ceis

Anticiper les risques et adopter le *Cloud computing* en toute sérénité

Cindy Roth

Mai 2015

En partenariat avec

ATiPiC AVOCAT
Technologies - Informations - Propriété Intellectuelle - Communication

Business Digital Security
Secure & Accelerate Your Business

Les notes σtratégiques

CEIS est une société de conseil en stratégie et en management des risques. Notre vocation est d'assister nos clients dans leur développement en France et à l'international et de contribuer à la protection de leurs intérêts. Pour cela, nous associons systématiquement vision prospective et approche opérationnelle, maîtrise des informations utiles à la décision et accompagnement dans l'action. CEIS intervient notamment dans le domaine de la confiance numérique et, à ce titre, est l'un des membres fondateurs de l'association Cloud Confidence. Réunissant une quinzaine d'acteurs du Cloud, offreurs (SaaS, IaaS, PaaS…), utilisateurs et membres de l'écosystème, cette association a pour objectif d'accélérer l'usage du Cloud, au service de l'économie et de ses clients.

Ce livre blanc a été écrit en collaboration avec ATIPIC Avocat et Business Digital Security (https://business-digital-security.com)

- Business Digital Security est un cabinet de conseil en stratégie intervenant dans les domaines de la cybersécurité, du numérique, et plus largement des technologies de l'information. Partenaire de confiance, Business Digital Security a pour mission d'accompagner ses clients à créer de la valeur business à l'aide du digital et d'éviter d'en détruire grâce à la cybersécurité, et de faciliter les relations entre les utilisateurs finaux et les fournisseurs.

- ATIPIC Avocat est une société d'avocat dédiée au droit lié aux nouvelles technologies dans toutes ses composantes (Technologies, Informations, Propriété Intellectuelle, Communication). Nous allions l'analyse juridique la plus rigoureuse à la compréhension profonde du fonctionnement technique et à l'expérience du monde de l'entreprise : nous proposons ainsi des solutions juridiques pragmatiques et opérationnelles, prenant en compte l'ensemble des impératifs existants.

« *Discontinued products and services are nothing new, of course, but what is new with the coming of the Cloud is the discontinuation of services to which people have entrusted a lot of personal or otherwise important data – and in many cases devoted a lot of time to creating and organizing that data. As businesses ratchet up their use of Cloud services, they're going to struggle with similar problems, sometimes on a much greater scale. I don't see any way around this – it's the price we pay for the convenience of centralized apps and databases – but it's worth keeping in mind that in the Cloud we're all guinea pigs, and that means we're all dispensable. Caveat Cloudster* »[1]

NICK CARR, auteur de Does IT Matter?, The Big Switch et The Shallows

« *We believe we're moving out of the Ice Age, the Iron Age, the Industrial Age, the Information Age, to the participation age. You get on the Net and you do stuff. You IM (instant message), you blog, you take pictures, you publish, you podcast, you transact, you distance learn, you telemedicine. You are participating on the Internet, not just viewing stuff. We build the infrastructure that goes in the data center that facilitates the participation age. We build that big friggin' Webtone switch. It has security, directory, identity, privacy, storage, compute, the whole Web services stack* ».

SCOTT MACNEALY, ex PDG de SUN MICROSYSTEMS

[1] *The Cloud giveth and the Cloud taketh away*, 23 novembre 2011 : http://www.roughtype.com/?p=1553 (consulté le 30 avril 2015).

Sommaire

Préface

Que vous l'utilisiez sans vraiment savoir de quoi il s'agit, que vos collaborateurs l'aient adopté sans que vous n'en ayez été informé, votre entreprise fait peut-être partie des 30% de sociétés qui ont recours à des services de *Cloud computing*.

Le concept de *Cloud computing* continue de prendre de l'ampleur. A cet effet, le livre blanc a pour objectif de donner au client tous les éléments essentiels pour une adoption raisonnée et à risque maîtrisé d'une offre de service *Cloud*. Le but est de fournir au client un outil puissant de pilotage, de *reporting* et de communication des risques majeurs auprès de la Direction générale, de la Direction des Risques/Conformité, des Directions métiers et de l'Audit/Contrôle interne. Le livre blanc s'inscrit dans une démarche visant à doter le client d'une connaissance fine et en continu de son environnement *Cloud* et de ses fournisseurs stratégiques.

Introduction

Le *Cloud computing* ou l'informatique en nuage se définit au sens du Vocabulaire de l'informatique et de l'internet comme « *un mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire* »[2]. Le terme d'informatique en nuage n'a pas été choisi au hasard et crée dans l'esprit du client l'idée que ses données sont virtuellement stockées partout et nulle part en même temps. La légèreté et la simplicité de fonctionnement que sous-entend implicitement l'image n'est qu'apparente : en réalité, même s'il n'en perçoit pas immédiatement tous les arcanes, le client doit faire face à un mécanisme complexe qui comprend différents niveaux de services (IaaS, SaaS, PaaS). Le *software as a service (SaaS)*, le mode d'exploitation commerciale des logiciels le plus couramment utilisé par les entreprises existait bien avant l'émergence du *Cloud computing*.

Avec les offres *Cloud*, le client recherche également l'argument d'un fonctionnement global, aux performances uniformisées indépendamment du pays de connexion. Toutefois, cela implique souvent que les données soient stockées dans des datacenters situés dans différents pays sur différents continents. Le client doit être conscient, avant de souscrire une offre *Cloud*, que ses données peuvent être stockées en Chine, aux Etats-Unis ou en Corée du Sud. Il est donc primordial de mener des investigations sur le prestataire pour que le client ait toutes les clés en main, et soit en mesure de connaître les législations étrangères qui sont susceptibles de s'appliquer.

Il nous a semblé que le plan que nous allons vous proposer permettait d'appréhender les différentes facettes du *Cloud* et de présenter les solutions pouvant être apportées afin de diminuer les risques et de permettre à l'entreprise de maximiser les opportunités offertes. Ainsi, même si la présentation des problématiques est opérée sous une forme parfois linéaire, c'est en gardant toujours à l'esprit que la plupart d'entre elles sont intrinsèquement liées. De même qu'il nous a paru plus pertinent d'effectuer un classement des risques selon leurs impacts pour le client.

Différentes catégories de risques intrinsèques au fournisseur et à son service peuvent être distinguées, qu'il s'agira d'apprécier et de surveiller tout au long de la vie de l'abonnement au service, et de mettre en perspective avec les enjeux métier et l'organisation du client.

---

[2] J.O. du 6 juin 2010, p. 10453 : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022309303 (consulté le 9 mars 2015).

Celui-ci connaît-il les lieux d'hébergement de ses données ? Est-il informé des incidents qui surviennent ? Peut-il effectuer des audits ? Comment les données qu'il détient (qui lui appartiennent en propre ou qui appartiennent à ses propres clients) sont-elles traitées, ou transférées ? D'un service à un autre ? Peut-il les récupérer ? S'assurer de leur effacement ? Quels éléments de traçabilité a-t-il à sa disposition ? Comment s'organise la fin de contrat ? Le client est-il en situation de dépendance technologique ? La maîtrise de ses données et de ses systèmes d'information impliquent nécessairement qu'il soit conscient des risques de gouvernance qu'il envisage de prendre (I).

Pour que le prestataire puisse gagner la confiance du client, il doit communiquer des informations sur lui-même et son environnement juridique (société-mère, filiales, participations). Cela apparaît d'autant plus nécessaire que le marché des prestations de services *Cloud* a vu naître ces dernières années une foule de nouveaux acteurs, de tailles très variées, sur lesquels filtrent parfois peu d'informations. Plusieurs questions se posent alors concernant la solidité financière du prestataire. Depuis combien d'années la société évolue-t-elle sur le marché ? Quel est l'intérêt du prestataire pour ses activités en France ? Le client peut-il contracter avec elle sans risque qu'elle ne disparaisse à l'avenir ? La société est-elle détenue par une autre société ? Le prestataire est-il propriétaire de ses datacenters ? D'autres questions ont également trait à la réputation du prestataire. A-t-il connu des ennuis financiers nécessitant l'ouverture d'une procédure collective ? Ses dirigeants sont-ils irréprochables ? Autant de risques tenant aux prestataires qu'il conviendra d'analyser (II).

