EXPANSION CLOUD

La nouvelle donne juridique – Aide ou contrainte ?

Exposé d'Éléonore Varet et Grégoire Dumas
présenté par Laurent Hanaud

« Le Cloud a permis de faire vendre de la ressource informatique comme un service de commodité, au même titre que le gaz, l'eau ou l'électricité. Basée sur un service en ligne fourni par un sous-traitant, la mise en œuvre est simple. A priori, le client n'ayant plus à se préoccuper du fonctionnement de l'informatique, les contraintes géographiques et organisationnelles semblent disparaître. L'utilisateur y gagne en agilité, flexibilité et rapidité.

Toutefois, de par sa configuration, cette nouvelle forme d'infogérance nécessite d'appréhender des risques nouveaux en termes de responsabilité, de protection des données personnelles et de transferts internationaux d'information. Quels sont-ils ? Quelles sont les recommandations pour définir le périmètre contractuel ? Comment encadrer la sécurité dans ce nouvel environnement ?

Pour y répondre, ADELI avait fait venir Maître Varet et Maître Dumas du cabinet Osborne Clarke. À présent, donnons leur la parole !

CLOUD COMPUTING : LES CLÉS POUR SORTIR DU NUAGE

Éléonore Varet ouvrit la session en s'expliquant sur ce titre « les clés pour sortir du nuage ». Ce titre avait été donné, en 2013, à un article antérieur[1]. Tout en tenant compte de l'évolution du marché, avec des offres plus matures, plus diversifiées, et mieux encadrées, il y a toujours cette idée de sortir de la nébuleuse, car le Cloud continue de susciter beaucoup d'interrogations, aussi bien du côté client que du côté fournisseur.
Les clients sont plus portés sur la contractualisation, l'engouement pour le « shadow IT » by-passant la DSI, l'évolution des compétences, la remise en cause des modèles économiques et des politiques d'achat et les difficultés de mise en œuvre des modèles hybrides.
Pour les fournisseurs, les questions de confiance et de transparence des engagements, les modèles économiques et le partage de la valeur, les nouveaux partenariats, la contractualisation et les SLA ainsi que les questions d'interopérabilité et de réversibilité constituent les principaux enjeux.
Sur un plan juridique, toutes ces interrogations se fédèrent autour de deux axes majeurs : les pratiques contractuelles et la protection des données à caractère personnel.

LE CONTRAT DE CLOUD COMPUTING

Cloud, de quoi parle-t-on ? C'est une nouvelle forme de distribution et de consommation de l'informatique. Elle se distingue de l'informatique traditionnelle par le fait qu'elle met à disposition, via Internet et à la demande, un ensemble de ressources et de services mutualisés, dématérialisés, évolutifs et ce sur un mode pay as you go.

[1] *IT Expert magazine - Contrats Cloud : les clés pour sortir du nuage - Eléonore Varet, Mars 2013.*

À cet égard, la définition qu'en donne le NIST[2], est intéressante. Tout en reprenant les caractéristiques telles que la virtualité, la facilité d'accès à la demande, le partage des ressources ; elle met l'accent sur un point important : le minimum d'effort de gestion ou d'interaction avec le fournisseur, concept structurant des contrats de Cloud computing.

Face à l'avènement d'un nouveau modèle

Cela amène une différence fondamentale avec le modèle plus classique d'infogérance. Passer de cet ancien modèle à celui du Cloud, revient à basculer d'une contractualisation lourde nécessitant une gouvernance solide pour coller aux besoins du client, à un système où, de par la multitude d'acteurs, le fournisseur répercute au client ses contraintes sans qu'il puisse, pour autant, décliner à ses sous-traitants les contraintes de son client. On est dans une logique de standardisation adressée au plus grand nombre, où les offres Cloud ne sont généralement pas spécifiquement adaptées aux besoins du client.
Peuvent être livrés différents types de services Cloud ; certains se limitant à la mise à disposition d'une infrastructure seule, mais pouvant s'étendre en plus de l'infrastructure à la prise en charge des plateformes voire du software. De plus, les services Cloud peuvent être livrés sur différents modèles (Cloud privé, Cloud public ou Cloud hybride)[3].

