La dématérialisation du dépôt : l'exemple du contrat de *cloud computing*

par Antoine **Gendreau**
Avocat associé, Osmose

Le *cloud computing* désigne un mode d'externalisation de tout ou partie du système d'information de l'entreprise. Il vise une réalité à géométrie variable. La prestation peut couvrir l'hébergement de données, mais également différentes « couches » du système d'information allant de l'infrastructure applicative à l'infrastructure technique[1].

La valeur ajoutée du service réside dans le fait que le client rémunère le prestataire en fonction de la consommation qu'il fait des ressources informatiques mises à sa disposition. Cette valeur ajoutée peut être proposée car l'infrastructure sur laquelle s'appuie le prestataire est mutualisée sur des équipements localisés en différents endroits, si bien que la dimension géographique et physique de ce qui est dédié au client passe au second plan[2].

Dans un premier temps, la technologie est donc perçue de façon très favorable. Elle permet une gestion très souple dans la mesure où la ressource facturée correspond à la ressource consommée et non à une immobilisation susceptible d'être inutilement surdimensionnée ou trop rapidement sous-dimensionnée.

Dans un second temps, elle peut entraîner une certaine méfiance, car elle crée une dépendance et un sentiment de dépossession des actifs immatériels de l'entreprise, sentiment de dépossession supérieur à celui qui existait dans les formes plus traditionnelles de l'infogérance. Quoique cette dépendance existât déjà dans les anciens modèles d'externalisation, le *cloud computing* vient renforcer cette perception en raison du caractère « occulte » des moyens employés.

Pour mesurer l'étendue des obligations respectives des parties, c'est sans succès que l'on aura recours aux catégories de contrats spéciaux prévues par le code civil. Soit elles ne sont pas appropriées, soit elles sont insuffisantes. Il serait tentant de faire entrer certains aspects du contrat relatifs à l'hébergement des données dans la catégorie du contrat de dépôt. En effet, le client va confier à un tiers des données dont il est propriétaire afin que le prestataire les conserve sur ses serveurs. La doctrine unanime considère que tel ne peut pas être le cas s'agissant des biens meubles incorporels[3]. De plus, le contrat de *cloud computing* ne porte pas exclusivement sur un hébergement de données. Souvent, il comprend également la concession de droits d'usage sur des applications, des actions de maintenance, etc. Pour autant, les parties pourront utilement se rapporter conventionnellement à cette qualification pour identifier certaines dispositions relatives aux obligations du déposant et du dépositaire[4]. En revanche, le contrat peut être qualifié de contrat de louage d'ouvrage au sens de l'article 1710 du code civil, plus communément appelé, désormais, « contrat de prestation de service ». Les conséquences de cette qualification sont en revanche de peu de secours pour déterminer le régime du contrat. C'est dès lors aux parties de détailler un contrat qui, par le faible nombre de dispositions supplétives et le caractère novateur des prestations, va nécessiter une rédaction longue et minutieuse. Cette rédaction est d'autant plus cruciale que le client, non sans raison, est désireux de compenser la perte de maîtrise de l'environnement technologique par la mise en place d'un dispositif contractuel de contrôle.

La question se pose donc de savoir quels sont les mécanismes contractuels qui doivent être mis en place et quelle peut être leur efficacité. Le contenu du contrat est en partie dicté par certaines obligations réglementaires. Quand bien même l'entreprise cliente ne ressortirait pas en totalité au champ d'application de ces textes, les problématiques qu'ils traitent constituent un excellent point de départ pour établir ce contrat d'externalisation.

Le point de départ : les contraintes réglementaires

Le contenu du contrat est dicté par des contraintes juridiques générales et sectorielles.

