CHAPITRE 3
Les enjeux juridiques du Cloud computing

Rose-Marie BORGES
Maître de conférences, Université d'Auvergne

La révolution numérique entamée ces dernières années a vu émerger de nouvelles offres de services parmi lesquelles le Cloud computing tend à occuper une place de choix.

Le Cloud computing est un modèle d'accès à des ressources informatiques partagées telles que des réseaux, des serveurs, du stockage, des applications et des services. L'accès à ces ressources se fait grâce à Internet ou à l'Intranet de l'entreprise. Le Cloud présente de nombreux avantages pour les entreprises qui décident d'y recourir en raison de la souplesse du système, d'un accès théorique à des ressources illimitées et de la réduction des coûts liée à l'externalisation de certains traitements.

La décision d'externaliser la totalité ou une partie des données et de leur traitement doit résulter d'un choix mûrement réfléchi de l'entreprise en raison des risques induits par ce choix. En effet, aux risques traditionnels liés à la sécurité des données dans l'entreprise, s'ajoutent les risques générés par l'intervention d'un prestataire extérieur, notamment en ce qui concerne la protection des données qui lui sont confiées. Ces risques existent quel que soit le type de Cloud choisi mais sont accentués par les spécificités de certains d'entre eux.

L'entreprise a le choix entre trois modèles principaux de Cloud :

- Infrastructure as a Service (IaaS) : c'est le service de plus bas niveau. Le fournisseur de Cloud offre l'accès à un parc informatique virtualisé sur lequel le client peut installer un système d'exploitation et des applications. Il est ainsi dispensé de l'achat de matériel informatique ;

- Platform as a Service (PaaS) : c'est le niveau de service au-dessus du précédent. L'infrastructure et le système d'exploitation sont fournis par le prestataire de Cloud et le client peut ajouter ses propres outils et des applications ;

- Software as a Service (SaaS) : des applications sont mises à la disposition des clients, accessibles via Internet. Le client n'a plus à se préoccuper de la manière dont le service est fourni (c'est par exemple le cas du service Gmail).

Ces modèles de Cloud peuvent être déployés selon trois schémas qui sont fonction de leur degré de mutualisation :

- Cloud privé : le service est dédié à un client ;

- Cloud public : le service est partagé et mutualisé entre plusieurs clients, plus ou moins nombreux ;

- Cloud hybride : le service est partiellement dans un cloud privé et un cloud public.

Le Cloud public entièrement externalisé, dont l'application la plus courante est la messagerie électronique, est constitué de services gratuits ou payants de stockage et d'applications Web généralement destinés au grand public. Ces services sont accessibles via le réseau Internet. Ce modèle de Cloud est celui qui génère le plus grand nombre de risques juridiques. Il repose en effet sur la disponibilité et l'accessibilité des données pour l'utilisateur. Ces données peuvent être stockées directement chez le fournisseur de Cloud ou chez l'un de ses sous-traitants. Les infrastructures de stockage peuvent également être situées dans plusieurs pays, empêchant alors l'utilisateur de géolocaliser ses données. L'éparpillement des sites de stockage soulève la question de la législation applicable en cas de litige, les données étant en principe soumises à la loi du pays d'hébergement (II). Comme tout système d'hébergement le Cloud computing doit respecter un certain niveau de sécurité mais celui-ci peut s'avérer insuffisant pour garantir l'intégrité ou la confidentialité des données (I).

1. La sécurisation juridique des données hébergées en Cloud

Les données hébergées en Cloud sont très diverses et peuvent représenter une valeur plus ou moins importante pour l'entreprise. La CNIL a identifié quatre catégories de données pouvant être impactées par le Cloud, selon leur intérêt pour l'entreprise[1] :

- **Les données à caractère personnel** : 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.

- **Les données sensibles** : ce sont des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. Sont également concernées les données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté.

- **Les données stratégiques pour l'entreprise** : ce sont celles qui peuvent éventuellement lui procurer un avantage concurrentiel.

- **Les données utilisées dans les applications métiers**

Le Cloud géré en externe et à usage ouvert ou Cloud public est l'environnement qui suscite le plus de craintes car il peut directement porter atteinte aux principes de disponibilité, d'intégrité, de traçabilité et de confidentialité, qui régissent les services informatiques.

