d'organisations sans approbation de la direction des systèmes d'information.

3.1.3. Un vecteur d'innovation

Troisième raison : l'innovation.

Le *Cloud Computing* véhicule une autre façon de voir l'informatique et le système d'information et offre notamment une facilité nouvelle dans l'innovation. Il permet en effet de tester de nouveaux services et applications, de nouveaux concepts technologiques ou métiers plus rapidement, en limitant les impacts sur le SI existant.

Sur le plan de l'organisation de la fonction informatique dans l'entreprise, le *Cloud* apparaît aussi comme un vecteur de transformation, car les solutions IaaS représentent une évolution naturelle des *Datacenter* : dans les démarches actuelles de rationalisation, les entreprises s'obligent à s'intéresser plus aux usages qu'aux infrastructures qui sont progressivement vues comme une contrainte et non plus comme le moteur principal de la transformation. Pourtant la maîtrise des infrastructures reste une nécessité pour les entreprises, mais celle-ci se déplace progressivement de problématiques techniques vers des problématiques contractuelles avec les acteurs du *Cloud*, comme nous le verrons ci-dessous.

3.1.4. La pression des fournisseurs

Quatrième raison : la pression des fournisseurs.

On peut distinguer deux types de fournisseurs de *Cloud* :

1. Ceux qui disposent d'une offre plutôt de niche, assez spécialisée. Ces derniers ne visent pas nécessairement le volume, mais une marge suffisante client par client. Leurs atouts sont leurs compétences « spécifiques », mais aussi le mode « service » qui évite à l'entreprise d'investir sur des sujets soit éloignés de son cœur d'activités, soit très prospectifs ou émergents.
2. Ceux qui proposent une offre de masse et qui font du profit sur la mutualisation. Le présent paragraphe s'applique prioritairement à ce type de fournisseurs.

Certains fournisseurs de *Cloud* externes jouent donc sur l'effet volume pour pouvoir proposer des offres agressives. Ils cherchent à placer leurs offres *Cloud* auprès d'un maximum d'entreprises. Pour cela ils ciblent en priorité les directions métiers et très souvent avec succès, nonobstant l'adhérence forte à certaines solutions qui permet parfois difficilement de mettre en œuvre les clauses de réversibilité[8].

[8] On parle de réversibilité pour dire qu'en cas de rupture de contrat d'infogérance externalisée, le prestataire doit fournir toute information utile au client pour permettre au prestataire repreneur, ou au service informatique interne, d'assurer la reprise de la gestion du système informatique. La réversibilité a pour finalité

Cette pénétration de l'offre *Cloud* entraîne des conséquences : les entreprises doivent accepter d'utiliser des solutions standard qui ne rentrent pas forcément dans leurs référentiels actuels. Les contraintes de rationalisation et les règles d'exploitation et d'engagement de service des fournisseurs sont difficilement adaptables aux besoins particuliers d'une entreprise. Avec ce type de *Cloud* externe l'entreprise est contrainte de s'adapter.

On observe aussi du côté des éditeurs de logiciel une volonté de proposer leurs solutions uniquement sur le *Cloud*, et non plus par une installation de leur produit sur les machines de leurs clients. L'entreprise peut alors se trouver dans une transition forcée difficilement gérable en raison du niveau de sensibilité des données manipulées par les logiciels concernés.

3.2. … Et des promesses moins vérifiées

3.2.1. La simplification et l'harmonisation

Le *Cloud* apporte une « promesse » initiale de simplification et d'harmonisation dans un certain nombre de domaines :

- Celui des architectures et des infrastructures serveurs : Dans le cas de Clouds privés, c'est prioritairement la rationalisation des Datacenter qui est recherchée. L'objectif est de faire diminuer l nombre de serveurs classiques (de fait il tend vers zéro dans le cas de *Cloud* externes) pour bénéficier d'une réduction du coût lié à leur exploitation/support. L'objectif est aussi de tirer tout le profit d'une architecture flexible, qui permette par exemple de provisionner rapidement et automatiquement des capacités sur différents sites. Le mécanisme d'automatisation nécessaire pour la mise en place du *Cloud* doit enfin apporter le bénéfice d'une réduction drastique du nombre d'erreurs humaines.

- Celui du fonctionnement général de l'entreprise : dans les entreprises fortement décentralisées ou organisées en de multiples entités, le *Cloud* doit permettre de s'affranchir de la multiplicité des solutions. Pour les Groupes qui sont dans une configuration d'acquisition d'entreprises, il apparaît plus aisé de fédérer chacune d'entre elles autour de services métiers communs plutôt que de faire cohabiter les

de permettre au client de ne pas être dépendant de son prestataire informatique dans le cas où il souhaite rompre le contrat.

différents systèmes historiques de ces entreprises. Le *Cloud* doit donc faciliter la normalisation et l'harmonisation des systèmes d'informations de l'entreprise.

Pour autant, l'expérience montre aussi que si les approches *Cloud* masquent aux utilisateurs et aux métiers la complexité « traditionnelle » du SI, elles ne la réduisent pas pour autant. De même si elles améliorent l'interopérabilité des systèmes, elles ne les harmonisent pas.