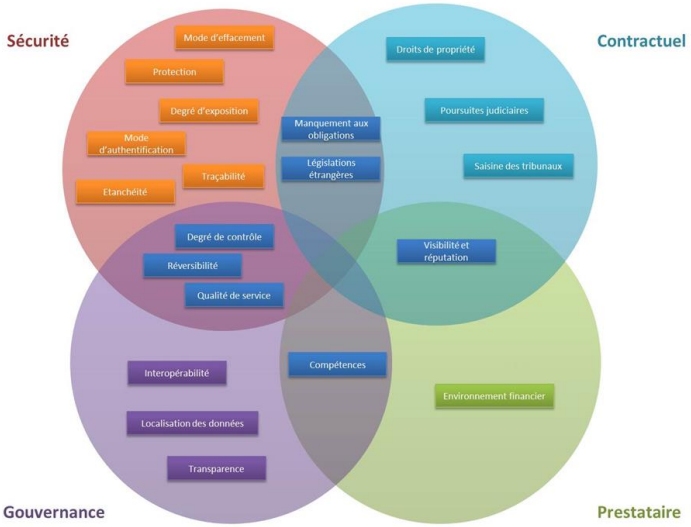
Au niveau juridique et concernant les quelques problématiques qui n'auraient pas déjà été mentionnées et traitées dans la partie ci-dessus, le manque d'information et de prudence peut mettre en danger les droits de propriété du client sur ses données d'autant plus si elle concerne une œuvre, un brevet, un modèle soumis au droit de propriété intellectuelle. En outre, le client risque des poursuites judiciaires s'il ne contrôle pas l'activité de son prestataire. Autant d'éléments qui doivent être prévus contractuellement (III). Les risques juridiques sont également étroitement liés au niveau de sécurisation qui entoure le traitement des données.

Ainsi, en matière de sécurité des systèmes d'information, les enjeux et risques concernent la confidentialité, la disponibilité, l'intégrité et la traçabilité des données (IV). Est-ce que le prestataire propose un mode d'effacement ou de destruction complet des données au terme de la relation contractuelle ? Le personnel et les sous-traitants sont-ils tenus au secret ? Quels sont les moyens mis en œuvre pour lutter contre les risques d'intrusions physiques et logiques ? Les législations étrangères sont-elles applicables ? L'authentification des utilisateurs

de la plate-forme est-elle sécurisée ? Quel niveau de service est proposé par le prestataire ? Existe-t-il des moyens de traçabilité des actions des utilisateurs ?

Autant de risques qu'il serait nécessaire d'analyser avant toute entrée en relation d'affaires et *a fortiori* avant toute relation contractuelle. En effet, avec un peu de vigilance et une bonne négociation de son contrat, le service peut s'avérer bien plus sécurisant qu'une gestion en interne des ressources. Une bonne maîtrise de stratégie passe nécessairement par une analyse des risques. Certaines associations comme Cloud Confidence ont pour objectif de « *garantir la transparence des offres Cloud, maîtriser le risque business et juridique, et promouvoir un espace d'échanges sans porter atteinte aux principes de protection des données personnelles* ».

Une vision globale et régulièrement actualisée n'en est que d'autant plus nécessaire pour appréhender la complexité du *Cloud*, et bénéficier de la simplicité offerte par ses services sans mauvaises surprises.



1. LES RISQUES DE GOUVERNANCE

1.1. Les risques liés à une mauvaise réversibilité des données

Qu'est-ce que la réversibilité des données ? Tous les contrats informatiques comprenant une externalisation des services - le service n'est plus géré en interne par l'entreprise mais par un prestataire tiers - prennent fin à un moment ou à un autre. Le client doit donc pouvoir reprendre de manière totale ou partielle l'environnement informatique qu'il avait confié au prestataire tiers pour orchestrer le transfert vers un autre prestataire. Et ce besoin de réversibilité intervient quelle que soit la cause de la fin de la relation contractuelle : échéance normale, force majeure, choix du client, manquement de l'une ou l'autre des parties.

En matière de *Cloud computing*, il faut prendre conscience de la difficulté d'une réversibilité totale et simplifiée des données. A travers la négociation de la clause contractuelle, le client pourra minimiser les risques et proposer ce qui lui est favorable en termes de format et de délai. En mode SaaS, le rapatriement des données paraît assez simple car standardisé. Cependant, leur intégration depuis une application en mode SaaS vers une application interne peut poser des problèmes. Dans ce cas, le client se trouvera dans une situation de *lock-in* dans laquelle il sera dépendant, technologiquement et commercialement, du prestataire *Cloud* sans pouvoir en changer selon son gré. Et si le contrat doit prendre fin pour une raison ou pour une autre, le risque pour le client est qu'il pourrait soit ne pas récupérer ses données, soit se retrouver avec des données inexploitables.

Ainsi, certaines offres ne garantissent pas toujours la portabilité des données, des applications ou des services. Concrètement, cela signifie que le choix du prestataire de services *Cloud* doit être étudié très attentivement par les différentes directions concernées de l'entreprise. En parallèle, des solutions techniques contournant ce problème se développent. Pour exemple, le logiciel *open source* Docker pourrait permettre de basculer une application - placée dans un container virtuel - entre les plate-formes de service *Cloud* d'Amazon, de Microsoft et de Google[3]. Le client doit tout de même être vigilant : un logiciel *open source* n'offre pas les mêmes garanties en termes de sécurité qu'un logiciel sous licence.

[3] CROCHET-DAMAIS Antoine, Cloud : pourquoi Docker peut tout changer, JDN.net, 13 février 2015 : http://www.journaldunet.com/solutions/Cloud-computing/docker-definition-avantages-inconvenients.shtml (consulté le 27 avril 2015).

Il existe néanmoins des solutions juridiques sur lesquelles s'appuyer. Tout d'abord, une clause contractuelle de réversibilité devra contenir plusieurs éléments pour limiter les risques de perte de données ou de dépendance technologique :

- La durée de la phase de réversibilité va varier en fonction des besoins du client. Si le client stocke ses données dans le *Cloud* depuis plusieurs années, on peut aisément imaginer qu'un délai de 30 jours soit beaucoup trop court. L'ordonnance rendue le 30 novembre 2012 par le TGI de Nanterre, dans l'affaire *UMP c/ Oracle*, a ainsi pu prévoir que le délai, dans cette affaire, ne devait pas être inférieur à 2 mois. Il est également important de prévoir le point de départ de ce délai.

- Le format de restitution est très important à déterminer pour permettre au client d'exploiter ses données après l'échéance du contrat. Un format Microsoft tel que le .csv est souvent proposé au client. Néanmoins, il sera plus favorable pour lui de définir un format de réversibilité qui le satisfait pleinement en fonction de son environnement informatique. La difficulté du transfert des données vers un autre service *Cloud* d'un prestataire tiers est également à prendre en considération.

- Les modalités du calcul des coûts de réversibilité sont à prévoir. En effet, la réversibilité peut être gratuite ou facturée en fonction du tarif en vigueur au moment de la notification de réversibilité.

Ensuite, un plan détaillé de réversibilité annexé au contrat pourra être prévu. Il sera actualisé, complété et/ou modifié à échéance régulière entre les parties.

1.2. Les risques liés à un manque d'interopérabilité

Certains prestataires de services *Cloud* concluent des partenariats avec d'autres prestataires pour permettre l'interopérabilité des services. Pour exemple, le partenariat Microsoft-Salesforce permet aux clients de l'un et de l'autre « *d'accéder, de partager, d'éditer et de collaborer sur du contenu Office depuis Salesforce et sur Salesforce1 en utilisant Office sur mobile, iPad et Office365* »[4]. Pourtant, ce n'est pas toujours le cas : de nombreux prestataires souhaitent imposer leurs standards pour empêcher l'utilisation d'autres plate-formes (PaaS) ou d'avoir

[4] La revue du digital, Microsoft et Salesforce resserrent les liens entre Office365, le CRM et Windows, 30 mai 2014 : http://www.larevuedudigital.com/2014/05/30/microsoft-et-salesforce-resserrent-les-liens-entre-office365-le-crm-et-windows (consulté le 4 mars 2015).

recours à d'autres services (SaaS). Un modèle ouvert de plate-forme est à privilégier, ce qui se traduit par la mise à disposition d'APIs.