1.1 La disponibilité des données

La disponibilité des données hébergées sur le Cloud est fortement dépendante de la disponibilité du réseau Lorsque ces données sont accessibles via Internet, leur disponibilité sera fonction de celle du réseau Internet, or celle-ci ne peut en aucun cas être garantie. Il sera donc difficile d'imposer au prestataire un taux de disponibilité de l'infrastructure comme on pourrait le faire dans le cadre d'un Cloud privé.

1. Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing, CNIL juin 2012, p. 2.

Le contrat conclu entre l'entreprise et le prestataire devrait contenir une clause précisant les sanctions applicables en cas d'indisponibilité du service. Ces sanctions sont généralement représentées par le versement de pénalités contractuellement déterminées. Ces sommes ne compensent cependant pas nécessairement le préjudice effectivement subi par l'entreprise, l'indisponibilité des données pouvant avoir des effets particulièrement néfastes pour les différents services du client.

De surcroît, ces clauses, dont le contenu peut s'avérer insuffisant au regard du dommage causé, sont difficilement applicables aux prestataires de Cloud dont le service transite par Internet, en raison de l'absence de maîtrise de ce réseau par le prestataire.

1.2 La confidentialité des données

La confidentialité des données hébergées en Cloud constitue aujourd'hui le plus important des freins pour les entreprises désirant avoir recours à ce service. Le critère de confidentialité prend toute son importance lorsque les données hébergées présentent un contenu stratégique pour l'entreprise ou lorsqu'elles peuvent être considérées comme des données à caractère personnel. C'est ce dernier aspect qui a pour l'instant cristallisé l'essentiel des problèmes soulevés par le Cloud, bien que les données personnelles ne représentent qu'une partie des données concernées. Ce sont cependant celles qui ont le lien le plus étroit avec la vie privée, laquelle constitue un domaine éminemment sensible.

La confidentialité des données peut être remise en cause par des membres des services du prestataire ou de l'entreprise cliente, ainsi que par une personne totalement extérieure à ces services. Il convient donc de mettre en place une sécurisation particulièrement poussée de l'accès à ces données surtout si elles sont accessibles via Internet. L'une des solutions techniques envisageable est le chiffrement des données. Cette solution n'est cependant pas aisée à mettre en œuvre : outre que cette technique est parfois interdite par certaines législations, le prestataire peut vouloir imposer et gérer l'outil et les clés de chiffrement, ce qui lui permettrait d'avoir accès aux données en clair. La confidentialité de ces données, personnelles ou non, ne serait alors plus totalement assurée. Une telle méthode supposerait également que le déchiffrement soit réalisé chez le client et non chez le prestataire car celui-ci disposerait alors d'une copie des données.

La confidentialité des données peut également être malmenée par la réglementation applicable au prestataire, notamment si celui-ci est domicilié aux États-Unis.

Le « Patriot Act » américain[2] prévoit en effet que l'administration américaine peut à tout moment demander aux hébergeurs américains ou aux hébergeurs étrangers utilisant des Data centers sur le territoire américain, de leur fournir toutes les données qu'elles possèdent sur une personne, quel que soit le lieu de stockage de ces données. Cette demande doit en principe se faire via les autorités judiciaires américaines mais dans certains cas « urgents », l'administration peut se passer de l'intermédiaire judiciaire et s'adresser directement à l'hébergeur concerné. Le client quant à lui n'aura pas nécessairement connaissance de la demande faite par les autorités américaines. Quant à l'utilisation des données recueillies, bien qu'elle soit en principe limitée à la recherche d'activités terroristes, rien ne garantit qu'il n'en soit pas fait un usage différent, notamment à des fins économiques, lorsque la personne visée par la mesure a pour concurrents des entreprises américaines.

Si la sécurité et la confidentialité des données sont aujourd'hui nécessairement traitées par voie contractuelle, les engagements de niveau de services (Services Level Agreements ou SLAs) pesant sur le prestataire sont parfois difficiles à mettre en œuvre selon l'offre de Cloud choisie. La plupart des offres de Cloud prennent la forme de contrats d'adhésion, qui ferment toute possibilité de négociation entre le client et le prestataire. Cela est d'autant plus vrai en cas de Cloud public, l'offre étant alors standardisée et difficilement adaptable à chaque client. Le client doit alors définir son niveau d'exigences et évaluer les offres en fonction de celui-ci.

1.3 L'intégrité des données

Les prestataires de Cloud ont l'obligation de garantir l'intégrité des données hébergées.