Une fois le décor posé, Éléonore entra dans le vif du sujet : les caractéristiques d'un contrat Cloud.

Comprendre les caractéristiques du contrat Cloud

De manière synthétique, les contrats Cloud sont des contrats souples et évolutifs dans lesquels les engagements de niveaux de service jouent un rôle central. Ce sont le plus souvent des contrats standards, même si cette affirmation doit être nuancée pour les offres de Cloud privés. Quelles en sont les caractéristiques ?

- En premier lieu, les contrats Cloud sont souples et agiles, car les services peuvent être souscrits selon les besoins et des conditions de sortie plus simples. Pour répondre à cette flexibilité, le prestataire doit proposer une durée et des conditions de résiliation, incluant le délai de préavis pour dénoncer le contrat, en phase avec les besoins du client.
- De plus, ils sont évolutifs. Il est possible de souscrire de nouveaux services et de les faire évoluer en même temps que l'évolution des besoins. Néanmoins, sous l'angle juridique, l'évolutivité peut se traduire par un objet indéterminé. Dans les faits, le prestataire se réfère à une notion de « services » sans plus de précision ou prévoit des mécanismes de modifications unilatérales. Afin d'assurer la sécurité des engagements, il faut garder en tête qu'un engagement dont l'objet est indéterminé est nul et que l'engagement dont la réalisation dépend de celui qui s'engage l'est également. Par conséquent, attention à bien lire les engagements du fournisseur dans le contrat.
- Les engagements de service jouent un rôle central. Dans la fourniture de la prestation, le service level agreement ou SLA reflète notamment l'ensemble des contraintes des intervenants qui seront répercutées au client en back-to-back. De ce fait, les contrats Cloud obligent à prendre en compte de nouvelles contraintes opérationnelles et techniques.
- Enfin, ils se caractérisent par une standardisation des offres qui vise à simplifier la contractualisation en présence d'un grand nombre d'utilisateurs. C'est particulièrement le cas pour les offres de Cloud public, avec des contrats d'adhésion au clic.

---

[2] Pour le NIST (National Institute of Standards and Technology), Le Cloud computing « est un modèle informatique qui permet un accès facile et à la demande par le réseau à un ensemble partagé de ressources informatiques configurables (serveurs, stockage, applications et services) qui peuvent être rapidement provisionnées et libérées par un minimum d'efforts de gestion ou d'interaction avec le fournisseur du service »
[3] Pour plus de détails, rappelons que tous ces principes avaient déjà été présentés dans un article de la lettre n°82 intitulé « Cloud Computing, juste du buzz ? ».

Face à cette standardisation, quels réflexes faut-il adopter ? Question d'autant plus importante qu'il appartient au client :

- non seulement d'identifier ses besoins (ce qui est commun à tout contrat) ;
- mais aussi de définir la solution la plus à même d'y répondre, avec les niveaux de service associés.

Et savoir déterminer l'offre la plus pertinente

En conséquence, davantage de contraintes reposent sur les épaules des utilisateurs, obligeant ces derniers à une analyse poussée de leurs exigences pour déterminer en amont l'offre la plus pertinente et ce en anticipant les engagements contractuels. Une grosse partie de l'effort est donc déplacée, en amont, sur le client. L'approche peut se décomposer en trois phases :

- Tout d'abord, l'entreprise cliente doit identifier l'éligibilité au Cloud et le type de Cloud à déployer en fonction de la criticité des applications, de la sensibilité des données, de la sécurité attendue et des responsabilités associées.
- Ensuite elle doit mener une analyse complète de ses besoins en suivant différentes méthodes, telles qu'eBIOS4 ou l'eSCM-CL5. Elle peut également se référer aux différents risques identifiés par la CNIL et par l'ENISA (agence européenne chargée de la sécurité des réseaux et de l'information) pour cerner leurs besoins.
- Enfin, après avoir défini les certifications, labels et autres normes dont le respect est à exiger du prestataire, il lui restera alors à négocier le contrat en ayant pris soin d'identifier les principaux risques et les marges de négociation.