En réalité, même si certaines parties de l'architecture sont allégées ou simplifiées, les problèmes sont souvent reportés vers d'autres domaines comme la connectivité (le réseau, les passerelles etc…), la gestion des droits et habilitations (SSO[9], annuaire d'identité…) et l'interopérabilité.

La simplification et l'harmonisation réelles des SI passent prioritairement par l'urbanisation du SI, la classification et la gouvernance des données, comme avant mais dans un contexte rendu lui plus complexe par l'ouverture à l'extérieur (dans le cas de *Cloud* externe).

La maîtrise de toutes ces dimensions confère aux DSIs un rôle clé de coordination et de conseil.

3.2.2. La réduction des coûts

Les membres du groupe de travail ont été prudents sur ce sujet.

Parmi les arguments mis en avant par les fournisseurs de *Cloud*, les gains financiers viennent souvent en tête. Or les discussions au sein du Groupe de Travail du CIGREF montrent que cette promesse n'est pas nécessairement vérifiée dans certaines situations : l'exemple régulièrement cité est celui du IaaS en mode *Cloud* privé. En effet, il peut arriver que les équipes internes aux entreprises opèrent des plateformes virtualisées avec des technologies semblables à celles du *Cloud*, pour des coûts inférieurs à des offres comparables de grands fournisseurs de *Cloud*. Cette situation peut être amenée à évoluer avec la maturité des grands fournisseurs de *Cloud*, et il pourrait être utile de refaire le point sur ce sujet d'ici quelques années. Pour autant, le maintien d'équipes internes, dans certaines entreprises, capables de mettre en œuvre des plateformes virtualisées demeure un bon moyen de maintenir une certaine pression concurrentielle sur les grands fournisseurs de *Cloud* et d'éviter que ceux-ci ne bénéficient d'une position oligopolistique à l'avenir.

[9] SSO : *Single Sign-On* centralisateur d'authentification permettant à l'utilisateur d'accéder à toutes les ressources (machines, systèmes, réseaux) auxquels il est autorisé d'accéder, en s'étant identifié une seule fois sur le réseau.

En ce qui concerne le SaaS les gains sont également difficiles à évaluer par manque d'éléments de comparaison avec un existant. De plus certains coûts induits sont difficiles à estimer comme ceux dus à l'augmentation des débits des réseaux à faible latence.

La promesse de diminution des coûts d'usage est aussi associée à la promesse de simplification dont les limites ont été exposées précédemment. Par exemple les entreprises sont intéressées par la messagerie sur le *Cloud* qui paraît avoir un très bon TCO[10] sur du court-moyen terme. Mais au-delà de 3 ans les entreprises constatent que la promesse de réduction des coûts devient incertaine et que sur le long terme, l'incertitude sur l'évolution des prix devient un véritable handicap.

Enfin, il convient de garder à l'esprit que le *Cloud* modifie la structure de coûts des systèmes d'information, parce qu'il substitue à des investissements un coût d'usage correspondant à l'utilisation du service. Il diminue donc les CapEx[11] et augmente les OpEx[12] de l'entreprise.

Cette variabilité des coûts est un facteur de complexité dans l'évaluation économique de projets dans le *Cloud*, comparée à des solutions plus traditionnelles. En effet, il faut comparer, pour ce qui est du *Cloud*, des coûts variables actualisés qui s'étendent sur toute la durée de vie de la solution retenue, avec, pour ce qui est des solutions plus traditionnelles, un coût d'investissement venant en amont, auquel s'ajoutent des coûts de maintien en condition opérationnelle pendant la durée de vie de la solution.

Parce que le *Cloud* n'exige pas l'investissement amont, il peut ressortir comme économiquement intéressant pour des solutions à durée de vie courte. Dès que la durée de vie s'allonge (au-delà de trois ans), il devient plus dur de démontrer l'intérêt des solutions hébergées dans le *Cloud*, d'autant que les coûts de ces services deviennent plus incertains à cet horizon, comme nous l'avons mentionné précédemment.

Le « *business case* » conduisant à adopter des solutions dans le *Cloud* doit donc être précisément établi sur la base d'hypothèses explicites, et les équipes SI gagneraient à expliciter la sensibilité du choix de la solution aux hypothèses retenues, en particulier la durée de vie de la solution.

[10] *Total Cost of Ownership*

[11] CapEx : *Capital Expenditures* : montant payé pour acquérir ou améliorer ses immobilisations corporelles ou incorporelles

[12] OpEx : *Operational Expenses* : représente les coûts d'exploitation

4. MISE EN ŒUVRE DU *CLOUD* : DES FACTEURS CLES DE SUCCES

4.1. La gouvernance

La plupart des entreprises estiment que le recours au *Cloud*, sous quelque forme que ce soit (interne ou externe), est inéluctable. Comme nous l'avons déjà évoqué, celui-ci provoque des transformations, nécessaires à l'entreprise dans sa démarche de transition vers le numérique, qui impliquent donc une gouvernance adaptée. Celle-ci repose sur l'association de l'ensemble des acteurs au projet *Cloud* au travers d'une organisation particulière visant à garantir le succès du projet et la maîtrise des risques induits.