Les contraintes générales

L'article 4 du règlement du 27 avril 2016 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 (« RGPD »)[5] dispose que le « responsable du traitement » est celui qui, « seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement » tandis que le « sous-traitant » est celui qui « traite des données à caractère personnel pour le compte du responsable du traitement ». Le premier réflexe est de considérer le prestataire comme un sous-traitant au sens du RGPD, qualité que les contrats rappellent très fréquemment. Il faut cependant souligner que cette qualification n'est pas subordonnée à la seule volonté des parties. C'est en fonction du rôle dévolu à chacun que l'analyse pourra être

(1) Dissociation des prestations de SaaS (Software as a Service), PaaS (Plateforme), IaaS (Infrastructure) : National Institute of Standards and Technology (« The NIST Definition Cloud Computing »)(https://www.nist.gov/).

(2) Commission générale de terminologie et de néologie / Vocabulaire de l'informatique (JO 6 juin 2010) : « L'informatique en nuage est une forme particulière de gérance de l'informatique, dans laquelle l'emplacement et le fonctionnement du nuage ne sont pas portés à la connaissance des clients. »

(3) G. Brunaux « *Cloud computing*, protection des données : et si la solution résidait dans le droit des contrats spéciaux ? » D. 2013. Chron. 1158 ; R. de Quenaudon et Ph. Schultz, J.-Cl. Civ., art. 1915 à 1920, « Dépôt – Principes Généraux », nos 16 s.

(4) Par exemple les articles 1929 et 1944 du code civil.

(5) Règl. (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, JOUE, n° L 119, 4 mai.

confirmée. Il conviendra donc de vérifier si le prestataire ne pourrait pas être considéré comme un coresponsable de traitements.
Le sous-traitant doit être lié au responsable du traitement par « un contrat ou un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre »[6]. Le RGPD fixe, de façon non limitative, un certain nombre de dispositions relatives au contenu de cet acte. Nous n'en citerons que trois, mentionnées à l'article 23, § 3. Cet article dispose que le contrat conclu doit stipuler que le sous-traitant « ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ». Bien qu'il soit fréquemment avancé que le territoire sur lequel s'exerce la prestation est indéfini, le « nuage » n'échappe pas à l'attraction terrestre. Les données sont bien naturellement hébergées sur des équipements localisés dans certains États qui doivent présenter un niveau de protection adéquat. Or, entre la date d'expiration des accords du *Safe Harbor* et l'adoption du *Privacy Shield*, il est fort à craindre que nombre de données à caractère personnel ont été stockées de façon « inappropriée » sur des serveurs situés aux États-Unis[7].

Bien qu'il soit fréquemment avancé que le territoire sur lequel s'exerce la prestation est indéfini, le « nuage » n'échappe pas à l'attraction terrestre. Les données sont bien naturellement hébergées sur des équipements localisés dans certains États qui doivent présenter un niveau de protection adéquat

Le contrat doit stipuler que le sous-traitant prend l'ensemble des mesures « techniques et organisationnelles appropriées » permettant d'assurer la sécurité des traitements, et, à ce titre, des moyens « permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement »[8]. Nous mesurons l'étendue des obligations de conseil et de mise en garde que devrait souscrire le sous-traitant.
De même, le contrat doit stipuler que le sous-traitant « aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont il est saisi par les personnes » dont les données sont collectées lorsqu'elles exercent leurs droits.
Rappelons que les infractions à certaines dispositions du RGPD relatives aux droits dont bénéficient les personnes concernées font l'objet d'amendes administratives pouvant s'élever jusqu'à 20 000 000 € ou jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.
La nécessité pour l'entreprise de faire face à ses obligations réglementaires de résultat implique donc la mise en place d'un niveau de service exigeant.