Sur ce dernier point, force est de constater que l'on assiste depuis quelque temps à une prolifération de référentiels. Dans ce domaine, se distinguent deux catégories : les normes ISO et les labels.

À l'heure actuelle, il n'est plus utile de présenter ce qu'est une norme ISO, standard international. Pour le sujet qui nous concerne, nous pouvons citer les suivantes :

- la norme ISO 17788 sur l'organisation du Cloud ;
- la norme ISO 17789 sur l'architecture fonctionnelle ;
- la norme ISO 27018 sur la protection des données personnelles dans le Cloud (surcouche à ISO 27001).

Les labels ont plutôt pour objectif d'apporter une réponse afin de pallier un manque de confiance que certains utilisateurs ont dans le Cloud. Si l'initiative est louable, il est toujours difficile pour l'utilisateur d'identifier et comprendre concrètement son contenu. Par conséquent, le client doit rester très vigilant sur ce point et ne pas hésiter à se renseigner sur la nature du référentiel, sa finalité, les modalités de certification, etc. Parmi tous ces labels peuvent être cités :

- « Cloud confidence » un cadre pour la protection des données d'affaires ;
- « Secure Cloud » label européen du copil de la nouvelle France industrielle ;
- le Référentiel de l'ANSSI[6].

Ajoutons aussi, une publication de la Commission européenne traitant des « lignes directrices en matière de SLAs[7] ». Ce guide a été rédigé par un groupe d'experts[8] en vue d'harmoniser les pratiques et d'aboutir à des engagements plus clairs et plus complets.

À présent penchons-nous sur le contrat Cloud et ses clauses.

---

[4] Expression des Besoins et Identification des Objectifs de Sécurité. Porte sur gestion des risques SSI. A été créé en 1995 par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) : http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

[5] Voir l'article de la lettre n° 65 intitulé « eSCM-CL L'engagement client renforcé ».

[6] Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (Cloud computing) - référentiel d'exigences - Version 1.3 du 30/07/2014 : http://www.ssi.gouv.fr/uploads/IMG/pdf/cloud_referentiel_exigences_anssi.pdf

[7] Publié en Juin 2014 sous l'intitulé « Cloud Service Level Agreement Standardisation Guidelines ».

[8] Ils représentent les principaux acteurs du marché. La liste est jointe dans le guide

En traitant les clauses fondamentales du contrat Cloud

La première clause qui vient à l'esprit est la clause d'objet. Elle définit les services fournis et le référentiel contractuel, c'est-à-dire les documents ayant valeur contractuelle. Les services doivent être définis avec précision afin que les parties puissent s'engager sur des documents contractuels clairs et exhaustifs et permettre que l'ensemble des documents soit librement accepté et opposable. Or une pratique se répand de plus en plus, et plus particulièrement dans les souscriptions en ligne, consistant à mettre en place des renvois par des liens hypertextes et des annexes aboutissant à un ensemble assez flou. Il est recommandé au client d'exiger à ce que tous les documents contractuels soient communiqués avant l'acceptation du contrat. Ajoutons à cela que doit être :

- établie la liste des documents entrant dans le champ contractuel ;
- stipulé l'ordre de prévalence des documents contractuels en cas de contradiction ;
- définie avec précision l'obligation à la charge de chacune des parties. Les caractéristiques du service doivent également être précisées.

Deuxième clause importante, la clause limitative de responsabilité. Dans le contrat Cloud, certains fournisseurs sont plus ou moins enclins à se décharger de toute responsabilité. Pour ce faire, ils peuvent avoir recours à différents moyens. L'exemple classique est un contrat avec un plafond trop bas, librement accepté, qui ne permet pas de couvrir les dommages résultant d'une perte de données stratégiques, le contrat prévoyant que le client est seul responsable des sauvegardes de données. Inutile de dire que les négociations butent souvent sur cette clause. Pour bien négocier, il appartient à chacune des parties, d'éviter de s'appuyer sur des propositions de principe, mais de bien identifier au préalable où se situent les risques pour pouvoir les chiffrer. Reste ensuite, à proportionner la responsabilité du fournisseur aux risques pour l'entreprise. Toute clause limitative ou exclusive de responsabilité n'est valable que si notamment :

- le montant de plafond négocié est suffisant pour contraindre le fournisseur à s'exécuter ;
- la limitation de responsabilité est un juste reflet de la répartition des risques entre parties ;
- le contrat prévoit des contreparties à la limitation et reflète l'équilibre entre les droits et obligations réciproques des parties.

