

Les rendez-vous experts

Contrats IT

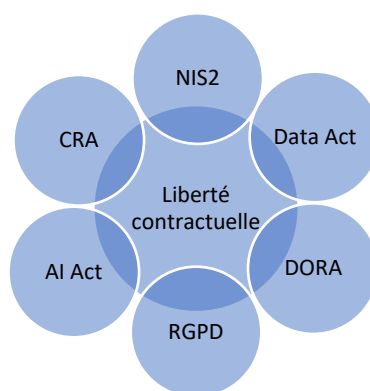
ÉPISODE #4 : Conformité légale des contrats IT : quelle liberté contractuelle ?

La notion de contrat informatique, aussi protéiforme qu'elle soit (contrat de licence ou de vente de logiciel, d'assistance ou de maintenance de logiciel, d'intégration de logiciel, de développement de logiciel, d'infogérance, d'hébergement, etc.), a pour point commun qu'elle est, par principe, guidée par la liberté contractuelle.

Les contrats informatiques deviennent toutefois les témoins de l'essor des normes européennes, avec pour conséquence un amoindrissement de la place de la volonté des parties.

NIS2, DORA, CRA, Data Act, RGPD, AI Act, Cyber Resilience Act, tous ont pour point commun de limiter la liberté contractuelle des parties. Ces impératifs réglementaires amenuisent la capacité de négocier les contrats informatiques.

Certaines clauses méritent que l'on prenne le temps de les négocier, afin de conserver une marge de manœuvre et de ne pas se retrouver dans une position de vulnérabilité en cas de différend.



Avant d'évoquer la liberté résiduelle de négociation laissée aux parties, à travers les clauses primordiales, importantes et comportant des conséquences variables selon l'objet du contrat, il est essentiel de rappeler que certains contrats doivent se négocier de manière groupée. Il serait par

exemple inutile de vouloir négocier un contrat SaaS sans que le contrat d'intégration soit négocié concomitamment, tout comme le fait de renvoyer à plus tard la négociation du contrat de support ou de maintenance.

Les clauses primordiales

Il est d'usage de définir les types d'anomalies selon une classification partagée – anomalie bloquante, anomalie majeure, anomalie mineure. Cette clause doit toujours faire l'objet de vérifications car elle est le nid de contentieux importants.

Parallèlement, le *service-level agreement (SLA)* doit être négocié en fonction de l'importance du service fourni. Si le logiciel est au cœur de l'activité du client, le *SLA* devra prévoir une garantie de temps d'intervention, une garantie de temps de rétablissement, un niveau de disponibilité et des pénalités associées.

La clause de responsabilité fait aussi partie des clauses primordiales. Elle peut se révéler inefficace selon que le préjudice indemnisable soit limité au préjudice direct ou intègre le préjudice indirect, ce qui suppose de s'y attarder.

La clause d'exclusion peut produire des effets particulièrement restrictifs, raison pour laquelle elle ne doit pas donner lieu à des concessions. Cette clause fait partie de celles qui sont décrites comme étant des pratiques de marché sur lesquelles il convient de ne pas céder.

La négociation doit également porter sur la clause de réparation, notamment quant au plafond qui ne devra jamais se révéler inférieur au montant du contrat. Le plafond peut être découpé entre plusieurs plafonds selon chaque poste de préjudice. Un *super cap* pourra alors être déterminé. Ces différents plafonds peuvent se révéler avantageux comme contraignants, selon le ou les préjudices en cause. Un plafonnement graduel en fonction de la gravité du préjudice peut aussi être envisagé. La clause de réparation peut enfin comporter une stipulation de mise en place d'une solution tierce aux frais du prestataire lorsque sa solution est défailante.

Les clauses importantes

L'absence de clause de disponibilité des données est un facteur de risque, en particulier lorsque les données peuvent être rendues indisponibles en cas d'exécution du contrat par l'acheteur. Il est donc important que la disponibilité des données soit garantie sans interruption.

La clause de réversibilité décrit les conditions de remise des données – qu'elles soient personnelles ou non – par le prestataire, au client. Du délai de restitution des données (avant ou après le terme du contrat, période de restitution) au délai de suppression des données par le prestataire en passant par les frais complémentaires en cas de restitution d'un nombre important de données, les « pièges » sont nombreux.

Sans être propre aux contrats informatiques, la clause de loi applicable et de juridiction présente une importance particulière dans la mesure où les contrats informatiques sollicitent souvent des acteurs établis à l'international.