Présenter de manière conjointe (par la DSI et les Directions Métier) cette gouvernance *Cloud* au plus haut de l'entreprise apparaît utile, voire indispensable. Quelques entreprises ont ainsi impliqué leur Comité Exécutif dans la décision d'adopter le *Cloud*. Il ne s'agissait pas seulement pour elles de chercher l'accord des dirigeants mais d'obtenir leur adhésion complète et leur soutien actif à cette stratégie.

L'un des objectifs de cette gouvernance est de créer les conditions pour que les directions métiers travaillent moins en silos et de manière transversale, mutualisent leurs réflexions et actions avec les autres directions et la DSI. Ceci, entre autres choses, pour éviter ou maîtriser le *shadow IT*.

Elle doit aussi prendre en compte les aspects sécurité pour les faire évoluer en conséquence. En particulier en ce qui concerne la classification des données : les entreprises membre du groupe de travail estiment que tout ne peut pas être mis dans le *Cloud*, et qu'il faut donc segmenter les données en fonction de leur niveau de sensibilité et de l'usage attendu : aussi devient-il nécessaire de préciser qui détient la responsabilité de ces données et dans quel cadre d'organisation, pour décider de leur usage, leur exploitation, leur protection, leurs évolutions, etc…Ces éléments deviennent constitutifs d'une véritable politique de la donnée.

Cette gouvernance doit aussi être capable de s'adapter pour gérer les évolutions fonctionnelles et techniques permanentes du *Cloud*. Elle doit donc permettre à l'ensemble des parties prenantes de suivre l'évolution technologique du *Cloud* et de son marché mais aussi de maîtriser ces évolutions en se donnant le temps de les tester pour pouvoir les intégrer.

Dans cette gouvernance, la DSI doit prendre toute sa place auprès des métiers pour les aider à sélectionner les bons produits et services, contractualiser de bonne manière avec les fournisseurs de *Cloud*, intégrer le service *Cloud* dans l'écosystème des systèmes

d'information de l'entreprise, mais aussi anticiper sur les innovations et les proposer de manière proactive aux métiers.

En termes d'organisation, certaines entreprises ont mis en place côté métiers un responsable « expérience client » et un responsable « expérience employés » pour couvrir l'ensemble des usages, internes et business, du projet de *Cloud*. Du côté du SI, c'est l'ensemble des équipes de la DSI qui doit être impliqué dans cette démarche touchant les services, les applicatifs, l'architecture, le réseau, les développements, la sécurité, les données etc…

Un point sensible est à garder en mémoire : l'arrivée du *Cloud* est susceptible de faire aussi évoluer le dialogue social : celui-ci doit désormais prendre en compte les changements rapides des outils, de l'organisation et de l'environnement de travail des salariés.

4.2. La contractualisation

Les entreprises membres du groupe de travail du CIGREF font le constat que les contrats des fournisseurs de produits et services dans le *Cloud* sont actuellement largement perfectibles dans l'intérêt des utilisateurs de ces offres. Or, un accord avec les fournisseurs nécessite une analyse approfondie et complexe des risques dans le nouveau paradigme du *Cloud*, requérant des compétences pointues et variées.

Généralement, ces contrats sont jugés trop en faveur des fournisseurs de services *Cloud*. Les entreprises utilisatrices doivent donc s'efforcer de les rééquilibrer (même si les négociations se révèlent souvent difficiles). Il s'agit en effet :

- Commercialement : de se mettre d'accord très en amont sur des prix et d'en limiter l'augmentation à l'occasion de l'éventuel futur renouvellement du contrat (par exemple 3 ans plus tard). Cela nécessite au passage d'adapter les processus d'achat au *Cloud* ;
- Sur le plan de la sécurité : de vérifier le niveau de sécurité du fournisseur - ce qui demeure difficile à faire en théorie et en l'absence de réelles certifications globales spécifiques au *Cloud* et élaborées par des organismes indépendants – et de traduire les engagements correspondants dans le texte du contrat ;
- Sur le plan des engagements : de responsabiliser davantage le fournisseur par des clauses de responsabilité, de réversibilité, de confidentialité et de tenter d'y introduire des clauses rarement prévues de responsabilité en cas de destruction des données ou de leur exposition à l'extérieur ;

- Sur le plan des SLAs[13], du support, des délais de correction, etc… : de parvenir à une mesure de la réalité du service apporté par le *Cloud*, mais également celle d'une dégradation des performances en cas de partage des infrastructures par plusieurs clients, dans le contexte d'un *Cloud* public. Sachant que les opérateurs ne s'engagent que sur des performances au sein de leurs *datacenters*, et pas via le réseau internet, ces SLA sont souvent insuffisants mais non négociables et les pénalités associées souvent dérisoires. Tous ces points peuvent constituer un obstacle au déploiement d'un *Cloud* et renforcent la nécessité de pouvoir conduire des audits sur les installations et sur leurs architectures, ainsi que sur l'organisation du fournisseur du service *Cloud* ;
- Sur le plan de la conformité juridique : de s'assurer que le contrat est conforme aux législations françaises et européennes.