Alors que le marché du *Cloud* est appelé à exploser au cours des prochaines années, certains gros acteurs mènent en effet un intense lobbying pour imposer leurs normes. Des discussions sont en cours à l'échelle nationale pour l'élaboration de normes mondiales. Les opinions divergent sur ce point et selon, Olivier Teitgen, chef de projet au département transports, énergie et communication à l'Afnor et secrétaire de la commission de normalisation du *Cloud* en France, « *imposer des normes (…) c'est interférer dans la politique commerciale des fournisseurs* ».

S'ils ne sont pas publiquement disponibles, ces éléments devront être réclamés au prestataire afin de prendre une décision en toute connaissance de cause.

1.3. Les risques liés à un manque de transparence des informations

La transparence du prestataire est un gage de confiance apportée au client. Dans son intérêt, et parce que légalement il y sera de toute façon bientôt obligé, le prestataire de services *Cloud* doit pouvoir notifier au client tout incident, toute tentative d'intrusion dans le système et toute violation de la protection des données personnelles le concernant ou pouvant potentiellement le concerner, ne serait-ce qu'en effet d'image. Cette notification, à laquelle le client risque lui-même d'être astreint en tant que responsable de traitement de données notamment, devra nécessairement être coordonnée entre ces deux acteurs (gestion de crise, communication, etc.).

Pour garantir cette transparence, le client doit être autorisé par le prestataire à effectuer, faire effectuer ou profiter et avoir accès aux résultats des audits, des tests de vulnérabilités et des tests d'intrusion sur les actifs informatiques de ce dernier pour s'assurer du niveau de sécurité global du service, sachant qu'il aura lui-même à répondre de cette sécurité vis-à-vis de ses propres clients.

Cette faculté d'audit technique peut être prévue par le contrat. Le prestataire peut proposer au client la possibilité de contrôler s'il se conforme bien aux référentiels « sécurité » et technique établis. Le contrat doit prévoir plusieurs aspects :

- Les modalités de déclenchement des procédures d'audit doivent être spécifiées. Exemple : notification avec respect d'un préavis, etc. ;

- La fréquence de ces audits (minimum d'un an, etc.) ;

- Les personnes habilitées à conduire les audits doivent être mentionnées. On conseillera un auditeur externe et indépendant aux parties. Dans ce cas, un accord de confidentialité sera nécessaire. Les frais seront à la charge du client.

A noter : selon une analyse de l'Autorité de contrôle prudentiel et de résolution (ACPR) sur le *Cloud computing* publiée en juillet 2013[5] dans le secteur de la banque et des assurances, celle-ci s'est réservée, dans une formule sibylline, toute la latitude nécessaire pour considérer qu'une simple prestation dite de support pouvait être considérée comme une prestation de services essentielle externalisée (PSEE) à partir du moment où elle était opérée dans le *Cloud*. Rappelons que les PSEE désignent les « *prestations de services ou autres tâches opérationnelles essentielles ou importantes* » introduites par le Comité de la Réglementation Bancaire et Financière (CRBF) dans son règlement n° 97-02 remplacé par l'arrêté du 3 novembre 2014, imposant des contraintes toutes particulières aux établissements financiers (clauses spécifiques, droit d'audit de l'ACPR, etc.). Une potentielle pression règlementaire forte donc, expliquant et nécessitant en pratique que les banques soient en droit d'imposer aux prestataires de services *Cloud* des garanties à la hauteur de leurs obligations[6].

Enfin, des exemples tels que celui de l'affaire *Code Spaces* de 2014 montrent à l'inverse qu'il ne suffit pas de s'appuyer sur une offre permettant la mise en place de solutions de sécurité élaborées, encore faut-il que le client les active et les respecte lui-même, sauf à mettre en cause sa responsabilité vis-à-vis de ses propres clients en jeu ou son existence même. Dans cette affaire, le défaut de sécurisation des moyens d'authentification de cette société d'hébergement de codes sources a conduit au piratage de son compte sur la plate-forme de *Cloud* Amazon Web Services qu'elle utilisait. Le pirate a pu, lors de la lutte pour la reprise du contrôle du compte *Cloud*, détruire les fichiers stockés. Cela a causé la fermeture de la société en 2014 sans que les clients finaux aient pu récupérer leurs données.

---

[5] ACP, Analyses et Synthèses, Les risques associés au *Cloud computing*, n°16, juillet 2013 : http://www.acp.banque-france.fr/uploads/media/201307-Risques-associes-au-Cloud-computing_01.pdf (consulté le 1er avril 2015).

[6] COUPEZ François, *Pour l'ACPR, prestations dans le Cloud = externalisation de prestations de services essentielles (PSEE),* Blog ATIPIC avocats, 25 septembre 2014 : http://blogatipic-avocat.com/retour-vers-le-futur-1-juillet-2013-lacpr-et-le-Cloud-computing (consulté le 10 mars 2015).

1.4. Les risques liés à un manque d'informations sur la localisation des données

Pour conserver le contrôle de ses systèmes et informations, et répondre aux obligations existantes en matière de protection des données à caractère personnel qu'il peut être amené à traiter, le client doit connaître les lieux d'implantation des datacenters. Cependant, la localisation des données est souvent complexe à établir avec précision car les données peuvent être déplacées très rapidement d'un continent à un autre. Certains offreurs choisissent la carte de la transparence et dévoilent la localisation de leurs datacenters, en tout cas le pays d'implantation. Ajoutons que certains prestataires, notamment de services SaaS, plus petits, peuvent également louer leurs datacenters, compliquant la tâche de reconstitution de la « chaîne de transmission » des données.

2. LES RISQUES PRESTATAIRES

Alors que le marché du *Cloud* en France devrait poursuivre sa croissance à deux chiffres pour 2015 (21% selon le cabinet Xerfi, contre 20% en 2014), la tendance est au recours croissant par les grands groupes du CAC 40 à des offres localisées émanant des PME, soucieuses d'assurer la sécurité de leurs données dans le contexte des révélations de l'affaire PRISM, en traitant avec des pépites françaises et en souscrivant des offres « localisées ». Salesforce, IBM, Microsoft et SAP ont ainsi annoncé l'ouverture de datacenters dans l'Hexagone d'ici la fin de l'année.

A l'heure actuelle, on retrouve des prestataires français dans tous les secteurs (IaaS, PaaS et SaaS) même si les fournisseurs américains dominent largement les deux premiers. La France abrite de nombreuses sociétés sur le segment des éditeurs SaaS, pour la plupart des *« niche players »*. Ajoutons à cela que la filière *Cloud* devrait connaître une concentration importante (fusions-acquisitions) au cours des prochaines années en Europe. Autant d'éléments rendant le choix du prestataire « idéal » complexe pour des structures ne disposant pas de moyens financiers et techniques conséquents : « l'erreur », i.e. traiter avec une société faisant faillite dans les quelques mois suivant la signature du contrat, peut se payer au « prix fort » comme l'ont constaté les clients de la société *Code Spaces* (voir plus haut), et qui présentait pourtant son offre comme étant « solide comme un roc ».

Ainsi, si les sociétés recherchent des garanties en matière de gouvernance ou de sécurité, elles auront également le souci de nouer des liens commerciaux avec des sociétés solides d'un point de vue juridique et financier, jouissant d'une réputation d'expert, au-delà de la simple plaquette commerciale ou de démonstrations sur les réseaux sociaux.