Les clauses emportant des conséquences variables

La description du produit ou de la prestation objet du contrat ne figure pas systématiquement au contrat. Ne pas figer de description offre davantage de flexibilité pour faire évoluer le produit, mais constitue également une source de risques potentiels. Selon la prestation ou le produit objet du contrat, il peut être pertinent d'y faire figurer une description détaillée comprenant la liste des fonctionnalités attendues. Si le contrat porte sur une succession de prestations, l'état des prestations antérieures devra aussi y figurer, tout comme l'expression des besoins de la part de l'acheteur. L'objectif est « d'essentialiser » certaines fonctionnalités du produit ou certains services.

A cela s'ajoute la clause d'objectif qui précise les critères à remplir pour que le contrat soit exécuté. Cette clause présente une importance particulière dans les contrats de développement, situation dans laquelle la méthode *agile* est souvent utilisée. Cette méthode génère des adaptations constantes en fonction de l'évolution du projet et limite la faculté de définir certains objectifs en amont. Les fonctionnalités secondaires peuvent en effet devenir des fonctionnalités principales ou être substituées par de nouvelles fonctionnalités, en fonction des besoins du client.

La clause d'assurance cyber d'un prestataire a une importance variable, selon la nature de la prestation. La fourniture d'un logiciel SaaS pour des actions de *reporting* RSE, qui comportera des fichiers sans données personnelles, n'emporte pas la nécessité d'une assurance cyber. Elle sera en revanche indispensable pour un prestataire qui propose un CRM ou un hébergement HDS par exemple, puisque la donnée est au cœur du service. Outre la nécessité d'imposer une telle clause, le délai d'intervention de l'équipe cyber et le plafond d'indemnisation sont des éléments à ne pas négliger.

Une clause de garantie doit également décrire les garanties minimales attendues, ce qui peut se révéler un piège selon la rédaction adoptée. La garantie peut porter sur l'évolutivité du produit ou service, sur sa performance selon des KPI déterminés, sa disponibilité, sa sécurité, sa conformité aux attentes réglementaires du client (en fonction de sa zone géographique d'activité), l'accessibilité des données, l'interopérabilité, la compétence et la disponibilité des équipes (développement, maintenance, support) et la non dépendance à une ou plusieurs personnes clés. Les garanties décrites ne sont pas fongibles avec les prestations commandées, puisque ce ne sont que des garanties minimales. Finement rédigée, la clause de garantie peut se révéler à l'avantage du prestataire.

Une clause de RACI (*responsible, accountable, consulted, informed*) permet aussi de clarifier les rôles de chacune des parties, évitant ainsi des mises en cause réciproques, lorsque plusieurs acteurs interviennent sur un même projet.

Enfin, la clause d'audit est souvent source de négociation, ce qui peut s'avérer utile, mais aussi chronophage, notamment lorsque le client sait pertinemment qu'il ne procédera jamais à un audit du prestataire.



[PROCHAIN rdv] RDV le 1^{er} Juin pour notre prochain épisode :
Comment contracter le partage de données avec le Data Act ?

Voir nos précédents épisodes

[ÉPISODE #1 : Pourquoi les contrats IT ne sont pas des contrats comme les autres](#)

[ÉPISODE #2 : Contrats IA – Rien ne change, mais tout est différent](#)

[ÉPISODE #3 : Les effets des réglementations cyber \(DORA et NIS2\) sur les contrats IT](#)

A propos de l'auteur – Alexandre Minot-Chartier, Avocat collaborateur

Avocat au cabinet Racine, Alexandre conseille et représente les clients en matière de propriété intellectuelle et de droit du numérique, avec une expertise particulière au service des acteurs aux enjeux industriels. Il intervient ainsi aussi bien en phase de conseil, pour sécuriser et structurer les projets en amont, qu'en contentieux, pour défendre les intérêts des clients devant les autorités et juridictions compétentes.

A propos de l'équipe IP IT & Data de Racine

Racine dispose d'une équipe de 11 avocats accompagnant groupes internationaux, grandes entreprises, ETI, acteurs du numérique et start-up dans leurs projets de transformation digitale et sur leurs problématiques liées au droit de la propriété intellectuelle.

Ainsi, l'équipe intervient principalement dans 3 domaines de compétences :

- L'IT : informatique, télécommunications, sécurité des systèmes d'information, intelligence artificielle. L'équipe dispose d'une expertise reconnue dans l'accompagnement des projets informatiques et numériques.
- Data Protection : protection des données à caractère personnel et le déploiement du RGPD, contrôle et contentieux devant l'autorité de contrôle.
- L'IP : protection et valorisation du patrimoine immatériel et contentieux associés.



Alexandre Minot-Chartier
Avocat collaborateur
aminot-chartier@racine.eu
Tel. : +33 (0)1 44 82 43 00
www.racine.eu