Pour conclure ce point, il est important de rappeler que se focaliser sur la clause de responsabilité ne fait pas tout, il faut aussi penser et faire attention à l'ensemble des mécanismes de garantie, aux indemnités ou au « Service Level Agreement » ; ce dernier, avec les pénalités qui en découlent, pouvant être considéré comme étant un dispositif incitant le fournisseur à respecter ses engagements.

Ce qui nous amène tout naturellement à la troisième clause celle du « Service Level Agreement », ou SLA. Étant un élément clé des contrats Cloud, il est nécessaire d'y accorder une grande attention. Doivent être clairement définis :

- chaque service et les niveaux de service associés ;
- les méthodes de calcul et moyens de mesurer les niveaux de service ;
- le périmètre de responsabilité associé et les modalités d'application des mécanismes de sanction du non-respect des niveaux de service ;
- les sanctions du non-respect des niveaux de service.

Il ne suffit pas de déclarer 99,9% de disponibilité. Il importe de spécifier la période, la prise en compte ou pas de la maintenance, la nature de l'indisponibilité (simple dégradation ou impossibilité d'accès), les conditions (avec ou sans délai), les modalités de pénalités (cumulable, plafonnée, libératoire, automatique), etc. Détail et transparence sont les maîtres mots pour savoir quoi attendre du contrat.

Autre clause sensible pour le contrat, celle de la réversibilité. Cette clause est primordiale pour pouvoir changer de prestataire et faire jouer la concurrence tout en assurant la continuité des services durant le transfert. Il importe de gérer la sortie du contrat sans accroc et de récupérer intégralement les données.

Toute opération de réversibilité doit couvrir :

- les facteurs déclencheurs de la réversibilité ;
- les conditions de réversibilité (restitution des données, formats, modalités de collaboration, volume des transferts, niveaux de service applicables) ;
- les modalités financières ;
- la durée de la réversibilité.

Il est à noter que la jurisprudence a déjà dû se prononcer sur la réversibilité le 30 novembre 2012 dans une affaire opposant l'UMP à Oracle. En l'espèce, le TGI[9] de Nanterre a condamné le prestataire (Oracle) à garantir à son client (UMP) l'exportation des données hébergées dans des délais compatibles avec leur reprise par un nouveau prestataire ; Oracle ne prévoyant initialement qu'un délai de soixante jours à compter de la résiliation du contrat pour que l'utilisateur puisse accéder au service et récupère son fichier de données.

La clause des conditions financières doit être bien définie dans l'élaboration d'un contrat Cloud. En effet, on présente toujours le Cloud comme une solution avantageuse permettant de passer d'un modèle Capex à un modèle Opex avec pour avantages :

- de réduire, d'une part, les investissements du fait de la mutualisation des ressources
- et obtenir d'autre part, plus de souplesse pour suivre l'évolution des besoins des utilisateurs et éviter toute rupture technologique.

Ceci n'est pas faux. Cependant, cela n'exclut pas le fait de bien définir le mode de calcul du prix et de suivre son évolution par la mise en place d'outils adaptés. Les pénalités doivent pouvoir s'appliquer automatiquement. La maîtrise des coûts étant difficile, le client devrait pouvoir vérifier et contester les bases de facturation, par des mécanismes d'audit et d'escalade. Pour piloter son budget, le client pourra privilégier les offres dont le prix comprend des éléments fixes.

La clause de droit applicable[10] et de juridiction compétente[11] doit être stipulée au contrat, sachant que beaucoup de contrats Cloud sont soumis aux lois américaines ou britanniques. Par conséquent, le client doit être vigilant sur ce point pour éviter toute difficulté d'exécution, notamment en identifiant le lieu de fourniture des prestations, la localisation des data center, etc.[12].