2.1. Les risques liés à une inadéquation des compétences du prestataire

Le secteur étant en cours de structuration, la question se pose de savoir qui se cache derrière les dénominations commerciales. En s'informant sur l'historique des sociétés et les parcours de leurs dirigeants et actionnaires, il est possible d'évaluer le degré de crédibilité du fournisseur. Si ces dirigeants se trouvent être des « marqueteurs » ou des investisseurs présents sur plusieurs marchés à la fois, se sont-ils entourés d'une équipe disposant des compétences techniques nécessaires pour proposer une offre de qualité ? Leur conseil d'administration se

compose-t-il de « figures » du monde informatique ? Ou bien ont-ils délégué la partie « technique » à des sous-traitants, ajoutant un niveau supplémentaire dans la chaîne des interlocuteurs ? *In fine*, le client doit avoir l'assurance qu'il travaille avec des « gens sérieux », « libres de tous reproches » du point de vue de l'éthique professionnelle. Une première investigation permettra ainsi de raccourcir la liste des prospects.

2.2. Les risques liés à un environnement financier et / ou juridique incertain du prestataire

Afin de prévenir tout risque lié à une entrée en relation d'affaires, il semble primordial de se renseigner sur la situation juridique et financière du prestataire de services *Cloud*.

Beaucoup de fournisseurs se trouvent en effet dans une situation économique fragile ou ne sont en activité que depuis peu d'années. Une enquête préalable permettra de savoir si le prestataire a déjà fait l'objet de procédures collectives, s'il a franchi un seuil en matière d'activités (années d'existence, nombre de salariés, etc.), s'il parvient à dégager du « cash », etc. Le degré d'intérêt du prestataire pour sa filiale française serait également un indicateur fort : va-t-il l'aider financièrement en cas de besoin ou préfèrera-t-il la « sacrifier » au profit d'autres marchés ? Pour exemple, un prestataire américain comme Salesforce porte beaucoup d'intérêt à la France et au marché français, et est à ce titre soutenu par les pouvoirs publics, comme en témoigne la présence en juin dernier de l'ancienne Secrétaire d'Etat chargée du Commerce extérieur, Fleur Pellerin, lors de l'inauguration de ses nouveaux locaux parisiens. A contrario, un faible intérêt pour le marché français, en raison d'exigences sur la localisation des datacenters par exemple, ou une offre intéressante associée à un environnement juridique flou et à une santé financière moribonde devront alerter le client quant à la viabilité des opérations de l'entité.

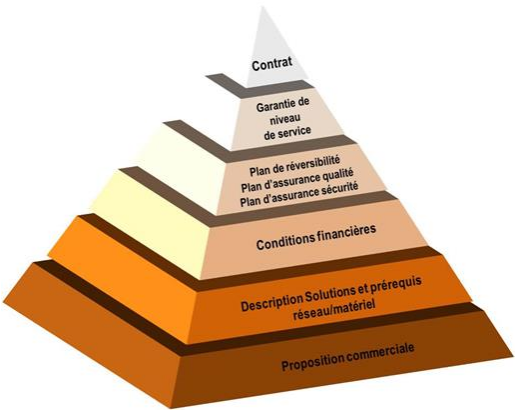
Pour éviter les mauvaises surprises et garder une certaine maîtrise de ses données, la société cliente doit savoir si le prestataire de services *Cloud* est indépendant et qui donne les ordres. Est-ce que le prestataire a été racheté ? Il est également essentiel de savoir si le prestataire est propriétaire de ses datacenters. Ses engagements pourraient se révéler moins fiables s'il n'en a pas la maîtrise. Dans ce cas de figure, il sera utile de procéder à des recherches permettant d'identifier l'opérateur des datacenters.

2.3. Les risques liés à la faible qualité des services proposés

Cette troisième et dernière interrogation majeure doit permettre au client de dépasser l'étude « à froid » des solutions proposées par le client pour recueillir des informations, par des sources ouvertes ou par le biais d'entretiens, des témoignages critiques, qu'ils soient positifs ou négatifs, sur la disponibilité des dirigeants, les moyens mis en œuvre par la société pour répondre aux attentes de ses clients, la qualité du service proposé. Trop souvent, les fonctions achats passent « à côté » de ces éléments, privilégiant les aspects financiers. Il est par ailleurs nécessaire, dans un contexte où le prestataire est relativement peu visible, de savoir s'il compte un portefeuille de clients actualisé et diversifié. Si aucune référence commerciale n'est identifiée, il sera important de réclamer au prestataire une liste de clients récente.

3. LES RISQUES CONTRACTUELS

Une clause contractuelle pourra lister les documents qui régissent la relation contractuelle, les annexer, les exclure et prévoir une hiérarchie des documents. Le contrat et les documents en annexes constitueront l'intégralité des engagements remplaçant et annulant tout engagement oral ou écrit antérieur. En cas de contradiction, cette hiérarchie permet que le document de rang supérieur prévale (cf. le schéma ci-dessous, la liste des documents contractuels mentionnés n'étant pas exhaustive).



3.1. Les risques pour les droits de propriété

Un contrat entre un prestataire de services *Cloud* et une entreprise peut contraindre cette dernière à renoncer à certains de ses droits sur ses données. Pour exemple, les conditions générales d'utilisation de Google Drive prévoient que le client reste propriétaire des contenus

déposés sur son service. Cependant, de manière plus floue, Google affirme garder le droit d'utiliser ces données afin « d'améliorer ses services »[7].

A qui appartiennent alors les données soumises au droit d'auteur, au droit des marques ou au droit des logiciels stockées dans le *Cloud* ? Cette question, dont la réponse peut parfois apparaître floue tant certains acteurs économiques étrangers voudraient parfois imposer des règles qui n'ont pas lieu d'être en l'occurrence (si les critères du droit français de la propriété intellectuelle sont réunis, le stockage dans le *Cloud* en lui-même n'accorde aucun droit au prestataire), peut aisément être réglée par une clause contractuelle claire. Car le contrat est la « *loi des parties* » et si le stockage dans le *Cloud* en soi ne confère pas de droit particulier au prestataire, le fait pour celui-ci d'insérer dans le contrat ou dans un document faisant partie du cadre contractuel une clause prévoyant le transfert de droit reste possible dans le cas d'une relation B to B[8]. Dans tous les cas, il est sain de rappeler les principes par une clause dénuée d'ambiguïté, insérée dans le document tout en haut de la pyramide contractuelle présentée ci-dessus : le client est et demeure le propriétaire de l'ensemble des données qu'il utilise *via* les services à sa disposition dans le cadre du contrat. Le prestataire, quant à lui, demeure titulaire des droits de propriété sur les services et l'infrastructure informatique mis à la disposition du client.

3.2. Les risques de poursuites judiciaires

Certains types de données dans certains secteurs particuliers nécessitent des mesures spécifiques. Le client doit s'y conformer sous peine d'engager sa responsabilité. Pour exemple, le secteur bancaire est soumis à une réglementation très contraignante en matière de contrôle

[7] ZDNet, *A quel point Google Drive est-il propriétaire de vos données ?* 25 avril 2012 : http://www.zdnet.fr/actualites/a-quel-point-google-drive-est-il-proprietaire-de-vos-donnees-39771132.htm (consulté le 26 février 2015).

[8] En BtoC, les règles protectrices du droit de la consommation pourront protéger le consommateur en déclarant certaines clauses « abusives », donc nulles et non avenues. Voir à ce titre la recommandation n° 2014-02 « relative aux contrats proposés par les fournisseurs de services de réseaux sociaux » qu'a adopté le 7 novembre 2014 la Commission des clauses abusives (téléchargeable sur http://www.clauses-abusives.fr/recom/14r02.htm) : parmi les 46 propositions concrètes émises dans le document, 27 sont des recommandations qui peuvent s'appliquer à tout site de commerce électronique et 9 à tout site traitant des données à caractère professionnel d'une large clientèle. Pour une analyse plus complète de cette recommandation, voir la Newsletter ATIPIC Avocat n°1 téléchargeable sur http://www.atipic-avocat.com/app/download/10877446/2015-1-Newsletter+ATIPIC+Avocat+JanvFev.pdf.

interne[9] tout comme le secteur des assurances[10]. Dans le secteur médical, le prestataire de services *Cloud* doit être agréé par le ministre chargé de la santé pour héberger des données de santé[11].

3.2.1. Le cas des données à caractère personnel

Selon l'article 2 de la loi « Informatique et libertés » du 6 janvier 1978[12], « *constitue une donnée à caractère personnel 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.* » Des informations comme le nom, le prénom, l'adresse d'un client, d'un salarié ou d'un prospect constituent des données à caractère personnel.

