Nations Unies A/CN.9/WG.IV/WP.148

Assemblée générale

Distr. limitée
30 janvier 2018
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Cinquante-sixième session
New York, 16-20 avril 2018

Aspects contractuels de l'informatique en nuage

Note du Secrétariat

Table des matières

V.18-00390 (F)

I. Introduction

1. Le Groupe de travail voudra peut-être se référer aux paragraphes 1 à 6 du document A/CN.9/WG.IV/WP.142, qui contiennent des informations générales sur les travaux qu'il a menés au sujet de l'informatique en nuage avant sa cinquante-cinquième session (New York, 24-28 avril 2017). On trouvera un résumé des débats menés à ce sujet par le Groupe de travail à sa cinquante-cinquième session et par la Commission à sa cinquantième session dans l'ordre du jour provisoire de la cinquante-sixième session (voir document A/CN.9/WG.IV/WP.147, par. 7 et 8).

2. Conformément à la recommandation que le Groupe de travail a formulée au sujet des travaux qui pourraient être menés dans le domaine de l'informatique en nuage (A/CN.9/902, par. 23) et aux avis exprimés par la Commission à sa cinquantième session sur ce sujet[1], le Secrétariat présente ci-après, en vue de son examen par le Groupe de travail, un projet d'aide-mémoire recensant les principales questions liées aux contrats d'informatique en nuage. Ce projet d'aide-mémoire, qui a été établi par le Secrétariat avec l'aide d'experts, tient compte des premières considérations du Groupe de travail en ce qui concerne la portée et le contenu, ainsi que la rédaction, d'un tel document (A/CN.9/902, par. 11 à 28).

3. Le Groupe de travail devrait rendre compte à la Commission, à sa cinquante et unième session (New York, 25 juin-13 juillet 2018)[2], des progrès enregistrés dans les travaux consacrés à l'informatique en nuage. Compte tenu des utilisateurs auxquels serait destiné le projet d'aide-mémoire et des transactions que celui-ci devrait viser, le Groupe de travail voudra peut-être se demander s'il conviendrait de l'établir sous la forme d'un outil de référence en ligne. Dans ce cas, il voudra peut-être recommander cette démarche à la Commission, en précisant que le Secrétariat élaborerait alors un outil de référence en ligne qui reprendrait le contenu du projet d'aide-mémoire révisé par le Groupe de travail à sa cinquante-sixième session et par la Commission à sa cinquante et unième session.

II. Projet d'aide-mémoire recensant les principales questions liées aux contrats d'informatique en nuage

[*Les termes apparaissant en caractères gras dans l'aide-mémoire sont définis dans le glossaire figurant à la fin du document. Dans un outil en ligne, ils pourraient être définis de manière plus conviviale.*]

Introduction

1. L'aide-mémoire aborde les principales questions liées aux contrats d'informatique en nuage conclus entre des entités commerciales dans lesquels une partie (le fournisseur) fournit à l'autre partie (le client) un ou plusieurs **services d'informatique en nuage** à des fins d'utilisation finale. Les contrats prévoyant la revente ou d'autres formes de redistribution de ces services sont exclus de la portée de l'aide-mémoire, de même que les contrats conclus avec des **partenaires de services d'informatique en nuage** ou d'autres tiers qui peuvent participer à la fourniture de ces services au client (par exemple contrats passés avec des sous-traitants ou des fournisseurs de services Internet).

2. Selon la loi applicable, les contrats d'informatique en nuage pourront être qualifiés de contrat de service, de location, d'externalisation, de licence, de contrat mixte ou autre. Les exigences légales relatives à la forme et au contenu de ces contrats peuvent varier en conséquence. Dans certains pays, les parties peuvent elles-mêmes, dans le contrat, en qualifier le type lorsque la législation ne dit rien, ou reste vague à ce sujet. Le tribunal tiendra compte de cette qualification pour interpréter les termes du contrat, à moins que

[1] *Documents officiels de l'Assemblée générale, soixante-douzième session, Supplément nº 17* (A/72/17), par. 116 à 127.
[2] Ibid., par. 116 et 127.

cela ne soit contraire à la législation, à la pratique judiciaire, à la véritable intention des parties, à la situation de fait ou aux coutumes ou pratiques commerciales.

3. Les questions abordées dans le présent aide-mémoire peuvent se poser en relation avec des contrats d'informatique en nuage, indépendamment du type de **services d'informatique en nuage** qu'ils concernent (par exemple, **IaaS, PaaS ou SaaS**), de leur **modèle de déploiement** (par exemple, public, **communautaire, privé ou hybride**) et des conditions de paiement (contre ou sans rémunération). L'aide-mémoire met avant tout l'accent sur les contrats d'informatique en nuage **public** de type **SaaS** prévoyant une rémunération.