Les contraintes sectorielles

Les réglementations de certains secteurs d'activité ou de certains types d'exercice professionnel viennent imposer des règles complémentaires qui doivent trouver leur traduction contractuelle.
Dans le domaine de la santé, rien ne s'oppose à ce que des données de santé soient hébergées dans une infrastructure de type *cloud* dès lors que cet hébergement répond au dispositif du « décret hébergeur » fixant notamment les conditions auxquelles est subordonné l'agrément de l'hébergeur. Le dossier d'agrément déposé par l'hébergeur de données de santé comprend un contrat type à conclure entre lui et le déposant. Le régime de ce contrat est en partie dicté par les dispositions de l'article R. 1111-13 du code de la santé publique. Cet article fixe une liste des différentes clauses qui doivent figurer dans la convention. Ainsi le contrat doit-il, entre autres clauses, déterminer les obligations de l'hébergeur « en cas de modifications ou d'évolutions techniques introduites par lui » ou encore les conditions de recours à des prestataires techniques externes et « les engagements de l'hébergeur pour que ce recours assure un niveau équivalent de garantie au regard des obligations pesant sur l'activité d'hébergement ».
Dans le domaine bancaire, l'arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement[9] impose que les entreprises du secteur s'assurent que leurs prestataires externes « mettent en œuvre des mécanismes de secours en cas de difficulté grave affectant la continuité du service ». Ces textes sont traduits par l'établissement de plans de reprise d'activité et un plan de continuation d'activité (PRA/PCA), par exemple.
Concernant plus particulièrement les sociétés commercialisant des biens et des services aux consommateurs, l'article L. 224-42-1 du code de la consommation créé par la loi du 7 octobre 2016 pour une République numérique reprend un dispositif du RGPD[10] imposant aux entreprises de disposer des mesures techniques permettant au consommateur d'exercer son droit à la « récupération de l'ensemble de ses données »[11] (mesure dite de « portabilité des données »). Le contrat devra bien entendu traiter ce point.
En réalité, les problématiques qu'abordent les réglementations sectorielles ou générales relèvent d'une approche saine du contrat d'externalisation. Leur prise en compte constitue un très bon point de départ pour la formalisation de la convention quand bien même l'entreprise cliente ne ressortirait pas à une réglementation sectorielle spécifique.

Au-delà des contraintes réglementaires

Contexte

Il faut au préalable relever que les contrats de *cloud* constituent souvent un exemple typique de contrat d'adhésion, « dont les conditions générales, soustraites à la négociation, sont déterminées à l'avance par l'une des parties »[12], en l'occurrence le prestataire. Cette adhésion se vérifie non seulement au moment de la conclusion du contrat, mais également au cours de son exécution. C'est ainsi que l'Autorité de contrôle prudentiel et de résolution faisait observer que « le principal obstacle semble prendre sa

(6) RGPD, art. 28, §3.
(7) Et il n'est pas exclu que cette situation puisse se reproduire : C. Castets-Renard, « Adoption du *Privacy Shield* : des raisons de douter de la solidité de cet accord », Dalloz IP/IT 2016. 444.
(8) RGPD, art. 32.
(9) JO 5 nov.
(10) Le RGPD entre en vigueur le 25 mai 2018.
(11) L. n° 2016-1321 du 7 oct. 2016 pour une République numérique, art. 48, créant l'article L. 224-42-1 du code de la consommation (lequel reprend l'article 20 du RGPD). Ce texte entre en vigueur à la même date que le RGPD.
(12) C. civ., art. 1110 et 1171.

source dans la très faible marge de négociation lors de la contractualisation de l'offre de service, majoritairement générique »[13]. Cette standardisation est souvent la contrepartie de ressources mutualisées[14].
Certains prestataires se réservent en outre le droit de modifier unilatéralement certaines fonctionnalités du service, le niveau de service offert et, d'une façon générale, le contrat, l'utilisation du service étant réputée constituer une acceptation de ces modifications. Le prestataire indique qu'il incombe au client de vérifier régulièrement en ligne les modifications intervenues[15]. Si le client dispose de la possibilité de résilier le contrat en cas de « modification substantielle », cette faculté reste théorique. Outre le fait que cette pratique manifeste un déséquilibre peu souhaitable, elle peut s'avérer peu compatible avec certaines contraintes réglementaires. Ainsi l'arrêté du 3 novembre 2014 précité prévoit-il que les entreprises assujetties s'assurent que leurs prestataires externes « ne peuvent imposer une modification substantielle de la prestation qu'ils assurent sans l'accord préalable de l'entreprise assujettie »[16].
Il existe dans cette clause, sur la légitimité de laquelle on doit s'interroger, une certaine réalité, à savoir la recherche de souplesse dans l'évolution du lien contractuel. En effet, les évolutions technologiques ou légales qui peuvent s'imposer aux entreprises offrant ou bénéficiant des prestations de *cloud* doivent pouvoir s'insérer dans un cadre contractuel évolutif.