Le principe d'intégrité présente deux aspects complémentaires : les données doivent être sauvegardées de manière à ce qu'aucune perte ne puisse intervenir mais elles ne doivent être conservées que pendant la durée déterminée par le client. L'intégrité peut être ébranlée par l'insuffisance de moyens techniques mis en œuvre, en particulier lorsque les données transitent par le réseau Internet.

L'une des possibilités pour limiter le risque d'atteinte à l'intégrité des données consiste à prévoir contractuellement la mise en place d'un système de double sauvegarde sur des serveurs distincts. Le contrat devrait également envisager un plan de réversibilité et de portabilité des données dans un format couramment utilisé.

2. Titre V du Patriot Act du 26 octobre 2001.

La réversibilité permet d'assurer le transfert du service de Cloud d'un prestataire à un autre en cas de besoin. Il convient alors de préciser les causes de réversibilité (défaillance du prestataire, fin du contrat, dysfonctionnements répétés…).

La durée de conservation des données doit être fixée par le client au regard des finalités pour lesquelles elles ont été collectées. Le prestataire s'engage alors à ne pas les conserver au-delà de la durée fixée ou après l'expiration du contrat. Le contrat peut également prévoir une obligation de restitution des données à l'issue du contrat ou en cas de rupture anticipée de celui-ci. Une fois la restitution opérée, les données détenues par le prestataire devront être détruites.

1.4 La traçabilité des données

Toute action sur un système informatique est en principe consignée dans un journal d'évènements (consultation, changement de configuration, administration…). Ces journaux sont généralement la propriété du fournisseur de Cloud. Le client doit alors prévoir contractuellement la possibilité d'accéder à ces journaux à tout moment de façon à suivre les actions effectuées sur les données, tant par le personnel de l'entreprise que par celui du prestataire. Les données générées par les journaux d'évènements doivent elles-mêmes remplir les conditions de disponibilité, d'intégrité et de confidentialité.

En cas de Cloud public, la consultation de ces données peut être compliquée par le fait qu'ils peuvent intégrer des données relatives à d'autres clients. Il appartient donc au prestataire de faire en sorte que les journaux transmis au client ne contiennent que les données le concernant.

2. La réglementation applicable au traitement des données

L'une des caractéristiques du Cloud est la grande dispersion des serveurs sur lesquels sont stockées les données. Ces serveurs peuvent être situés dans plusieurs pays, ce qui rend très difficile la localisation de ses données par le client. Or, certaines données sont soumises à une réglementation spécifique, particulièrement en ce qui concerne les données personnelles. La plupart des pays de l'Union européenne disposent de règles juridiques strictes concernant les données à caractère personnel, tant en ce qui concerne leur traitement que leur transfert. Dans le cas du Cloud, les données pouvant être localisées dans plusieurs pays, il est souvent très délicat pour le client d'assurer une protection adéquate de ces données en raison de la pluralité de législations pouvant trouver à s'appliquer.

L'utilisation et le traitement de données, qu'elles soient personnelles ou non, sont en principe sous le contrôle du responsable de traitement, lequel devra répondre de tout usage illicite des informations. L'identification du responsable de traitement constitue l'un des indices permettant de déterminer la loi applicable au traitement des données et sa localisation représente un élément essentiel de définition des règles applicables aux transferts internationaux de données.

2.1 La loi applicable au traitement des données

L'article 3 de la loi Informatique et libertés[3] définit le responsable de traitement comme la personne, l'autorité publique, le service ou l'organisme qui détermine les finalités et les moyens du traitement des données. Cette définition est reprise de façon quasi-identique dans le projet de règlement sur les données personnelles[4].

Lorsqu'un client fait appel à un prestataire de service, il est en principe admis qu'il sera responsable du traitement des données puisqu'il les collecte et détermine les finalités et les moyens de leur traitement. Le prestataire de service sera quant à lui considéré comme sous-traitant puisqu'il agit normalement pour le compte et sur les instructions du client.

Lorsque la répartition des rôles entre client et prestataire est clairement établie, il est alors possible d'instaurer une présomption de sous-traitance pesant sur le prestataire. Cette situation se rencontre généralement dans les cas du Cloud privé, spécialement créé pour un client déterminé, lequel garde la maîtrise de la réalisation du service par le prestataire. La mise en place d'une présomption de sous-traitance avait été proposée par la CNIL en 2012[5] afin de faciliter l'identification du responsable de traitement mais elle s'avère inadaptée au cas du Cloud public. En effet, la plupart des contrats proposés dans ce cadre peuvent être qualifiées de contrats d'adhésion dans lesquels le client, responsable de traitement, n'a pas la possibilité de négocier avec le prestataire et de faire respecter des ins-

3. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF 7 janvier 1978, p. 227.