Enfin dernier point, la sécurité du Cloud. L'argument de la sécurité est très souvent cité par les fournisseurs pour encourager les entreprises à basculer du « on-premise » vers le Cloud. Les prestataires assurent ainsi pouvoir offrir plus de sécurité au client que celui-ci ne pourrait s'offrir et ce n'est pas nécessairement faux, sauf que les engagements en matière de sécurité sont parfois les grands absents des contrats Cloud. Les exigences du client doivent être spécifiées dans le contrat par des engagements fermes du fournisseur afin de conserver une maîtrise globale en termes de sécurité. Rappelons que cette maîtrise doit garantir :

- la confidentialité (vis-à-vis des tiers non-autorisés) ;
- l'intégrité des données (ni perte, ni dégradation) ;
- la disponibilité des données et du service rendu (aussi bien en cours qu'en fin de contrat) ;
- la traçabilité des données à des fins probatoires.

Ajoutons, qu'il appartient au client d'agir en amont, en formant à la sécurité, en mettant en place des outils de contrôle d'accès et en n'hésitant pas à revoir sa charte IT pour répondre aux nouvelles fonctionnalités du Cloud.

À présent, laissons place à Grégoire Dumas sur la protection des données à caractère personnel très souvent la première question à laquelle on s'attache lorsqu'on parle de Cloud.

---

[9] Tribunal de Grande Instance
[10] Règlement 2001/44/CE = celle de l'État membre dans lequel le demandeur a son domicile.
[11] Règlement n°593/2008 du 17 juin 2008 dit Rome 1: "Le contrat de prestation de services est régi par la loi du pays dans lequel le prestataire de services à sa résidence habituelle"
[12] Siège social, établissement principal ou établissement qui fournit la prestation par exemple.

LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Effectivement, des risques existent quant au traitement de données personnelles dans le Cloud. Citons :

- la Perte des données ;
- le piratage et vol de données ;
- la dépendance technologique (« kidnapping » des données par le prestataire Cloud) ;
- l'utilisation des données par le prestataire Cloud ;
- l'indisponibilité du service rendant tout accès aux données impossible.

Prendre la pleine mesure du cadre juridique

Il existe en France un cadre juridique. Dans ce domaine, la France a même été précurseur en adoptant la loi du 6 janvier 1978 dite loi Informatique et libertés : première loi européenne sur les données à caractère personnel. Elle fut suivie à l'échelle européenne par la directive du 24 octobre 1995 sur la protection des personnes physiques à l'égard de traitements de données à caractère personnel et à la libre circulation des données. L'application de la loi Informatique et libertés est supervisée par la CNIL[13].
Cette loi stipule dans son article 2 son champ d'application :

> *« s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers ». Pour compléter elle spécifie la donnée à caractère personnel comme étant « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».*

La définition est donc très large. Par conséquent, un matricule, un nom, une adresse postale, l'âge, une adresse IP, un identifiant mac, sont considérés comme étant des données à caractère personnel.
À l'article 5, elle stipule aussi que :

> *« sont soumis à la présente loi les traitements de données à caractère personnel :*
> *1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;*
> *2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français.. »*

Qu'est-ce qu'une donnée à caractère personnel ? Les données anonymisées n'en sont pas si aucune identification n'est possible par croisement de données. Et qu'est-ce qu'un traitement ? La réglementation s'appliquant aux « traitements de données à caractère personnel », l'article 2 de la loi définit le traitement de façon très large comme étant :

> *« toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction. »*

[13] http://www.cnil.fr/linstitution/qui-sommes-nous/ Commission nationale de l'informatique et des libertés, qui est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie *privée, ni aux libertés individuelles ou publiques.*