La qualité de la prestation

La qualité de la prestation fait généralement l'objet d'un document spécifique qui détermine les niveaux de service. Il est généralement intitulé « Service Legal Agreement » (SLA). C'est, indirectement, à ce document que fait référence l'article R. 1111-13 du code de la santé publique en exigeant que le contrat d'hébergement stipule les « indicateurs de qualité et de performance permettant la vérification du niveau de service annoncé, ainsi que de la périodicité de leur mesure ». Le SLA recense les principales caractéristiques techniques des engagements. Il détermine notamment le taux de disponibilité, c'est-à-dire le temps pendant lequel les utilisateurs peuvent utiliser les applications et les données, ainsi que les modalités de mesure et de calcul de ce taux, le temps de réponse pour effectuer les transactions informatiques, le nombre maximal d'interruptions de service, le temps maximal de reprise d'activité, etc. Pour qu'une négociation avance de façon efficace, il faudrait laisser de côté les débats portant sur la qualification des obligations de moyens et de résultat pour ne se concentrer que sur les critères auxquels est subordonnée la vérification de la conformité de la prestation et sur les causes d'exonération qui peuvent être invoquées. Le SLA est généralement sanctionné par le jeu de pénalités. Il faut s'assurer que le mode de calcul et le plafonnement conservent un caractère dissuasif si le client souhaite exercer une pression contribuant à lui permettre de remplir ses obligations réglementaires.

La sécurité

Quoique ces sujets ne relèvent pas tous de la même clause, on comprendra sous ce chapitre différents enjeux qui ont trait aux deux sujets suivants : d'une part, la conservation et les « transactions » ou traitements portant sur les données de telle sorte que leur intégrité et leur confidentialité soient assurées ; et, d'autre part, la mise en place de procédures en cas de suspension ou d'indisponibilité des équipements de telle sorte que, autant que faire se peut, le client puisse bénéficier des services sans solution de continuité (plan de continuité d'activité et plan de reprise d'activité).

Les audits

Les mécanismes contractuels de sanction ne sont pas suffisants. Tout aussi importantes sont les actions préventives qui, si elles ne sont pas imposées à l'initiative du client, peuvent être rendues obligatoires sur le plan réglementaire[17]. L'exercice de cette clause ne doit pas rester théorique. À ce titre, la répartition des coûts engendrés par les mesures d'audit doit être précisée, de telle sorte que les frais induits ne dissuadent pas le client d'y procéder, les audits étant généralement à la charge de celui qui les diligente. Il importe que les audits puissent s'appuyer sur des comptes rendus détaillés des prestataires portant par exemple sur l'adéquation des mesures techniques de sécurité, de telle sorte que le client puisse déterminer les contrôles qu'il va choisir d'effectuer avec l'aide de ses conseils dont les conditions d'intervention à ses côtés doivent être précisées.