Une société cliente qui conserve et traite ces données est qualifiée de responsable de traitement[13]. Elle doit prendre des précautions particulières. En effet, selon l'article 34 de la loi de 1978, le client doit « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.* » Il peut choisir de déléguer la gestion des traitements comme en matière de *Cloud* mais il doit s'assurer que le prestataire dispose bien de toutes les « garanties suffisantes » en matière de sécurité technique. Car de toute façon, il ne fait que déléguer le traitement, en aucun cas sa responsabilité sur celui-ci, comme a pu le montrer la sanction de la société Orange le 7 août 2014 : les données clients indûment accédées ne l'ont pas été *via* le piratage du système d'information d'Orange en tant que tel, c'est en réalité le sous-traitant d'un sous-traitant d'Orange qui a été victime de la faille de sécurité[14].

---

[9] Règlement CRBF 97-02 du 21 février 1997 abrogé et remplacé par l'arrêté du 3 novembre 2014 disponible sur Legifrance (consulté le 22 février 2015).
[10] Article R. 336-1 du Code des assurances modifié par le décret n°2014-1315 du 3 novembre 2014 disponible sur Legifrance (consulté le 22 février 2015).
[11] Article R. 1111-10 du Code de la santé publique modifié par le décret n°2011-246 du mars 2011 disponible sur Legifrance (consulté le 22 février 2015).
[12] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, disponible sur Legifrance (consulté le 22 février 2015).
[13] Article 3 de la loi « Informatique et libertés » précitée, disponible sur Legifrance (consulté le 21 février 2015).
[14] Voir la décision de sanction de la CNIL sur http://www.cnil.fr/linstitution/actualite/article/article/la-societe-orange-sanctionnee-pour-defaut-de-securite-des-donnees-dans-le-cadre-de-campagnes/

En outre, selon l'article 68 de la même loi, il est interdit de transférer des données à caractère personnel hors de l'Union Européenne sauf à fournir des garanties suffisantes en matière de sécurité. Certaines formalités imposées par la Commission nationale de l'informatique et des libertés (CNIL) sont à effectuer (clauses contractuelles types, autorisations).

Concernant les transferts à destination des Etats-Unis, l'entreprise américaine ou sa filiale à l'étranger doit figurer sur la liste *Safe Harbor* du site du département américain du commerce et remplir les conditions en matière de protection des données personnelles, étant entendu que certains secteurs sont exclus de l'accord (secteur financier) et que le prestataire adhérant de façon complètement volontaire au système peut y mettre fin à tout moment. Cette adhérence au *Safe Harbor* est donc à suivre avec grande attention dans le temps et mérite là aussi un encadrement spécifique. Par ailleurs, en mars 2015, dans une affaire *Facebook* opposant un internaute autrichien et la CNIL irlandaise, l'avocat du gouvernement autrichien a estimé que « *Safe Harbor n'est pas adéquat pour les données des citoyens européens, mais est, au mieux, un port sûr pour les pirates de données* ». L'utilisateur refusait que ses données personnelles soient exploitées par les géants américains sans contrôle préalable. La CJUE doit rendre son avis le 24 juin prochain[15].

On conseillera donc au client de prévoir contractuellement que le prestataire restera adhérent au *Safe Harbor* pendant toute la durée du contrat et de renforcer au besoin *via* le contrat le niveau de ses obligations. Il pourrait ainsi être préférable de signer les clauses contractuelles types précitées, pour éviter au client toute déconvenue du fait d'un prestataire qui ne serait plus adhérent au *Safe Harbor* quelque temps après le début du contrat.

En effet, rappelons que le client encourt des sanctions pénales en cas de non-respect des dispositions de la loi « Informatique et libertés » et cela même en cas de délégation de la gestion du traitement à un prestataire de services *Cloud*. En pratique, il encourt surtout les sanctions de la CNIL. Si pour l'heure, c'est l'effet d'image qui l'emporte sur les montants financiers prononcés (qui ne dépassent qu'exceptionnellement les 100 000 €), la donne pourrait changer rapidement et de manière drastique : on parle ainsi de sanctions indexées sur un pourcentage du chiffre d'affaires annuel mondial (2 % ? 5 % ?), le renforcement étant prévu par le biais de la loi sur le numérique (fin 2015 ?) et en tout état de cause par le règlement

[15] Journal du Geek.com, *[Safe Harbor] La Commission européenne conseille de quitter Facebook pour échapper à la NSA*, 30 mars 2015 : http://www.journaldugeek.com/2015/03/30/safe-harbor-commission-europeenne-quitter-facebook-echapper-nsa (consulté le 9 avril 2015).

européen sur la protection des données à caractère personnel. Le texte de ce projet est toujours en discussion mais son adoption semble possible pour fin 2015 / début 2016.[16]

Enfin, le caractère insuffisant des informations sur les opérations de traitement d'un service *Cloud* présente un risque pour les responsables du traitement et pour les personnes concernées car s'ils ne sont pas informés des menaces et des risques éventuels, ils n'auront pas la possibilité de prendre les mesures qu'ils jugent les mieux indiquées, ce qui pourrait être considéré comme une atteinte aux droits des personnes en matière d'accès, de rectification et de suppression des données par manque de possibilités d'intervention[17]. En pratique, cela est surtout rigoureusement contraire à un principe essentiel porté par le projet de règlement européen susmentionné : « l'*accountability* », c'est-à-dire en substance l'obligation pour le responsable de traitement non seulement d'assurer une traçabilité de la donnée à toutes les étapes, de sa vie à sa mort, mais surtout d'apporter la preuve qu'il est bien en mesure d'assurer cette traçabilité. Une fois ce règlement adopté, la conformité devra être assurée, étant entendu qu'il est prévu en parallèle que le prestataire puisse devenir juridiquement co-responsable de la protection des données personnelles, ce qui l'incitera d'autant plus à faire des efforts de traçabilité et de visibilité.

3.3. Les difficultés de saisine des tribunaux

Il est important pour le client de connaître quel droit régit le contrat et devant quelle juridiction il pourra faire valoir ses droits. Selon le montant que le contrat rapportera au prestataire, et selon son propre poids sur le marché, le pouvoir de négociation du client sera plus ou moins important. Dans tous les cas, il faudra envisager une clause contractuelle prévoyant expressément le droit applicable et la juridiction compétente. Le client doit garder à l'esprit que la saisine des tribunaux français sera beaucoup plus aisée et moins coûteuse que la saisine de tribunaux étrangers dont le coût de la procédure dépend en fonction des pays. En pratique, le pays de saisine des tribunaux en cas de litige est l'objet habituel de négociation entre parties de deux pays étrangers, le recours à l'arbitrage pouvant souvent apparaître comme une solution de consensus.

[16] Un délai de 2 ans étant nécessaire avant son applicabilité à tous les pays de l'Union européenne, sans passer par la phase de transposition comme pour une directive.
[17] G29 sur la protection des données personnelles, avis 05/2012 sur l'informatique en nuage adopté le 1er juillet 2012.

4. LES RISQUES DE SECURITE

Les facteurs de risques de sécurité intrinsèques au prestataire *Cloud* et sa plate-forme sont multiples et peuvent porter atteinte à la confidentialité, l'intégrité et la disponibilité du service et des données confiées, et avoir des impacts pour l'organisation cliente (perte de réputation, perte de confiance des clients, pertes de revenus, etc.). La liste ci-dessous des risques et des mesures de réduction n'est pas exhaustive.

Certaines start-ups font de la sécurité des plate-formes *Cloud* leur spécialité. C'est le cas par exemple de CipherCloud et d'Elastica qui permettent un accès sécurisé au Cloud.

4.1. Les risques liés à un effacement insatisfaisant des données

A la fin du contrat, chacune des parties doit s'engager à restituer toutes les copies des documents et supports contenant des informations considérées comme confidentielles par le client. Ainsi, à la signature du contrat, une classification des données confiées au prestataire *Cloud* doit être effectuée par le client. Cependant, il faut bien prendre garde à la destruction effective de l'intégralité des données concernées, notamment en s'en assurant contractuellement par référence aux modalités choisies pour cette suppression. Cela s'explique, d'une part, en raison des exigences du projet de règlement européen sur la protection des données à caractère personnel et de l'obligation de traçabilité de la donnée susmentionnées, mais d'autre part, parce que le client peut lui-même être tenu à des engagements particuliers en la matière par ses propres clients, indépendamment de la nature de la donnée en elle-même (secrets de fabrique, etc.).