La prise en compte de ces spécificités a donc pour répercussion, à l'entrée, de rallonger de façon substantielle les délais de contractualisation (souvent de plus d'un an et demi par rapport à un contrat classique) mais également d'en rendre la renégociation plus difficile.

Mais il s'agit aussi d'éviter de mettre de fait l'entreprise en situation de *Lock In*[14].

Pour pallier ce risque, il est conseillé :

- Dès la négociation du contrat n, de prévoir le délai de préavis de négociation du contrat n+1 pour avoir le temps de l'adaptation ou de la mise en œuvre de la réversibilité de manière sereine,
- D'inclure un plafond ou une option à lever pour parer une évolution trop significative des prix du contrat suivant.

4.3. La mise en œuvre

Mettre en place un *Cloud* dans le SI nécessite une mise en œuvre en mode projet, incluant par exemple l'anticipation de la capacité en bande passante, une migration, une intégration au SI de l'entreprise et une conduite du changement. Deux points ont plus particulièrement fait l'objet de recommandations de la part des membres du groupe de travail : l'intégration du *Cloud* dans le SI et l'infrastructure réseau.

[13] *Service Level Agreements*

[14] Ou « d'enfermement »

4.3.1. Intégration

La réussite de l'intégration du *Cloud* dépend en grande partie de l'ouverture du fournisseur à l'interopérabilité et à la portabilité, via des standards non propriétaires (c'est conseillé) et des API[15].

L'intégration doit aussi prendre en compte le délai nécessaire à l'adaptation aux contraintes spécifiques de l'entreprise en termes de sécurité, de règles d'accès à l'information, de gestion des données, etc…

Outre les points précédents, une bonne intégration implique de respecter quelques règles complémentaires, en particulier face à la multiplicité des offres de la part des fournisseurs de services dans le *Cloud* public :

- Il est préférable d'éviter les assemblages de *Clouds* de différents fournisseurs car cette intégration est difficile à garantir dans la durée du fait de leurs évolutions permanentes,
- Il convient de limiter le nombre de connecteurs dédiés à chaque éditeur ou fournisseur de service qui peut, au final, être très important.

D'une manière générale, l'intégration d'un *Cloud* externe au SI de l'entreprise ne peut faire l'économie d'une étude d'impacts en termes de sécurité et de mises à niveau potentiellement nécessaires.

Dans le cas de *Clouds* internes développés par l'entreprise, il convient aussi de prêter attention aux points suivants :

- L'investissement en développement peut être conséquent ;
- Faire évoluer le service n'est pas automatiquement simple ;
- Les modèles économiques internes de l'entreprise se trouvent modifiés (typiquement le développement d'un service *Cloud* doit s'accompagner d'une forte élasticité de l'offre en fonction de la demande, et d'une facturation à l'usage) ;
- Il ne faut pas construire un système trop lourd qui risque de devenir le *SI historique* de demain.

Déployer du *Cloud* en interne passe enfin par l'adaptation du management des infrastructures pour que celui-ci se fixe la « standardisation » et la souplesse dans la réponse aux besoins comme des objectifs prioritaires.

---

[15] En informatique une interface de programmation (souvent désignée par le terme API pour *Application Programming Interface*) est un ensemble normalisé de classes, de méthodes ou de fonctions qui sert de façade par laquelle un logiciel offre des services à d'autres logiciels. Elle est offerte par une bibliothèque logicielle ou un service web, le plus souvent accompagnée d'une description qui spécifie comment des programmes *consommateurs* peuvent se servir des fonctionnalités du programme *fournisseur*.

4.3.2. Infrastructure réseau

Intégrer un *Cloud* interne comme externe au SI de l'entreprise implique au préalable de repenser son infrastructure, notamment réseau.

En effet, Internet ne garantit pas les niveaux de services d'un réseau d'entreprise en temps de réponse (certains membres du groupe de travail ont illustré ce point avec l'exemple des pays asiatiques, mais le problème est généralisable partout dans le monde). Il ne permet donc pas d'avoir des performances garanties à la hauteur de ce qu'offraient les infrastructures classiques. Ce point est problématique lorsqu'il faut interconnecter plusieurs *Clouds* dans différentes régions ou pays.

Pour résoudre cette difficulté, plusieurs entreprises recourent aux services d'opérateurs d'accès centralisés et s'y connectent en mettant en place du *peering*[16] afin de garantir des temps de réponses stables.

[16] Appairage : interconnexion directe des réseaux entre opérateurs, fournisseurs ou entreprises clientes, pour fiabiliser le trafic de données et éviter d'utiliser les équipements, souvent public, des grands fournisseurs nationaux ou internationaux. Cela permet notamment d'une part d'augmenter la vitesse de transmission des données et, d'autre part, à éviter d'avoir à verser des sommes considérables aux exploitants des grands réseaux.