4. Article 4(5) du projet de règlement : le responsable du traitement est « l*a personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités, les conditions et les moyens du traitement de données à caractère personnel* ».

5. Synthèse des réponses à la consultation publique sur le Cloud computing lancée par la CNIL d'octobre à décembre 2011 et analyse de la CNIL, juin 2012.

tructions et des moyens de contrôle. Le projet de règlement met en place un statut légal du sous-traitant. Celui-ci ne peut agir que sur instruction du responsable de traitement et ses obligations doivent être précisées dans une convention liant les deux parties. L'article 26 du projet énumère une série non exhaustive de mentions devant figurer sur la convention, parmi lesquelles l'obligation de confidentialité, l'obligation de prendre toutes les mesures nécessaires à la sécurité des données, l'obligation de conserver une trace documentaire de toutes les instructions données par le responsable de traitement, etc. Lorsque le prestataire de Cloud dispose d'une forte autonomie et ne rentre pas dans le cadre de la sous-traitance envisagée par le projet de règlement, il pourrait se voir reconnaître la qualité de responsable de traitement conjointement avec le client[6]. En cas de responsable de traitement conjoint, les parties devront définir, par voie d'accord, leurs obligations respectives, notamment en ce qui concerne l'exercice des droits des personnes concernées[7]. En tout état de cause, le prestataire de Cloud sera responsable de traitement dès lors qu'il utilise les données personnelles qui lui ont été confiées par les clients à des fins différentes de celles prévues dans le contrat de prestation de service. Une autorisation du client et éventuellement des personnes concernées sera alors nécessaire pour procéder à un traitement distinct.

Le projet de règlement sur la protection des données devrait permettre de mieux définir les obligations et les responsabilités subséquentes des différents acteurs du Cloud mais il ne résout pas toutes les difficultés liées notamment aux règles applicables aux transferts internationaux de données.

Le traitement et l'utilisation des données étant en principe soumis aux instructions du client, il semblerait logique que celui-ci soit déclaré responsable de tout usage illicite de celles-ci en sa qualité de responsable de traitement, et que l'on applique alors la loi du lieu d'établissement du client. Cette solution à priori évidente ne tient cependant pas compte du fait que le responsable de traitement peut être établi dans un Etat et utiliser des moyens de traitement situés dans un autre Etat. Or, certaines règlementations telles que la loi française peuvent trouver

6. Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE n° L 281, p. 31 : L'article 2d) désigne comme responsable du traitement la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel (…).

7. Projet de règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, COM (2012) 11 final, article 24.

à s'appliquer lorsque les moyens de traitement des données sont localisés en France, même si le responsable de traitement est établi dans un autre pays[8]. On pourrait dès lors potentiellement appliquer plusieurs règlementations aux mêmes faits. La solution consistant à ne retenir que la loi du responsable de traitement à l'exclusion de celle des moyens de traitement pourrait favoriser certaines pratiques de *forum shopping* déjà bien présentes dans d'autres secteurs. Le *forum shopping* consiste pour des entreprises à s'implanter dans un pays plutôt qu'un autre en considération des avantages qu'il peut retirer de la législation de ce pays. Pour limiter tant que faire se peut le risque de *forum shopping*, le projet de règlement distingue trois situations dans lesquelles il peut trouver à s'appliquer au traitement de données personnelles[9] :

- Lorsque le traitement des données est effectué dans le cadre de ses activités par le responsable de traitement ou un sous-traitant établis dans l'Union européenne. On retient donc ici la loi du pays d'établissement de l'entreprise.

- Lorsque le traitement des données est effectué par un responsable de traitement établi hors de l'Union européenne mais que les données en cause concernent des personnes ayant leur résidence sur le territoire de l'Union, si les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, ou à l'observation de leur comportement. La Commission a ici retenu le critère du ciblage, qui prend en compte les personnes visées par le traitement des données, pour déterminer la loi applicable. Cette disposition vise essentiellement à assurer une protection homogène des consommateurs résidant dans un pays de l'Union européenne et dont les habitudes de consommation font l'objet d'études de la part des fournisseurs de produits ou de services.

- Lorsque le traitement des données est effectué par un responsable de traitement établi hors de l'Union européenne mais que la législation d'un Etat membre de l'Union s'applique en vertu du droit international public.