Plusieurs recommandations existent en la matière, provenant essentiellement de services militaires à l'origine (US Army, US Department of Defense, NIST, etc.), pour permettre un effacement le plus sécurisé possible des données. Un engagement des prestataires de services *Cloud* à respecter les meilleures pratiques en la matière, avec indication des textes visés, peut être nécessaire en fonction de la sensibilité des données traitées, une fois celle-ci évaluée par le client (Sont-ce des données personnelles ? Des données produites ayant une valeur commerciale ? Etc.).

4.2. Les risques liés au manque d'étanchéité des ressources

Avec le *Cloud public* et une architecture « *multi-tenant* », un risque de décloisonnement des données de plusieurs clients peut être ressenti comme possible. Les mécanismes d'isolation technique (stockage, mémoire) peuvent être défaillants et l'intégrité ou la confidentialité des données compromises. Les infrastructures « haut de gamme » offrent un meilleur cloisonnement des données que les infrastructures moins onéreuses, assimilables à un *Cloud privé* exclusif à un client.

En outre, la société cliente doit pouvoir identifier les membres du personnel du prestataire de services *Cloud* qui ont accès aux données. Une politique stricte de contrôle d'accès aux données, d'autant plus selon leur nature et sensibilité (données de santé, données bancaires, etc.) devra s'appliquer aux membres du personnel du prestataire, tout comme la signature d'engagements de confidentialité exhaustifs.

4.3. Les risques d'intrusions physiques et logiques

Selon une étude publiée en juin 2014, le coût annuel du cybercrime serait compris entre 375 et 575 milliards de dollars dans le monde. Il existe des risques de vol de données confidentielles sur les clients et de vol de données de fonctionnement interne mais également des risques d'atteinte à l'image de l'entreprise[18]. En avril 2011, 77 millions de coordonnées bancaires ont été extraites du Playstation Network, le service de jeux et de médias en ligne distribué par Sony. En 2014, la chaîne de magasins Target aux Etats-Unis avait été piratée, le vol massif de données bancaires ayant été permis en raison d'une intrusion sur le système d'information de son sous-traitant d'air conditionné, interconnecté avec celui de Target. Ce ne sont ainsi pas moins de 40 millions de numéros de cartes bancaires qui ont été volés[19]. En mars 2015, IBM a alerté Dropbox d'une faille de sécurité touchant son application Android. Ce problème a été

[18] PLOUIN, Guillaume. *CLOUD COMPUTING, Sécurité, stratégie d'entreprise et panorama du marché*. Dunod Paris 2013.
[19] HERMANN Vincent, *Le piratage de la chaine Target viendrait de la réutilisation d'authentifiants,* Nextinpact.com, 6 février 2014 : http://www.nextinpact.com/news/85776-le-piratage-chaine-target-viendrait-reutilisation-dauthentifiants.htm (consulté le 7 avril 2015).

résolu grâce à un correctif de sécurité mais, concrètement, un hacker aurait pu accéder aux informations sensibles des utilisateurs[20].

Ainsi, l'organisation cliente doit s'assurer entre autres que le prestataire a mis en place des procédés techniques et des processus suffisamment robustes (contrôle d'accès physique et logique renforcé du personnel du prestataire, authentification forte des administrateurs, chiffrement des bases de données, sécurisation réseaux, détection d'évènements de sécurité, notification, etc.) permettant de protéger les données et réduire l'impact même en cas de violations. L'organisation cliente doit s'assurer que le prestataire de services *Cloud* s'est engagé dans une stratégie globale de certifications et d'attestations[21] afin de faire reconnaître la conformité de ses infrastructures et de ses services avec les bonnes pratiques et standards internationaux. Cette reconnaissance de savoir-faire renforce la chaîne de confiance entre le fournisseur et ses clients et partenaires. Les certifications à considérer sont par exemples : ISO/IEC 27001, PCI-DSS, SOC 1 TYPE II ET SOC 2 TYPE II, Cloud Confidence, Cloud Security Alliance STAR, etc. De plus, il est primordial d'analyser le périmètre couvert par la certification. Même si une certification ou une attestation ne garantit pas du niveau de sécurité d'un service *Cloud*, il démontre de la prise en compte des aspects de sécurité dans le service délivré.

4.4. Les risques liés à un mode d'authentification faible

Le prestataire de services *Cloud* doit mettre en place une identification et une authentification sécurisée des utilisateurs pour garantir la confidentialité et l'intégrité des données. En l'absence de ces garanties, il fait courir un risque à ses clients et aux clients de ses clients. Il est en effet primordial de limiter l'accès aux données.

L'authentification est une procédure qui consiste, pour un système informatique, à vérifier l'identité d'un accédant avant de lui autoriser l'accès au système. Dans le cas où le prestataire ne prévoit pas d'authentification, une personne malintentionnée réussissant à récupérer un mot de passe administrateur peut prendre le contrôle total sur le système et, par exemple, supprimer à sa guise tous les comptes utilisateurs de l'application SaaS ou même ceux d'un

[20] GAGLIORDI Natalie, *IBM uncovers severe vulnerability in Dropbox SDK for Android*, ZDNet.com, 11 mars 2015 : http://www.zdnet.com/article/ibm-uncovers-severe-vulnerability-in-dropbox-sdk-for-android (consulté le 12 mars 2015).

[21] Liste des schémas de certification référencés par l'ENISA : https://resilience.enisa.europa.eu/Cloud-computing-certification

service PaaS ou encore l'ensemble des boîtes de messagerie de toute l'entreprise[22]. On peut citer pour exemple l'intrusion dans l'espace de stockage de données en ligne Dropbox en juin 2012. Le hacker a pu mettre la main sur les adresses e-mails des clients de la start-up et spammer les messageries. Suite à cela, le prestataire Dropbox a mis en place un système d'authentification forte.

Le prestataire devra ainsi garantir un mode d'authentification si possible fort à deux facteurs (par exemple avec l'envoi d'un code unique par SMS sur le mobile de l'utilisateur) pour éviter un accès non autorisé aux données mais également une altération de ces dernières. Le prestataire devra également mettre tout en œuvre pour minimiser les risques d'intrusions physiques et logiques.

Par ailleurs, une fois l'utilisateur du service authentifié (ou les administrateurs du personnel du prestataire), le prestataire *Cloud* doit disposer de mécanismes de traçabilité des accès aux données. En effet, la société cliente doit pouvoir consulter les traces opérationnelles et de sécurité, afin d'être en mesure de surveiller en temps réel la sécurité de la plate-forme *Cloud* et des données, de faire des analyses *a posteriori* et d'accorder une certaine confiance à l'information.

4.5. Les risques liés à l'application des législations étrangères

En 2015, la Chine prévoit d'adopter un projet de loi de lutte contre le terrorisme qui imposerait aux sociétés américaines de leur remettre les clés de chiffrement et les mots de passe et d'installer des *backdoors* à des fins de surveillance[23].

La version américaine est plus ancienne et porte le nom de *Patriot Act* ou plus largement de *Foreign Intelligence Surveillance Amendement Act* (FISAA). Ces lois permettent à l'administration américaine de demander l'ouverture de ses bases de données à toute société ayant son siège aux Etats-Unis pour des motifs de lutte contre le terrorisme[24]. Le champ d'application de la FISAA n'est cependant pas défini : cette loi s'impose à tous les prestataires

[22] PLOUIN, Guillaume. *CLOUD COMPUTING, Sécurité, stratégie d'entreprise et panorama du marché*. Dunod Paris 2013.
[23] FLECHAUX Reynald, *Mesures protectionnistes chinoises : Obama s'énerve*, Silicon.fr, 3 mars 2015 : http://www.silicon.fr/mesures-protectionnistes-chinoises-obama-senerve-109783.html (consulté le 10 mars 2015).
[24] Sécurité & Stratégie. *Enquête au cœur des directions de sécurité et sûreté n°4*, novembre 2013 : http://www.securite-strategie.fr/international-informatique-en.html (consulté le 21 février 2015).

américains de services de communication et de services informatiques ainsi qu'à leurs filiales, indépendamment de leur lieu d'implantation, ou aux prestataires étrangers de ces services qui opèrent sur le territoire américain[25]. De manière plus concrète, la NSA et le FBI peuvent donc avoir accès aux données qu'une entreprise américaine héberge dans le *Cloud* et cela que les datacenters soient localisés aux Etats-Unis ou en Europe depuis l'affaire *Microsoft* (Cour fédérale New York, 25 avril 2014), tout en empêchant dans la plupart des cas aux prestataires de prévenir leurs clients de cet accès sous peine de sanctions pénales (« *gag order* »).