L'expiration du contrat

L'expiration normale ou anticipée du contrat, quelle qu'en soit la cause, donne lieu aux opérations de réversibilité dont le but est de permettre au client de « réinternaliser » ce service ou d'en faire assurer l'exécution par un nouveau prestataire[18]. Cette opération a pour fonction primaire d'assurer la migration des données.
La nécessité de prévoir des conditions de réversibilité adéquates est illustrée par une affaire qui a opposé l'UMP[19] à la société Oracle France avec laquelle elle avait conclu un contrat de SaaS[20] concernant la mise à disposition d'un logiciel de gestion d'une base de données nominatives. L'UMP avait décidé d'assurer la réversibilité au bénéfice d'un autre prestataire à l'expiration du contrat. Se trouvant dans l'impossibilité de récupérer les données en raison d'une anomalie « en cours de correction »[21], l'UMP avait assigné en référé Oracle devant le tribunal de grande instance de Nanterre. Oracle invoquait en défense notamment le fait que le contrat ne prévoit pas de délai de correction des anomalies. Par une ordonnance du 30 novembre 2012, le tribunal constate que « la société Oracle ne peut soutenir, de bonne foi, qu'elle ne manquerait pas à ses obligations contractuelles si elle ne permettait pas à l'UMP de bénéficier en temps utile de ses données pour permettre à son nouveau prestataire de les exploiter et d'être opérationnel dès la fin de sa propre prestation » et enjoint le prestataire sous astreinte soit de fournir à l'UMP les moyens techniques de nature à lui permettre sans délai l'exportation de l'ensemble de ses données nominatives hébergées, soit

(13) ACPR, « Les risques associés au *Cloud computing* », Analyses et synthèse, n° 16, juill. 2013.
(14) La contrainte n'est pas de même nature en cas de *private cloud*.
(15) https://aws.amazon.com/fr/agreement ; https://www.dropbox.com/privacy#business_agreement.
(16) Communication de la Commission du 27 sept. 2012, COM(2012) 529 : « *However, currently the greater flexibility of cloud computing as compared to traditional outsourcing is often counterbalanced by reduced certainty for the customer due to insufficiently specific and balanced contracts with cloud providers.* »
(17) Arr. 3 nov. 2014, art. 239 ; RGPD, art. 28 3. h).
(18) On parle dans ce cas de « transférabilité ».
(19) Il s'agit du parti politique « Union pour un mouvement populaire », devenu « Les Républicains ».
(20) *Software as a Service*.
(21) Anomalie affectant une fonctionnalité d'exportation des données.

de garantir à l'UMP qu'elle assurera gratuitement le service pendant deux mois à compter du jour où elle sera en mesure de procéder à l'exportation des données.
L'enjeu ne peut pas être résumé à une question de rapatriement de données, dont il n'est généralement pas discuté qu'elles sont la propriété du client. En revanche, les droits de propriété intellectuelle grevant la structure et le mode de gestion de la base de données peuvent appartenir au prestataire et les droits d'utilisation conférés au client ne pas survivre au contrat de *cloud computing*. La question que doit traiter le contrat est moins celle du principe de réversibilité que celle de son étendue et de ses modalités. La mise en place d'une procédure de réversibilité, régulièrement mise à jour afin de s'adapter aux évolutions techniques du contrat, la détermination du format de restitution des données et de la réalisation des programmes de migration, les modalités techniques et financières d'assistance post-contractuelles (« post termination assistance ») doivent être précisées. Il faut souligner que les détails techniques de réalisation des opérations de réversibilité donnent souvent lieu à des descriptions minutieuses. Il faut stipuler au contrat un certain nombre de principes généraux fixant les objectifs de chacune des parties afin que, en cas d'obsolescence des descriptions techniques, les bases d'une interprétation des contours de la volonté commune des parties puissent permettre de pallier les éventuelles failles.

L'efficacité des contrats

Comme pour toute convention, l'efficacité des engagements pris réside dans la capacité à en faire assurer l'exécution en cas d'infraction. Or, dans le cas où le contrat de *cloud computing* est confié à certains des acteurs les plus importants du marché, notamment nord-américains, la compétence des tribunaux du prestataire est retenue et la loi du for applicable au contrat. Dès lors, les possibilités dont dispose le client pour faire assurer la bonne exécution des engagements pris par le prestataire et dont certaines lui sont imposées par des contraintes réglementaires sévèrement sanctionnées restent souvent théoriques.
Dès lors, si le client souhaite préserver par la loi du contrat l'indépendance qu'il perd sur le plan technologique, parmi ceux qui conduisent au choix d'un prestataire de *cloud computing*, les critères juridiques doivent prendre une importance toute particulière dès la phase de lancement de l'appel d'offres.