2.2 Les transferts internationaux de données

Le stockage des données sur des serveurs localisés dans une multitude de pays peut complexifier à l'extrême la protection juridique des données pour le client, en particulier lorsque ces données sont collectées, traitées et/ou utilisées par des intervenants établis dans différents États.

8. Loi Informatique et libertés, préc., article 5-I-2°.
9. Projet de règlement préc., art. 3.

Le projet de règlement sur les données personnelles, qui abroge la directive 95/46/CE jusque-là applicable, encadre les transferts internationaux de données personnelles à destination de pays tiers, c'est-à-dire non membres de l'Union.

Aucune autorisation de transfert ne sera nécessaire entre deux responsables de traitement ou entre un responsable de traitement et un sous-traitant établis tous deux dans des pays où le niveau de protection est considéré comme adéquat par la Commission européenne (article 41-1 du projet de règlement). Ces pays figurent sur une liste établie par la Commission et comprennent les 31 Etats membres de l'Espace économique européen ainsi que Andorre, l'Argentine, l'Australie, le Canada, Guernesey, l'île de Man, les îles Féroé, Israël, Monaco et la Suisse.

Lorsque les entreprises réalisent des transferts de données vers des pays ne figurant pas sur cette liste ou lorsque les données, bien que demeurant physiquement sur le territoire d'un de ces pays, sont traitées ou utilisées par des personnes se trouvant dans des pays « tiers », les différents partenaires doivent mettre en place des instruments à même d'assurer une protection appropriée des données. Si les instruments mis en place par les parties ne sont pas juridiquement contraignants, le transfert sera soumis à une autorisation préalable de l'autorité nationale. Lorsqu'elle est concernée par des transferts internationaux de données, l'entreprise peut recourir à deux instruments principaux : les Binding Corporate Rules (BCR) et les modèles de contrats de transfert proposés par la Commission (article 42 et suivants du projet de règlement).

Les BCR sont des règles de bonne conduite qui définissent la politique interne d'un groupe en matière de transfert de données personnelles hors de l'UE. Sont principalement concernées les entreprises exportant des données depuis leur siège social ou leurs filiales situées dans l'UE, à destination de pays hors UE n'assurant pas un niveau de protection équivalent à celui de l'Union européenne. Une fois élaborées, les BCR doivent être validées par les autorités de protection des données des Etats concernés par les transferts[10]. Dans l'Espace économique européen, une grande majorité des autorités de protection des données ont mis en œuvre une procédure d'instruction simplifiée, fondée sur le principe de reconnaissance mutuelle : lorsqu'une autorité valide les BCR au motif qu'elles apportent un niveau de protection suffisant, les autres autorités approuvent alors automatiquement ces BCR.

10. En France, cette autorité est représentée par la CNIL.

Le principe de reconnaissance mutuelle permet de gagner un temps précieux dans le processus de validation des BCR[11].

La CNIL a établi en 2008 un cadre pour les règles d'entreprise contraignantes (BCR) permettant aux entreprises intéressées d'avoir une idée du contenu et de la structuration de telles règles[12].

Si elles n'envisagent pas d'adopter des BCR, les entreprises peuvent se tourner vers les modèles de contrats de transfert établis par la Commission. Ces contrats dépendent du type de transfert envisagé par l'entreprise.

Lorsque le client transfère des données à un prestataire de Cloud établi hors de l'Union européenne et agissant en qualité de sous-traitant, ils peuvent envisager d'adopter les clauses contractuelles type de 2010[13].

Lorsque le client transfère des données à un prestataire de Cloud établi hors de l'UE et agissant en tant que responsable de traitement, ils peuvent envisager l'adoption des clauses contractuelles type de 2001 ou 2004[14].

Lorsque le client transfère des données à un prestataire de Cloud établi dans l'UE et agissant en qualité de sous-traitant, lequel transfère ensuite ces données à un sous-traitant établi hors de l'UE, les parties peuvent soit adopter les clauses contractuelles type de 2010 (entre le responsable de traitement et le sous-traitant établi hors de l'UE), soit adopter un contrat de mandat, soit signer un contrat tripartite. L'adoption de ces clauses suppose bien évidemment que le sous-traitant établi dans l'UE informe le client de la désignation d'un second sous-traitant établi hors Union. L'idéal dans un tel cas est que le client dispose d'un droit de regard ou de veto sur le choix du second sous-traitant.

Si le Cloud computing permet à l'entreprise de réaliser des économies, du moins à court terme, il présente cependant de nombreux risques dont il ne convient de ne pas ignorer l'importance.