5. *CLOUD* ET REGLEMENTATION

5.1. Contexte

Le traitement des données, notamment personnelles, dans les différents pays européens présente des situations très disparates. Si tous les Etats se fondent sur la directive de 1995 sur les données personnelles[17], chacun d'entre eux adapte ensuite cette directive à son contexte national.

Toutefois, pour gommer ces disparités au sein de l'Union, la réflexion en cours au sein des instances européennes sur les données personnelles prône le passage du régime de la « Directive » à celui du « Règlement » dit *General Data Protection Regulation* (GDPR) qui s'appliquera de manière identique à l'ensemble des pays européens. Sa finalisation est prévue en 2016 pour une application en 2017 voire 2018.

5.2. Rééquilibrer les responsabilités

Aujourd'hui les contrats *Cloud* s'appuient par défaut sur la Directive de 1995 : L'entreprise définit les règles de sécurité et les impose à son fournisseur, dans une logique d'*outsourcing* ; l'entreprise utilisatrice endosse alors la responsabilité civile et pénale sur les données (en qualité de *Data Controller*), ce qui n'est pas le cas des opérateurs (*Data Processor*). Cette responsabilité des entreprises utilisatrices persiste même si leurs données se retrouvent publiquement accessibles sur internet du fait d'un défaut de sécurité de leur fournisseur de *Cloud*.

Cette situation pourrait se comprendre en partie dans le cas de *Cloud* privés où le prestataire construit le *Cloud* Privé selon les instructions de l'utilisateur/entreprise en lui fournissant son conseil et son expertise. Mais elle est plus difficilement acceptable dans le cadre de *Cloud* publics où l'ensemble des moyens de sécurité sont mis en œuvre par les fournisseurs du *Cloud* sans possibilité de prescription ni de modification de la part de l'entreprise cliente. Il apparaît essentiel que la répartition de la responsabilité soit revue dans le cadre de ce futur règlement et que celle-ci soit dévolue autant à l'auteur des décisions en matière de sécurité qu'à l'entreprise cliente. En effet, l'état actuel de la réglementation a pour effet de détourner en partie les utilisateurs du *Cloud*, il modifie l'équilibre des relations et celui des

[17] Directive 95/46/CE du Parlement européen et du Conseil, 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 : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML

contrats et ne crée pas la motivation nécessaire pour instaurer un niveau de sécurité suffisant. En effet, les fournisseurs ne sont pas incités à accomplir des efforts d'alignement de leur organisation et de leurs contrats dès lors qu'ils n'assument pas de responsabilité, les données des utilisateurs courent un risque et l'entreprise utilisatrice est prise en étau entre ses obligations et l'incapacité de les imposer.

Dans la Directive de 1995, en théorie, la personne physique ou morale, l'autorité publique, le service ou toute autre organisme qui est considéré comme responsable du traitement peut l'être seul ou conjointement avec des tiers (*Joint Controller*). Cette notion de coresponsabilité (*Joint Controller*) ouvre une voie au rééquilibrage entre utilisateurs et opérateurs. Elle sera toujours présente dans le futur Règlement, mais pratiquement il est encore difficile de déterminer dans quel cas elle pourra s'appliquer et si, dans la plupart des situations, l'utilisateur du *Cloud* restera seul *Data Controller* ou si le fournisseur définissant les moyens de sécurité sera qualifié lui aussi de *Data Controller* avec, en corollaire, une responsabilité sur la sécurité et ses conséquences. Or, ce point est très significatif dans la mesure où les amendes pourront s'élever à 5% du CA de l'entreprise.

En attendant ce Règlement, en ce qui concerne les contrats de *Cloud* public et à l'appui de cette notion de *Joint Controller*, il serait donc utile de définir contractuellement les domaines respectifs de responsabilité de l'utilisateur et du fournisseur :

- Soit en utilisant les clauses recommandées par la CNIL dans leur variante de co-responsables de traitement (ex : p.6 du document référencé en bas de page ; note[18]), sachant que ces clauses ne devraient pas être considérées comme optionnelles, car la CNIL souligne bien qu'une entreprise ne devrait pas souscrire de contrat avec un fournisseur refusant de les intégrer (p.11 paragraphes 3 et 4). Toutefois, la CNIL ne dispose pour point d'appui solide que la Directive de 1995 qu'elle a étoffée de ses recommandations, utiles aux entreprises utilisatrices mais difficiles à imposer aux fournisseurs de *Cloud* ; les géants du *Cloud* sont d'une taille plus importante que la plupart de leurs clients et la libre concurrence se révèle souvent insuffisante pour permettre d'infléchir leur position.
- Soit en y ajoutant, par voie d'avenant, les Clauses Contractuelles Types de la Commission Européenne[19] (nommées SCC ou Model Clauses) dans leur version 2004 orientée *Joint Controller*, et non dans celle de 2010 où le client est seul *Data*

[18] Recommandations pour les entreprises qui envisagent de souscrire à des services de *Cloud Computing* : http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_*Cloud*.pdf

[19] *Model Contracts for the transfer of personal data to third coun*tries : http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm

Controller, donc responsable. Il va sans dire que sans pression législative, les fournisseurs refusent en général la version 2004.