En s'attachant à la notion de responsabilité

La notion de traitement étant définie, qu'en est-il des responsabilités liées aux traitements ? Est considérée comme responsable, l'entité qui détermine les finalités et les moyens du traitement. La finalité indique la raison pour laquelle le traitement est effectué, les moyens expriment le comment. Par opposition, le sous-traitant n'est que l'entité pour le compte duquel sont traitées les données. Dans la plupart des contrats Cloud, le client est considéré comme responsable du traitement et le prestataire comme sous-traitant. La loi s'applique au responsable du traitement et exige du sous-traitant d'assurer la mise en œuvre des mesures de sécurité. Dans tous les cas le sous-traitant agit sur instruction du responsable des traitements. Cependant dans le cadre d'offres standardisées, telles que les applications SaaS notamment, le client n'est pas toujours en mesure de donner les instructions, ni de déterminer les moyens et finalités. En conséquence de quoi, il est bon de se poser la question : client et prestataire ne sont-ils pas tous deux responsables du traitement ? L'analyse se fera alors au cas par cas en fonction de différents indices, tels que :

- la transparence, spécifiant au nom de qui agit le prestataire ;
- le niveau d'instruction, donné par le client indiquant la marge de manœuvre accordée au prestataire ;
- le degré de contrôle du client sur la prestation du sous-traitant et les données utilisées ;
- l'expertise du prestataire permettant d'évaluer son aptitude à la décision.

Le responsable de traitement a un devoir général de sécurité, même en cas de sous-traitance (article 344 et 35 de la loi). Plus précisément, il devra s'assurer que :

- l'utilisation des données est licite et légitime ;
- la durée de conservation des données est limitée et raisonnable ;
- la coopération du prestataire avec les autorités compétentes est stipulée ;
- le respect du droit d'accès, d'opposition, de modification et de suppression de leurs données personnelles par les utilisateurs est effectif ;
- l'intégrité des données est préservée ;
- les règles en matière de transferts internationaux sont respectées.

Sans oublier la localisation des données, élément central

Autre élément important du Cloud, la localisation des données. Ce point a pris de l'importance suite à l'adoption du « Patriot Act » aux États-Unis, puis avec l'affaire Snowden. Il faut dire que cela peut devenir un sujet sensible pour le client. Normalement, les transferts internationaux de données personnelles ne se font en principe que sur des champs d'applications réduits, tel que l'espionnage ou le terrorisme, et ce à travers des procédures judiciaires établies. Ainsi, même si le « Patriot Act » autorise les autorités américaines à procéder à des contrôles sur les serveurs basés aux États-Unis, cela n'a pas empêché à Microsoft de s'opposer à la justice américaine qui demandait la communication d'e-mails d'un citoyen européen stockés sur un serveur localisé en Irlande. Par principe, le transfert des données à caractère personnel hors UE est interdit. Néanmoins il existe des exceptions. Ainsi :

- la commission européenne peut reconnaître le niveau de sécurité du pays de destination suffisant ;
- il est possible de transférer les données en faisant signer un contrat appliquant des Clauses Contractuelles Types de la Commission Européenne[14] ;
- Au sein d'un même groupe, tout transfert peut s'opérer sur la base de règles internes d'entreprise appelées BCR[15]. Ces règles définissent la politique du groupe en matière de transferts de données. Elles peuvent ainsi proposer une protection adéquate aux données transférées depuis l'Union européenne vers des pays tiers.

---

[14] Retrouvez les modèles de Clauses Contractuelles, sur le site de la CNIL.

[15] Binding Corporate Rules : La CNIL en présente le principe. Y sont archivés tous les outils nécessaires à leur bon fonctionnement Instructions, grilles d'analyse, checklist etc… La procédure de mise en œuvre est assez longue.

- L'adhésion au « Safe Harbor » permettait les transferts vers les États-Unis, sous certaines conditions. Mais par décision de la Cour de Justice de l'Union Européenne, ce dispositif a été invalidé le 6 octobre 2015.
- Enfin, il existe des exceptions[16] au principe d'interdiction de transfert, toutefois d'interprétation restrictive. Elles sont prévues par la directive 95/46 Ce du 24 octobre 1995, et à l'article 69 de la loi Informatique et Libertés.

Ainsi que certaines règles spécifiques, lorsque le contexte l'impose

Certains secteurs ont des règles spécifiques. Le premier d'entre eux est le secteur bancaire. L'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises[17] du secteur de la banque impose des exigences à tout établissement financier faisant appel à un prestataire Cloud. Ainsi, chaque organisme concerné doit s'assurer :

- du libre accès des données aux autorités prudentielles ;
- qu'un contrat est bien conclu entre le prestataire et le client ;
- de l'existence des plans de secours, des SLAs ;
- de la prise en compte des risques. Etc.