11. En 2012, les autorités de protection des données ayant adhéré au principe de reconnaissance mutuelle étaient : l'Allemagne, l'Autriche, la Belgique ? LA Bulgarie ? Chypre, l'Espagne, l'Estonie, la France, la Grande-Bretagne, l'Irlande, l'Islande, l'Italie, la Lettonie, le Lichtenstein, le Luxembourg, Malte, la Norvège, les Pays-Bas, la République Tchèque, la Slovaquie, la Slovénie.

12. *http://www.cnil.fr/fileadmin/documents/Vos_responsabilites/Transferts/Trame_fr.pdf*

13. Clauses contractuelles type 2010, JOUE n° L39, p. 5.

14. Clauses contractuelles type 2004, JOUE n° L285, p. 74. Ces documents sont également disponibles sur le site de la CNIL : *http://www.cnil.fr/vos-obligations/transfert-de-donnees-hors-ue/contrats-types-de-la-commission-europeenne/*

Le premier de ces risques est bien évidemment relatif à la sécurité des données et à leur confidentialité. L'utilisation du réseau Internet pour accéder aux données hébergées expose celles-ci à des risques d'intrusion supplémentaires. De plus, les entreprises utilisatrices de Cloud computing n'ont plus la possibilité de vérifier l'utilisation qui peut être faite de leurs données. Les contrats conclus entre le client et le prestataire de Cloud peuvent certes déterminer les obligations pesant sur le fournisseur de Cloud en ce qui concerne l'utilisation des données mais ils ne représentent qu'une garantie limitée. En effet, si une utilisation illicite est constatée, quelles sanctions autres que des sanctions financières, qui ne couvriront pas nécessairement le préjudice réellement subi ?

Un second risque important est la dépendance du client envers la qualité du réseau nécessaire pour accéder aux données. Or, aucun fournisseur de Cloud ne peut garantir une disponibilité totale du réseau, ce qui peut représenter pour l'entreprise une perte commerciale importante. Il est à cet égard intéressant de regarder les statistiques effectuées par l'International Working Group of Cloud Resiliency sur les défaillances de services de Cloud[15].

Un autre risque enfin, souvent sous-estimé, est celui lié aux difficultés à quitter ces services de Cloud et au coût parfois élevé de la réversibilité. Le client n'ayant plus la maîtrise des services informatiques, il peut se trouver bloqué au moment d'exporter les données hébergées en Cloud vers d'autres services. Cela est particulièrement vrai lorsque le fournisseur de Cloud pratique *l'enfermement propriétaire*, c'est-à-dire qu'il crée une particularité volontairement non standard dans son système (logiciel, machine, etc.), empêchant ainsi le client d'utiliser ses données avec les produits ou services d'un autre fournisseur. C'est un excellent moyen de rendre une clientèle captive, qui a déjà été mis en œuvre avec succès dans de nombreux secteurs. Les contrats de Cloud proposés aujourd'hui ne permettent pas aux entreprises de s'opposer à ces pratiques, même s'il est parfois possible de négocier des clauses de réversibilité.

Dans un marché du Cloud computing en pleine croissance[16], il est très important pour l'entreprise de bien évaluer les objectifs poursuivis et de procéder à une analyse des risques pour les différentes solutions de Cloud envisagées. Il est donc urgent de…prendre son temps.

---

15. *http://iwgcr.org*

16. D'après le cabinet IDC, le marché français du Cloud computing a progressé de 46 % en 2012 et devrait poursuivre sa croissance jusqu'en 2016. La part du Cloud computing devrait représenter 12% des dépenses informatiques des entreprises en 2016, contre 3 % en 2011 : *http://www.usine-digitale.fr/article/le-cloud-computing-pesera-12-des-depenses-informatiques-des-entreprises-en-2016.N198077*.

Bibliographie

Belouezzane S., Puybareau F. 2012, « Cloud computing, les enjeux de l'informatique en nuage », Cahiers du « Monde » n° 20910, *Le Monde* du 12 avril 2012.

CIGREF, IFACI, AFAI (2013), Cloud computing et protection des données.

CNIL (2012), Synthèse des réponses à la consultation publique sur le Cloud computing lancée par la CNIL d'octobre à décembre 2011 et analyse de la CNIL.

CNIL (2012), Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing.

INHESJ, CIGREF (2012), Protection de l'information d'entreprise et Cloud computing.