5.3. Faire connaître la réglementation applicable

Outre la nécessité de faire évoluer la réglementation pour un rééquilibrage des responsabilités, une vulgarisation de la réglementation d'ores et déjà applicable serait la bienvenue par la diffusion, par exemple, d'une *checklist* recensant les points légaux obligatoires dans les contrats *Cloud*. Il est important de rappeler en effet que :

- Le fournisseur doit inventorier les pays où les données sont susceptibles de se trouver, incluant les pays depuis lesquels un accès aux données peut avoir lieu (ex : cellule support aux Philippines) ;
- Tout nouveau pays doit passer par une notification auprès du client, et par son approbation préalable explicite ;
- Le fournisseur doit fournir la liste de ses sous-traitants et notifier tout nouveau sous-traitant ;
- Les obligations contractuelles du fournisseur doivent se transmettre à tous les sous-traitants (sécurité, responsabilité, confidentialité, réversibilité, protection des données, etc…) ;
- Le droit d'audit doit être prévu (pas seulement la possibilité de recevoir un rapport d'audit d'un auditeur tiers) ;
- Un niveau de sécurité suffisant doit être prévu (ce qui renvoie à la difficulté de définir ce « suffisant » afin de pouvoir le vérifier) ;
- En cas des données positionnées hors (ou accédées en dehors) de l'Union Européenne : les contractants doivent signer les SCC[20] Européennes, ou négocier des BCR[21] ;
- En cas de données positionnées aux (ou accédées depuis les) Etats-Unis : les parties doivent appliquer le *Safe Harbor* (qui semble toujours être valide même s'il a été suspendu par le Parlement Européen), voire comme précédemment signer les SCC, ou des BCR ;
- Cette liste n'est pas exhaustive.

[20] SCC : *Safety Checklists for Contractors*

[21] BCR : *Binding Corporate Rules* / Règles internes d'entreprise

5.4. Bâtir quelques solutions de type « Certifications »

Dans un contrat *Cloud*, pour une entreprise utilisatrice, deux points sont très importants :

- la sécurité technique et organisationnelle,
- et la conformité à la législation.

Sur la sécurité, les clauses européennes types (SCC) qui sont rassemblées dans l'annexe 2 du document cité (cf bas de page[22]) imposent aux utilisateurs de négocier avec les fournisseurs un ensemble de points. Or, comme nous l'avons déjà mentionné, les opérateurs refusent très souvent de négocier au motif que leur *Cloud* est standard et non modifiable par les clients et utilisateurs ; les contrats précisent souvent, en matière de sécurité, que le fournisseur ne fait qu'agir selon les instructions du client telles que décrites dans un paragraphe ou annexe… élaboré par le fournisseur.

Une certification franco-européenne pour garantir un bon niveau de sécurité et la conformité à la législation, afin de limiter les risques pour les européens, apparaîtrait donc comme très utile.

Les entreprises utilisatrices pourraient aussi créer de leur propre initiative un label ou certification « utilisateur » (par exemple dans le cadre de « *Cloud* Confidence[23] » ou du « Label *Cloud*[24] ») qui ne serait octroyé qu'aux fournisseurs incluant ces clauses dans leur contrat.

Ces certifications permettraient par exemple de répondre à des questions simples comme la localisation des données, information parfois très difficile à obtenir et pourtant exigée par la CNIL. Elles permettraient aussi de simplifier de nombreuses procédures et de retrouver une confiance dans le *Cloud*.

La confiance pourrait enfin être fortement restaurée par une certification sur la sécurité avalisée par des organismes de confiance comme l'ANSSI et son équivalent allemand BSI (cf.

[22] DÉCISION DE LA COMMISSION du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil : http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/CCT-2010-Ss_Traitants_VF.pdf

[23] *Cloud* Confidence : http://www.Cloudconfidence.eu/

[24] Label *Cloud* : http://www.label-*Cloud*.com/

par exemple leur initiative Secure *Cloud*[25]). De la même manière une certification sur la conformité apporterait de la confiance si elle était avalisée par la CNIL ou le G29[26] au niveau européen.

5.5. Participer à la réflexion

L'élaboration de textes régissant les obligations des acteurs du *Cloud* et de leurs clients est majoritairement empreinte de l'avis des fournisseurs qui se rendent très disponibles pour agir au sein des instances qui élaborent ces textes. A l'inverse, l'avis des utilisateurs du *Cloud* est moins pris en compte. Cette situation résulte du lobbying intense mis en œuvre par les fournisseurs ; il appartient donc aux entreprises utilisatrices de s'organiser, afin d'agir pour que les dispositions attendues soient construites de manière rigoureuse et équilibrée.