Autre secteur important : celui des données de santé. Vu la sensibilité de cette catégorie de données, inutile de dire que leur hébergement est strictement réglementé, et ce depuis la loi du 4 mars 2002. Dans l'esprit de cette dernière[18],

> *« la volonté des pouvoirs publics est d'organiser le dépôt et la conservation des données de santé dans des conditions de nature à garantir leur pérennité et leur confidentialité, de les mettre à la disposition des personnes autorisées selon des modalités définies par contrat, et de les restituer en fin de contrat ».*

Entre autres, de par cette loi :

- le stockage des données est réservé aux hébergeurs agréés par le Ministère de la santé qui répond juridiquement de la conformité de l'opération globale d'hébergement. Les conditions d'agrément des hébergeurs sont fixées par décret[19]. L'agrément est délivré par le ministre chargé de la santé, après avis motivé d'un comité d'agrément et de la CNIL.
- Le contrat de Cloud doit satisfaire aux exigences de ce décret.
- L'hébergeur doit remettre au Ministre des Affaires sociales et de la santé un rapport annuel d'évaluation et demander le renouvellement de son agrément tous les trois ans.

Rien ne s'oppose à ce que les données soient hébergées à l'étranger, sous réserve du respect du cadre rappelé ci-avant.

Quant aux évolutions à venir…

Enfin, pour terminer, l'évolution législative et réglementaire. Un projet de règlement révisant la directive 95/46/CE, devrait être adopté par les États membres de l'Union Européenne début 2016. Sa finalité est de pallier l'harmonisation insuffisante des réglementations nationales en la matière. En l'état, les sociétés tant européennes qu'étrangères sont contraintes de traiter avec les autorités de chacun des 28 États membres. Ainsi, la mise en place d'un guichet unique permettra de soumettre à l'autorité de l'État du principal établissement de l'entreprise, les traitements impliquant des transferts internationaux de données[20]. De plus, la collecte des données à caractère personnel et les déclarations s'en trouveront allégées et simplifiées.

---

[16] *Présentées sur le site de la CNIL.*
[17] *Pour plus de détail, se reporter au site de l'Autorité de Contrôle Prudentiel – ACPR.*
[18] *Tel que défini par l'agence des systèmes d'information partagés de santé – ASIP.*
[19] *Décret n°2006-6 du 4 janvier 2006.*
[20] Appelé aussi le « one stop shop approach ».

QUESTIONS-RÉPONSES

Au cours de la présentation, un échange put s'établir entre Maître Varet (EV) Maître Dumas (GD) et l'assistance (Ass). En voici les principales remarques :

Assistance *: La pauvre PME peut-elle négocier un contrat sans juriste ?*

Maître Varet : La première question à se poser est le poids des partenaires et déterminer où se situe le point d'équilibre. Certes, on pense le plus souvent aux grands acteurs du marché. Mais il existe aussi un grand nombre d'intervenants plus petits. Il est clair qu'il sera plus difficile à la pauvre PME de négocier avec les grands acteurs du fait de la rigidité de leur politique contractuelle. Ceci dit, il est toujours possible de trouver des marges de négociation et de concilier les intérêts de chacun.

Ass *: Quand on évoque la clause de responsabilité ainsi que les mécanismes permettant au fournisseur de respecter ses engagements, est-on dans une obligation de moyens ou de résultat ?*

E V : Il faut reconnaître que la jurisprudence est parfois peu cohérente sur ce point. Dans les faits, tout repose sur le contenu du contrat. Il est rare de voir un fournisseur accepter une obligation de résultat générale. Dans les contrats Cloud, le principal engagement est le « Service Level Agreement », le plus important étant la précision des indicateurs, les méthodes de calcul et l'encadrement des pénalités. Cette question d'obligation de moyens ou de résultats crispe trop souvent la relation client fournisseur sur un sujet qui n'est pas nécessairement le facteur clé de réussite d'un projet. De bons mécanismes de gouvernance ou d'arbitrage, intégrant l'évolution des besoins, dans une démarche collaborative apporteront souvent de biens meilleurs résultats sur la livraison du service. Se focaliser sur les moyens d'aboutir au résultat, davantage que sur la sanction, est une bonne pratique. La démarche consistant à externaliser le problème uniquement sur le fournisseur est une approche qui fonctionne mal.

