Contrats de prestations informatiques : quelques précautions juridiques

Les prestations informatiques couvrent un panel de services toujours plus important. La sécurité de l'information et des SI en fait partie. Les clauses de sécurité constituent dans certains contextes des engagements de résultat.

Les auteurs

Eric A. CAPRIOLI,
Avocat à la Cour, Docteur en droit, Vice-Président du CESIN.

Pascal AGOSTI
Avocats associés, Docteurs en droit

www.caprioli-avocats.com

En cette période de crise économique, les relations avec les prestataires de services informatiques subissent de profondes évolutions. De nouvelles formes de prestations informatiques font jour, portées le plus souvent par des prestataires étrangers (SAP, IBM, Oracle, Google...) : le SaaS (Software as a Service), le PaaS (Platform as a Service), le IaaS (Infrastructure as a Service), le Cloud Computing et autres termes techniques renvoyant à une externalisation des ressources informatiques sont devenues le langage quotidien des DSI, RSSI et Directions des Achats.

En outre, les prestations informatiques couvrent un panel de services toujours plus important. La sécurité de l'information et des SI en fait partie. Que ces prestations soient externalisées ou au contraire internalisées, elles doivent être étudiées au regard du droit des contrats informatiques même si certaines spécificités liées au caractère sensible du domaine (qui touche à des intérêts vitaux de la Nation ainsi que de l'entreprise) nécessitent certaines précisions.

Quelle marge de négociation sur le contenu contractuel ?

Les Contrats SaaS sont souvent des contrats d'adhésion. Dès lors, les Prestataires ont tendance à vouloir imposer certaines clauses sans négociations avec le Client, (hormis l'objet, le périmètre et les tarifs). **Si cette démarche peut se justifier pour des prestations standardisées (ex : accès à un Cloud public...), elle devient purement commerciale pour des prestations taillées sur mesure pour certains clients.** Dans tous les cas, un audit des offres SaaS proposées devra être établi en fonction de critères économiques et techniques/sécurité mais aussi en fonction d'exigences juridiques et de conformité légale. L'objectif sera de déterminer les conditions d'engagements acceptables pour le client et de ce fait, certaines clauses seront plus à même d'assurer la sécurité juridique du client et de ses intérêts.

Attention à certaines clauses du Contrat

Confrontée à cette situation, l'entreprise cliente doit porter une attention particulière au contrat d'adhésion qu'il devra auditer avant une souscription (lorsqu'il ne dispose d'aucune possibilité de négociation eu égard au poids du prestataire) ou au contrat informatique (qu'il devra négocier). Quelle que soit l'hypothèse, **de nombreuses clauses ou document devront être auditées par les services juridiques et techniques compétents pour être sûr de la conformité des prestations avec l'environnement interne et externe du système d'information Client.**

Quel Droit applicable ?

La loi applicable et le tribunal compétent doivent être désignés dans le contrat. Sans cette précaution fondamentale, chaque Partie pourrait réclamer défendre ses intérêts devant ses juridictions nationales, par essence plus favorables à ses ressortissants et demander l'application de sa loi. Rappelons que bon nombre de prestataires SaaS sont anglo-saxons. Les frais de justice dans ces pays sont vite prohibitifs et doivent être envisagés au moment du choix du prestataire. Lors d'un audit d'offres de SaaS, ce critère revêt une importance considérable (il constitue un coût caché loin d'être négligeable).

Une mutation des clauses de responsabilité et des modalités de réparation (pénalités)

Le contenu des clauses de limitation de responsabilité a évolué depuis quelques jurisprudences retentissantes. Ainsi, une décision (Cass. com, 29 juin 2010, Faurecia c/Oracle) a rappelé que le **manquement à une obligation essentielle ne suffit pas à écarter la clause limitative de responsabilité.** La clause ne doit toutefois pas amener le prestataire à s'affranchir de toute contrainte sérieuse à l'encontre de son client (par exemple, une clause limitant sa responsabilité en termes de restitution de données lorsqu'il a pour mission principale de les archiver...).

A la lumière de cette jurisprudence, les négociateurs de contrats informatiques doivent prendre la précaution de mieux préciser **l'assiette de réparation** (prix perçu, sommes versées par le client dans le cadre d'un projet informatique...) et prendre garde à certaines assimilations pour le moins hasardeuses (par exemple, intégrer comme plafond de responsabilité le montant de couverture prévu dans la police d'assurance ou intégrer les sommes dûes au titre de la garantie en contrefaçon dans ce plafond).

En outre, souvent, les contrats informatiques prévoient en Annexe des Conventions de service (ou Service

Level Agreement) où le non-respect des engagements quantitatifs (taux de disponibilité du service, de performance, niveaux d'opérations ...) entraîne des pénalités. Leurs modalités d'application sont protéiformes (selon le pouvoir de négociation du client et du prestataire, des négociations en termes de coût du service,...) et l'articulation avec les clauses de responsabilité et d'assurance devra être particulièrement soignée.