En France, des débats parlementaires ont actuellement lieu sur le projet de loi relatif au renseignement du 19 mars 2015 et les accès aux données – et en particulier aux métadonnées – qu'il peut prévoir. S'il est très tôt pour en faire une analyse précise, surtout au vu de la seule discussion à l'Assemblé nationale, il ne semble pas que le texte vise à permettre le niveau d'intrusion et d'accès que prévoit déjà le droit américain, loin de là.

Plus globalement, une étude attentive des textes applicables permet de déterminer que chaque pays a sa législation, parfois bien particulière dans le domaine, et qu'elle affectera le client selon le lieu d'hébergement de ses données. Alors que certains prestataires *Cloud* ne divulgueront les données que s'ils y sont invités par une décision judiciaire et informeront leurs clients, d'autres dévoileront plus facilement les données. En France, par exemple, les règles pourront également être différentes selon que les données soient des données à caractère personnel, et/ou des données fiscales, si une requête est présentée à un juge par exemple pour disposer de preuves dans un procès à venir ou encore si elles sont utilisées dans le cadre d'une procédure pénale.

En outre, la législation de chaque pays où les données sont hébergées peut s'appliquer. Il est donc primordial de bien comprendre et d'analyser correctement les règles s'appliquant aux prestataires en cause et qui pourraient le conduire à délivrer des informations, parfois sans en informer son client (cas du « *gag order* » fédéral précité). Définir le droit applicable et la juridiction compétente en cas de litige par une clause contractuelle ne prémunit en rien contre cela, les dispositions dites « d'ordre public » issues potentiellement de chaque droit local prévalent sur les règles contractuelles conclues entre les parties.

[25] BONNET Florence, Consultante CIL consulting. *Le Cloud Computing à l'ère post Snowden : et après ?* 4 juin 2014 : http://www.village-justice.com/articles/Cloud-computing-ere-post-Snowden,17060.html (consulté le 21 février 2015).

4.6. Les risques liés au degré d'exposition du prestataire

Un grand prestataire américain de services *Cloud* aura plus de visibilité qu'un prestataire de second rang et sera davantage exposé aux attaques. Reste à savoir s'il sera mieux armé qu'un petit prestataire en termes de sécurité. Il est important de connaître le nombre des attaques, des incidents avérés et leur fréquence. Pour avoir conscience des risques encourus, il est indispensable de connaître la nature de ses attaques. Les conséquences en termes de risques ne sont pas les mêmes qu'il s'agisse d'attaques dues à des failles de sécurité ou liées à une tentative de phishing. Pour exemple, un prestataire aussi important que Salesforce.com fait régulièrement, et très logiquement, l'objet de nombreuses tentatives de phishing. Il existe un facteur humain dans ces attaques : une sensibilisation préalable du personnel du prestataire et des clients est donc nécessaire pour remédier à ce type de risque.

4.7. Les risques pour l'intégrité des données

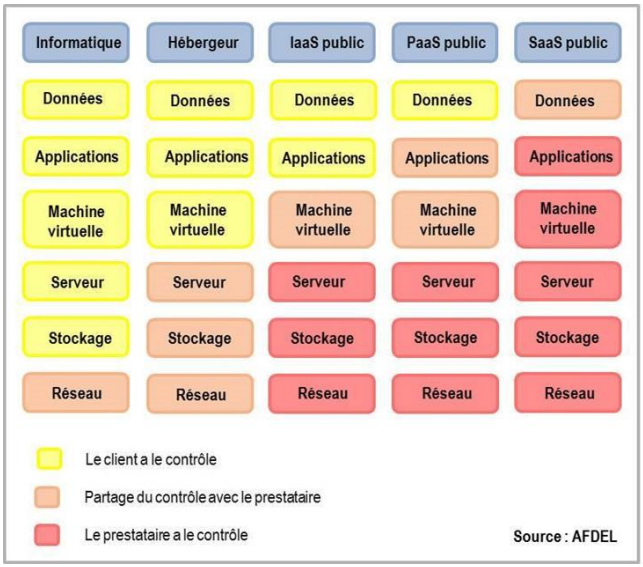
Les risques liés à l'intégrité des données et les moyens de s'en prémunir sont assez similaires à ceux constatés pour la confidentialité des données. Le prestataire devra garantir un mode d'authentification si possible fort à deux facteurs (par exemple avec l'envoi d'un code par SMS sur le mobile de l'utilisateur) pour éviter un accès non autorisé aux données et une altération de ces dernières. Le prestataire devra également mettre tout en œuvre pour minimiser au maximum les risques d'intrusions physiques et virtuelles. Malgré un risque d'attaques élevé selon le degré de visibilité du prestataire *Cloud*, la sécurité de l'intégrité des données passera nécessairement par le respect de normes techniques bien connues.

4.8. Les risques liés au degré de contrôle du prestataire

En utilisant les services *Cloud*, le client concède souvent au prestataire un contrôle total sur son infrastructure et son système d'information, y compris sur la gestion des incidents de sécurité[26]. Plus le client demande un service abouti et prêt à l'emploi (application SaaS), plus il peut perdre le contrôle sur ses systèmes et applications. Cela sera plus ou moins acceptable selon les secteurs d'activité.

[26] PLOUIN, Guillaume. *CLOUD COMPUTING, Sécurité, stratégie d'entreprise et panorama du marché*. Dunod Paris 2013.

En outre, le risque que les données soient « gelées » en cas de poursuite judiciaire est à considérer. On peut citer pour exemple la plate-forme de stockage *Megaupload* dont les serveurs étaient inaccessibles pour ses clients. Ils n'avaient donc plus accès aux fichiers stockés sur la plate-forme[27].



4.9. Les risques relatifs à la Qualité de Service

Le prestataire doit s'engager sur la qualité de son service par le biais d'une convention de niveau de service (*Service Level Agreement* ou *SLA*). Il sera important de s'accorder sur le type d'obligation incombant au prestataire. S'agit-il d'une obligation de moyen ? Une obligation de moyen renforcée ? Une obligation de résultat ? L'obligation de moyen implique que le prestataire s'engage à mettre tout en œuvre pour garantir le niveau de service promis, étant

[27] MURRAY Paul, SHRUM Sandy, *Common Risks of Using Business Apps in the Cloud*. US-CERT : https://www.us-cert.gov/sites/default/files/publications/using-Cloud-apps-for-business.pdf (consulté le 4 mars 2015).

entendu que la preuve contraire peut être rapportée par le client. En cas d'obligation de résultat, le prestataire doit atteindre à tout prix le niveau de service promis sous peine d'engager sa responsabilité. Dans une obligation de moyen renforcée, courante pour les services *Cloud*, le prestataire mettra les moyens nécessaires pour arriver au niveau de service prévu et devra prouver qu'il n'a pas commis de faute en cas de contentieux.

Les *SLA* font partie intégrante du contrat et établit notamment le taux de disponibilité du service, les délais d'interruption, les sauvegardes effectuées, les délais d'intervention, mais également des métriques de sécurité (par exemples réponse aux incidents, isolement des données, gestion des traces, etc.).[28]

Qu'est-ce que la disponibilité ? C'est l'accessibilité du client au service proposé par le prestataire. Selon les besoins du client, le taux de disponibilité sera plus ou moins élevé. Selon *Gartner Group*, on peut faire un classement[29] :

- La classe 1 concerne les applications de relations clients ou partenaires, les fonctions critiques pour le chiffre d'affaires. Dans ce cas, il faut une disponibilité à 99,9 % soit une interruption inférieure à 45 minutes par mois. Dans ce cas le temps de restauration maximal (*Recovery Point Objective ou RTO*) ne pourra dépasser deux heures et la période maximale de perte de données (*Recovery Point Objective ou RPO*) devra être nulle.