Il est de l'intérêt des entreprises utilisatrices de prendre part à l'élaboration des textes européens sur le *Cloud* et de s'organiser pour le faire en plus grand nombre. Ce point est d'autant plus important que l'on constate une écrasante majorité de fournisseurs non-européens dans les activités européennes du *Cloud* et un rapport de forces déséquilibré notamment entre les Etats-Unis et l'Europe. Du point de vue des membres du groupe de travail du CIGREF, une première mesure pour mieux faire valoir le point de vue des entreprises utilisatrices sur le futur Règlement sur la Protection des Données passerait par l'instauration d'une gouvernance où les fournisseurs et les utilisateurs auraient le même nombre de voix dans les instances où ils sont consultés et ce, quel que soit le nombre de leurs représentants.

Les instances européennes ont entre leurs mains le socle de l'avenir du *Cloud*, qui repose sur la sécurité des données (personnelles ou non) des européens et sur la protection juridique des entreprises européennes.

La Commission Européenne (DG JUSTICE), consciente de ce déséquilibre, a lancé une activité *Safe & Fair Cloud Contracts*[27] qui vise à définir des modèles de contrat. Cette activité cible prioritairement les petites et moyennes entreprises, à des fins de protection. Les résultats de

[25] Appel public à commentaires sur le référentiel d'exigences applicables aux prestataires de services sécurisés d'informatique en nuage : http://www.ssi.gouv.fr/actualite/appel-public-a-commentaires-sur-le-referentiel-dexigences-applicables-aux-prestataires-de-services-securises-dinformatique-en-nuage/

[26] G29 - Groupe européen des autorités de protection : http://www.cnil.fr/linstitution/international/g29/

[27] *Safe and fair model service contracts to boost Cloud Computing* : https://ec.europa.eu/digital-agenda/en/news/safe-and-fair-model-service-contracts-boost-*Cloud*-computing

cette action se font encore attendre, mais dans l'éventualité d'une publication reflétant notamment l'avis des utilisateurs, son intérêt irait au-delà de la cible initiale des PME et ETI.

Dans le cadre de sa stratégie *Cloud*, la Commission Européenne (DG CONNECT) a initié en 2012 quatre activités ayant débouché sur quatre livrables sur les Standards, les Certifications, les SLAs et la Protection des données ; pour ce dernier point un *Code of Conduct*[28] a pour vocation de traiter la problématique de la protection des données. Ce document a été écrit très majoritairement par des fournisseurs, tout comme les trois autres documents à des degrés divers. On y relève quelques reproductions des dispositions de la directive de 1995. Mais la Commission Européenne a souhaité recueillir l'avis des utilisateurs par une consultation : la quasi-totalité des grands groupes européens d'utilisateurs de *Cloud* ainsi consultés ont conclu à une impossibilité d'approuver ces livrables. En conséquence, une future version est envisagée afin d'y inclure davantage le point de vue des entreprises utilisatrices, ce qui permettrait d'obtenir pour elles enfin une avancée européenne concrète.

En tout état de cause, EuroCIO[29]a défini les points suivants qui lui semblent clés dès la contractualisation avec les acteurs du *Cloud*. Ces points peuvent servir de support à une prise de position dans les instances de concertation ou dans les négociations bipartites pour l'établissement des contrats :

[28] *Cloud Select Industry Group on Code of Conduct* : https://ec.europa.eu/digital-agenda/en/*Cloud*-select-industry-group-code-conduct