Ass *: La sécurité n'est-elle pas le talon d'Achille du Cloud ?*

E V : Structurellement, le fait de mutualiser les ressources et de virtualiser peut engendrer une perte de contrôle des éléments externalisés. Cependant, en interne le client doit mettre en place de bonnes pratiques. Pour ce faire, il importe que les parties concernées (DSI, achats, juridique et autre départements impliqués) puissent travailler ensemble sur le projet, afin de fédérer les compétences ; règle n°1 de bonne gouvernance sur le sujet. Et il faut faire preuve de vigilance en surveillant des engagements correctement établis.

Ass *: Les données à caractère personnel étrangères peuvent-elles être hébergées au sein de l'UE ?*

Maître Dumas : Oui absolument, le transfert est alors libre pour l'importateur auquel s'applique alors la législation précitée. Les garanties qui en découlent peuvent être valorisées. C'est une valeur exportable.

Ass *: On a parlé plusieurs fois de transfert, et une seule fois d'accès ; comment expliquer ce déséquilibre ?*

G D : Tout accès depuis un autre pays est considéré comme un transfert international en application de la loi Informatique et Libertés. Pour certains traitements, la CNIL peut être consultée dans le cadre de processus législatifs. D'autre part, selon le cas de figure, il faut se poser la question du régime déclaratif ; déclaration unique, normale ou simplifiée. En matière de données à caractère personnel, pour identifier les transferts, devrait être établi un document cartographiant les flux Où vont les données ? Cela devrait guider à la mise en place des bons outils.

LE MOT DE LA FIN

Voilà un sujet que l'on n'a pas l'habitude de traiter au sein d'Adeli. Ce fut une première.

- Concernant les contrats, la revue des caractéristiques et des clauses a été très enrichissante. Cela a apporté un éclairage nouveau et moins technique.
- Quant aux données à caractère personnel, ce fut une ouverture pour chacun d'entre nous en termes de notion de traitement et de définition des responsabilités associées.

Un grand merci à Éléonore et à Grégoire, pour cet éclairage et pour l'apport de leur expérience. Ce fut pour nous très instructif.

Rédigé par Laurent Hanaud
Laurent.hanaud@adeli.org / http://www.laurent-hanaud.fr/

Conférence animée par :
Eléonore Varet / Eleonore.Varet@osborneclarke.com
Gregoire Dumas / Gregoire.Dumas@osborneclarke.com
http://www.osborneclarke.com/international/country/france/

RÉFÉRENCES

Organismes

- CNIL - http://www.cnil.fr/linstitution/qui-sommes-nous/
- ANSII - http://www.ssi.gouv.fr/
- NIST - http://www.nist.gov/
- ACPR - https://acpr.banque-france.fr/accueil.html
- ASIPSanté - http://esante.gouv.fr/
- Commission européenne - http://ec.europa.eu/index_fr.htm

Publications

- IT Expert Magazine : « Contrats Cloud : les clés pour sortir du nuage » Éléonore Varet - Mars 2013.
- Lettre Adeli n°82 : « Cloud Computing, juste du buzz ? » Martine Otter – janvier 2011.
- ANSSI : « Expression des Besoins et Identification des Objectifs de Sécurité. Porte sur gestion des risques SSI ». 2004 – 2010.
- Lettre Adeli n° 65 intitulé « eSCM-CL L'engagement client renforcé » Laurent Hanaud – novembre 2006.
- ANSSI : « Référentiel de qualification de prestataires de services sécurisés d'informatique en nuage (Cloud computing) - référentiel d'exigences » - Version 1.3 du 30 juillet 2014
- Commission européenne : Cloud Service Level Agreement Standardisation Guidelines - juin 2014.