- La classe 2 concerne les fonctions génératrices de revenu moins critiques et les fonctions logistiques. La disponibilité sera de 99,5% soit une interruption inférieure à 3,5 heures/mois. Le *RTO* sera de 8 à 24 heures et le *RPO* de 4 heures.

- La classe 3 concerne les fonctions d'entreprise de type back office. La disponibilité sera de 99% soit une interruption inférieure à 5,5 heures par mois. Le *RTO* sera de 3 jours et le *RTO* d'un jour.

- La classe 4 concerne les fonctions départementales. La disponibilité pourra être de 98% soit une interruption inférieure à 13,5 heures par mois. Le *RTO* sera de 4 à 5 jours et le *RPO* d'un jour.

[28] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-Cloud-contracts/at_download/fullReport
[29] JACQUOT Thierry, *Reprise d'activité : n'oubliez pas le back up*, 01net.com, 5 août 2005 : http://pro.01net.com/editorial/285929/reprise-dactivite-noubliez-pas-le-back-up (consulté le 10 mars 2015).

Il paraît indispensable de préciser si les heures d'indisponibilité sont en continu ou espacées. En effet, un taux élevé de disponibilité de 99,9% peut correspondre à huit heures d'indisponibilité de suite par an. Ces informations sont donc essentielles, tout comme la durée, pour résoudre l'incident. Dans une affaire rendue par le tribunal de commerce de Paris, le 12 juillet 2011, le prestataire avait prévu une durée d'intervention de 30 jours. Au bout de 8 jours d'interruption de service (de la messagerie électronique de l'entreprise, stockée dans le *Cloud* en l'occurrence), le client a résilié le contrat. La rupture ayant été considérée comme abusive par le tribunal, il a été condamné à verser des dommages-intérêts au prestataire.

De plus, malgré ses promesses de disponibilité souvent à 99,9%, le prestataire de services *Cloud* n'est pas à l'abri d'une défaillance technique entraînant la perte ou l'altération des données portant atteinte à leur intégrité. Selon *l'International Working Group on Cloud Computing Resiliency* qui référence toutes les pannes, les 13 premiers prestataires de services *Cloud* dans le monde ont cumulé 600 heures d'indisponibilité sur les 5 dernières années[30]. Il paraît ainsi important de savoir si des copies des données sur des sites géographiquement distincts sont effectuées régulièrement. Pour exemple, l'offre *Cloud* de Microsoft Azure a subi plus de 100 interruptions de service en 2014 contre 86 pour le *Cloud Compute Engine* de Google et douze pour EC2 d'Amazon[31]. En octobre 2012, l'ouragan Sandy avait inondé les centres de données américains et, par ricochet, les infrastructures d'Amazon et de Google. Si les promesses de disponibilité ne sont pas tenues, encore faut-il toutefois que les clauses ad hoc du contrat prévoient une indemnisation à hauteur du préjudice que peut subir l'entreprise.

4.10. Les risques liés au manquement aux obligations de niveau de service

Ainsi, il est très important de faire attention à la portée de la clause limitative de responsabilité et au montant des pénalités forfaitaires. Tout d'abord, le prestataire qui aura prévu des pénalités très faibles préfèrera manquer à ses obligations en matière de niveau de service plutôt que de respecter ses engagements si cela lui coûte plus cher.

---

[30] Silicon.fr, *Comment garantir la sécurité du Cloud public*, 14 mars 2014 : http://www.silicon.fr/dossiers/comment-garantir-securite-Cloud-public (consulté le 20 février 2015).
[31] ZDNet, *Cloud Public : Microsoft Azure, champion des pannes en 2014*, 16 janvier 2015 : http://www.zdnet.fr/actualites/Cloud-public-microsoft-azure-champion-des-pannes-en-2014-39813127.htm (consulté le 20 février 2015).

En effet, la clause pénale fixe un montant forfaitaire de dommages-intérêts en cas d'inexécution (manquement) du contrat. Néanmoins, l'article 1152 du Code civil ajoute que « *le juge peut, même d'office, modérer ou augmenter la peine qui avait été convenue, si elle est manifestement excessive ou dérisoire* ». Si le prestataire prévoit une clause pénale libératoire, le client ne pourra pas demander en plus l'indemnisation du préjudice causé par ce même dommage (article 1229 du Code Civil).

Ensuite, le prestataire peut s'exonérer de toute responsabilité grâce à une clause limitative de responsabilité. Elle peut toutefois être écartée par le juge si elle contredit la portée de l'obligation essentielle du contrat et le vide de toute sa substance (Com, 29 juin 2010, *Sté Faurecia c/ Oracle*). Encore faut-il bien évidemment, dans ces deux cas, que le droit français soit applicable au contrat.

4.11. Les risques pour la traçabilité

Le prestataire doit disposer de mécanismes de traçabilité des accès aux données. En effet, la société cliente doit pouvoir consulter les traces opérationnelles et de sécurité. Afin d'être en mesure de monitorer en temps réel la sécurité du système et des données, de faire des analyses *a posteriori* et d'accorder une certaine confiance à l'information.

CUMULUS
Une offre unique de conseil en Management des Risques dédiée au Cloud computing

Notre expertise en matière de Due Diligence & Management des Risques d'une part, et de Conseil en Cybersécurité d'autre part, nous permet avec nos partenaires de proposer à nos clients une approche transverse et globale liée aux prestations *Cloud*, regroupant :

- Risque juridique, induit par les contrats & CGV,
- Risque commercial, lié intrinsèquement à vos prestataires,
- Risque IT, en particulier au niveau sécurité.

Pour analyser et évaluer les risques liés à l'adoption du cloud computing, CEIS, ATIPIC et Business Digital Security ont ainsi développé un référentiel qui s'appuie sur les travaux des autorités françaises et européennes telles que la CNIL, l'ANSSI, l'ENISA et l'Autorité de Contrôle Prudentiel (ACP) pour le secteur bancaire. Il s'appuie également sur les travaux d'organisations telles que Syntec Numérique, Cloud Security Alliance (CSA), EuroCloud, le *Committee of Sponsoring Organizations of the Treadway* Commission (COSO) et l'association Cloud Confidence.

Nous proposons un service personnalisé, adapté au niveau de maturité de votre organisation, et à votre « appétit » en termes d'adoption progressive de solutions *Cloud*.

Quelle que soit votre maturité, notre service inclut nativement une analyse stratégique, sécuritaire et juridique de vos fournisseurs et solutions *Cloud* stratégiques, grâce à des prestations de due diligence et de veille.

Pour plus de détails sur l'offre Cumulus :

Vincent RIOU | Directeur Business Development | CEIS

vriou@ceis.eu

Tél : +33 (0)6 07 34 09 14

ceis

Systèmes d'information opérationnels et de communication en Europe. Avril 2015

Quel référentiel pour les métiers de la cybersécurité ? Février 2015

Netmundial, un pas décisif dans l'évolution de la gouvernance Internet ? Février 2015

Comment développer la main d'œuvre en cybersécurité ? Février 2015

Cybercriminalité et réseaux sociaux : liaisons dangereuses ? Février 2015

L'entrainement « cyber », élément clé de la résilience des organisations. Janvier 2014 - English version available

Monnaies virtuelles et cybercriminalité - Etat des lieux et perspectives. Janvier 2014 - English version available

Cybersécurité des pays émergents - Etat des lieux. Janvier 2014 - English version available

CEIS

Compagnie Européenne d'Intelligence Stratégique

Société Anonyme au capital de 150 510 €

SIRET : 414 881 821 00022 – APE : 741 G

280 boulevard Saint Germain – 75007 Paris

Tél. : 01 45 55 00 20 – Fax : 01 45 55 00 60