[29] EuroCIO : http://www.eurocio.org/

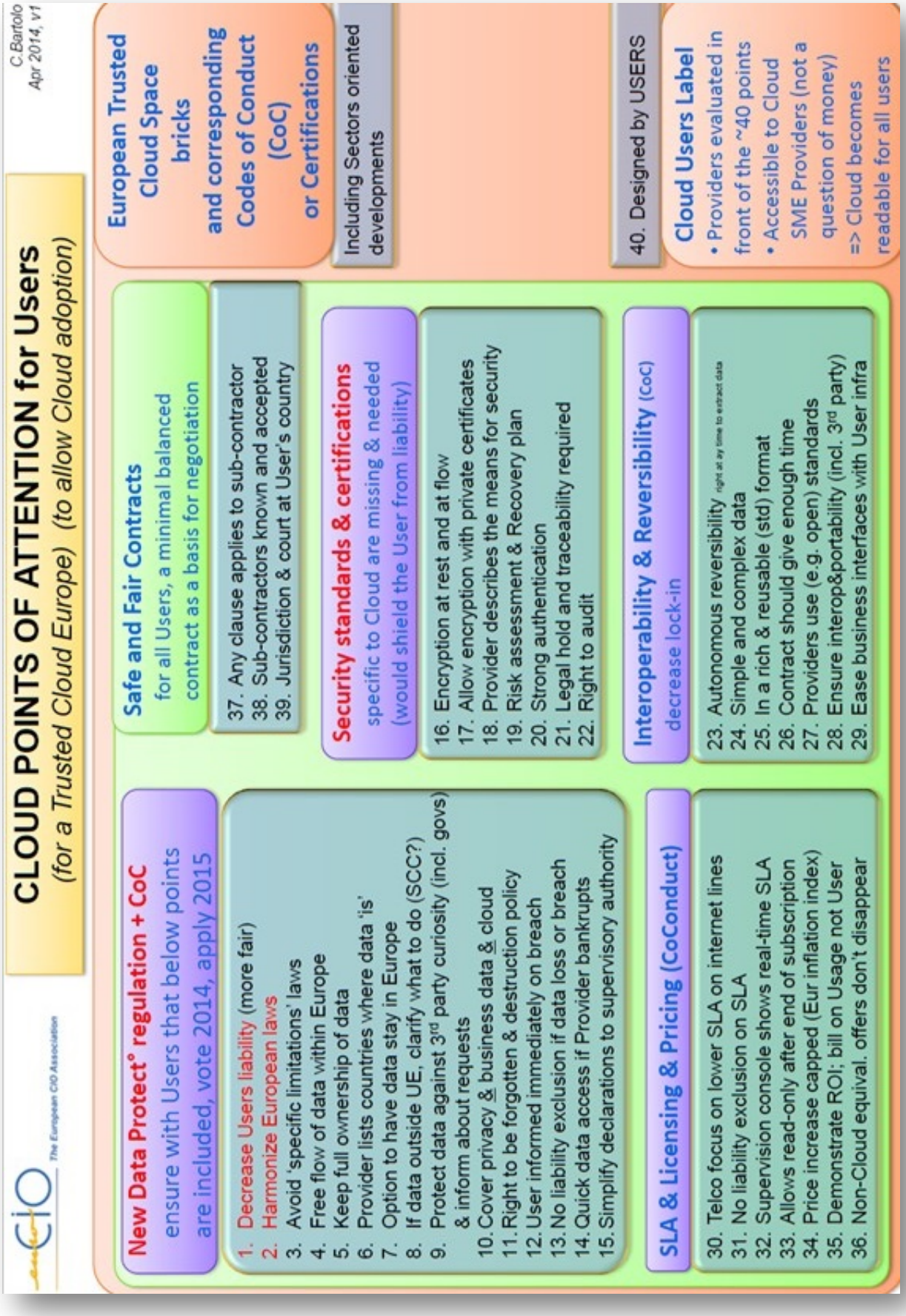

Figure 1 : Points d'attention dans une négociation Cloud et qui contribueraient à plus de confiance dans le Cloud

(Cette liste va au-delà des seuls points réglementaires) – Source EuroCIO

6. EN RESUME

Le *Cloud Computing* fait aujourd'hui partie de la réalité d'une majorité d'entreprises. La pression des marchés, les gains obtenus et promesses d'innovation espérées ont poussé à cette évolution. Mais les expériences sont variées : la disparité et la diversité des *Clouds* et des utilisateurs est telle qu'il est difficile d'en tirer des enseignements généraux.

On peut néanmoins affirmer aujourd'hui que le *Cloud Computing* tire l'ensemble de l'économie numérique :

- Il fait évoluer les infrastructures informatiques des entreprises (virtualisation, réseau, sécurité…) pour permettre les nouveaux usages. Des services innovants se développent chaque jour, générant de nouveaux usages et de nouveaux besoins, notamment autour des terminaux mobiles ;
- La valeur des données s'est révélée aux différents acteurs de l'entreprise (Marketing dans un premier temps, Industriel dans un second). Le *Cloud* facilite la constitution de gisements de données et de traitements massifs nouveaux ;
- Il a amené à développer les réflexions sur la sécurité au-delà du simple cadre technique (en intégrant les dimensions éthique, propriété, géographique, réglementaire, contractuel) ajoutant toutefois à ce jour plus de questions que de solutions ;
- Il fait émerger de nouvelles compétences et métiers ;
- Les modèles d'affaires des entreprises s'en trouvent transformés pour en tirer le meilleur parti sur le long terme.

Le *Cloud* apporte un bouleversement dans les modes de fonctionnement des entreprises ; C'est pourquoi sa mise en œuvre nécessite une conduite du changement et un accompagnement des utilisateurs pour lesquels les DSIs sont attendus.

Par les problématiques qu'il sous-tend (données, innovation, sécurité…) et parce qu'il devient progressivement le socle technologique du numérique (objets connectés, services en ligne, mobilité), il est au centre d'enjeux économiques forts. Il conduit enfin à un affrontement entre deux visions qui doivent maintenant se rapprocher pour un bénéfice mutuel : celle des fournisseurs et celle des utilisateurs.

Car cette lutte entre fournisseurs et utilisateurs érode la confiance et freine l'adoption du *Cloud*. Une réglementation claire, protectrice et équitable pourrait permettre de restaurer cette confiance, de même que des outils comme des certifications ou modèles de contrat créés par les entreprises utilisatrices ou pour elles par des tiers de confiance.

CIGREF

21 avenue de Messine

75008 PARIS

Tel. : +33 1 56 59 70 00

cigref@cigref.fr

www.cigref.fr