Des clauses de sécurité de plus en plus fouillées

La nouvelle version de la norme ISO 27001 *« Technologies de l'information – Techniques de sécurité – SMSI – Exigences »* en date du 27 décembre 2013 prévoit dans son Annexe A.15.1 différentes mesures relatives à la sécurité dans les relations avec les fournisseurs : *« Les exigences applicables liées à la sécurité de l'information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation »*. De plus, *« les accords conclus avec les fournisseurs doivent inclure des exigences sur le traitement des risques liés à la sécurité de l'information associé à la chaîne d'approvisionnement des produits et des services informatiques »*.
Les clauses de sécurité constituent dans certains contextes (ex : fourniture de Prestations dites essentielles dans un contexte bancaire...) des engagements de résultat au détriment des Prestataires. Cela signifie qu'ils ne peuvent déroger à cet engagement qu'en cas de force majeure ou s'ils arrivent à démontrer n'avoir commis aucune négligence.
Les clauses de sécurité s'articulent notamment autour **de l'analyse de la documentation de sécurité attenante** (ex : Politique de sécurité du Prestataire, PCA,...), d'une **capacité d'audit** renforcée des Systèmes d'information au profit des clients mais aussi des autorités réglementaires, de mesures de sécurité portant sur le système d'informations et les données (ex : gestion des accès, chiffrement, traçabilité...).
D'autres clauses sont logiquement liées aux aspects de sécurité. Il en est ainsi des **Clauses relatives à la Protection des données à caractère personnel.**
Conformément à l'article 34 de la Loi Informatique Fichiers et Libertés, le Prestataire doit assurer la sécurité et la confidentialité des données à caractère personnel lorsqu'il est responsable de traitement (si les données sont confiées au prestataire (sous-traitant au sens de l'article 35 de ladite loi), l'entreprise cliente reste le responsable du traitement). Tout manquement à ces obligations pourra être sanctionné pénalement ou par la CNIL (mais pas le prestataire qui n'est tenu que par les termes du contrat !). Cette question est loin d'être anodine notamment en cas de recours à des offres d'hébergement de services de Cloud computing et de transfert de données à caractère personnel hors UE à destination d'Etats tiers (question de la localisation des données). En outre, les notifications de violation de données à caractère personnel telles qu'introduites par l'ordonnance du 24 août 2011 et applicables actuellement aux seuls fournisseurs de services de communications électroniques au public, devraient se généraliser dans le cadre de la Proposition de Règlement *« Protection des Données à Caractère Personnel »*[1], voire en vertu du règlement européen (EiDAS) du 23 juillet 2014 sur l'identification et les services de confiance dans les transactions électroniques [2]

Que faire en cas de cessation du Contrat ?

Enfin, en cas de cessation des relations contractuelles ou en cas de changement de contrôle du Prestataire (voir plus loin), un **Plan de réversibilité** standard devra être prévu dans lequel seront décrites les modalités de migration/réversibilité (ex : coût, délai, contenu, formats techniques...).

Quel avenir pour les contrats avec un prestataire de sécurité informatique en cas de changement de contrôle capitalistique au profit d'une entreprise étrangère (hors UE et EEE) ?

Lors d'une acquisition, les contrats en général et plus particulièrement de prestations informatiques doivent faire l'objet d'un audit dans le cadre des diligences juridiques (« due diligence ») entre le cessionnaire et le cédant.
Le changement de contrôle capitalistique du Prestataire au profit d'un investisseur hors UE et EEE tel que prévu dans le cadre de l'article R. 153-52 du Code monétaire financier doit être pris en compte dans le cadre des clauses d'Intuitu personae (cela signifie que le contrat est conclu en raison de la « personnalité » du Client) des contrats entre certaines entreprises (notamment des Opérateurs d'Importance Vitale) et ledit Prestataire.
Rappelons que le Code monétaire et financier prévoit un mécanisme de déclaration administrative pour les investissements étrangers en France ainsi qu'une procédure d'autorisation administrative préalable auxquels sont soumis les investissements intervenant dans des secteurs considérés comme sensibles comme notamment :
« 4° Activités portant sur les matériels conçus pour l'interception des correspondances et la détection à distance des conversations, autorisés au titre de l'article 226-3 du code pénal ;
5° Activités de services dans le cadre de centres d'évaluation agréés dans les conditions prévues au décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;
6° Activités de production de biens ou de prestation de services de sécurité dans le secteur de la sécurité des systèmes d'information d'une entreprise liée par contrat passé avec un opérateur public ou privé gérant des installations au sens des articles L. 1332-1 à L. 1332-7 du code de la défense ; ».
Les clauses d'Intuitu Personae (ou « Caractère personnel du contrat ») doivent donc prévoir la possibilité de résilier les contrats conclus avec un prestataire de sécurité informatique lorsqu'un tel changement capitalistique adviendrait.
Le contrat reste un outil de prévisibilité et de sécurité juridique des relations entre un prestataire et son client. Son périmètre d'application nécessite – comme pour un audit Sécurité (ISO 27001) – que soit pris en compte ce type de risque contractuel même minime dans une matrice adaptée. ■

---

[1] Eric Caprioli et Isabelle Cantero, De la sécurité de l'information à la mise en œuvre du principe d'accountability, Mag Securs n°39, p.19-21.

[2] JOUE du 28 août 2014 ; v. également Eric Caprioli et Pascal Agosti, Identification électronique et services de confiance, Mag Securs, n°43, p.17-18 ; E. Caprioli, Signature électronique et dématérialisation, éd. LexisNexis, 2014 et le site www.caprioli-avocats.com.