4. La capacité de négocier des clauses contractuelles d'informatique en nuage dépendra de nombreux facteurs, en particulier de la question de savoir si le contrat prévoit des **solutions d'informatique en nuage normalisées pour multiabonnés** ou des solutions individuelles sur mesure, s'il existe des offres concurrentes, et du pouvoir de négociation des éventuelles parties. La capacité de négocier les termes d'un contrat, en particulier les clauses relatives à la suspension, à la résiliation ou à la modification unilatérale du contrat par le fournisseur, ainsi que les clauses de responsabilité, peut représenter un facteur important dans le choix d'un fournisseur, lorsqu'un tel choix existe [lien de renvoi]. L'aide-mémoire, établi principalement à l'usage de parties négociant un contrat d'informatique en nuage, pourrait aussi être utile aux clients qui examinent les conditions générales proposées par des fournisseurs pour déterminer si elles correspondent véritablement à leurs besoins.

5. L'aide-mémoire ne devrait pas être considéré par les parties comme une source exhaustive d'informations pour la rédaction de contrats d'informatique en nuage, ni comme un substitut à l'obtention de conseils et de services juridiques et techniques auprès de conseillers professionnels compétents. Il vise plutôt à présenter les aspects à prendre en considération avant et pendant la rédaction d'un contrat, sans toutefois donner à entendre que l'ensemble de ces aspects doit systématiquement être examiné. Les différentes solutions proposées aux questions abordées dans l'aide-mémoire ne régiront pas la relation entre les parties, à moins que celles-ci n'en conviennent expressément, ou qu'elles ne résultent de dispositions de la loi applicable. Les titres et sous-titres utilisés dans l'aide-mémoire, ainsi que l'ordre dans lequel ils apparaissent, ne doivent pas être considérés comme étant impératifs, ni comme indiquant une préférence de structure ou de style pour les contrats d'informatique en nuage. La forme, le contenu, le style et la structure des contrats d'informatique en nuage peuvent sensiblement varier en fonction des traditions juridiques, des styles rédactionnels, des exigences légales et des besoins et préférences des parties.

6. [La liste annotée n'entend pas refléter l'opinion de la CNUDCI en ce qui concerne l'opportunité de conclure des contrats d'informatique en nuage.]

7. L'aide-mémoire se présente en deux parties, suivies d'un glossaire. La première partie porte sur les principaux aspects précontractuels que les parties, en particulier le client, voudront peut-être examiner avant de conclure un tel contrat. La seconde porte sur les principales difficultés contractuelles que les parties peuvent rencontrer lorsqu'elles rédigent un tel contrat. Quant au glossaire, il décrit certains termes techniques utilisés dans l'aide-mémoire afin d'en faciliter la compréhension.

Première partie. Principaux aspects précontractuels

A. Vérification des dispositions de droit impératif et autres exigences

8. Le cadre juridique applicable au client, au fournisseur ou aux deux peut imposer des conditions pour la conclusion d'un contrat d'informatique en nuage. Ces conditions peuvent aussi provenir d'engagements contractuels, comme des **licences de propriété intellectuelle**. Le client et le fournisseur devraient en particulier avoir connaissance des lois et règlements relatifs aux **données personnelles**, à la cybersécurité, au contrôle des exportations, aux douanes, aux impôts, aux secrets commerciaux et à la propriété intellectuelle, ainsi que des **règlements sectoriels** qui peuvent leur être applicables, ainsi qu'à tout contrat qu'ils pourront conclure. La non-observation de conditions impératives peut avoir de graves conséquences, comme la nullité ou la non-exécution de tout ou partie d'un contrat, des pénalités administratives ou la responsabilité pénale.

9. Les conditions de conclusion d'un contrat d'informatique en nuage peuvent varier selon le secteur et le pays concernés. Elles peuvent notamment concerner l'obligation de prendre des mesures spéciales pour protéger les **droits des personnes concernées**, de déployer un modèle particulier (par exemple, **nuage privé** plutôt que **public**), de chiffrer les données placées dans le nuage et d'enregistrer une transaction ou un logiciel utilisé dans le traitement de **données personnelles** auprès des autorités publiques. Elles peuvent aussi prévoir des exigences en matière de **localisation des données**, ainsi que des exigences concernant le fournisseur.

- *Localisation des données*

10. Les exigences en matière de **localisation des données** peuvent en particulier découler de la loi applicable aux **données** personnelles, aux données comptables et aux données du secteur public, de la législation sur le contrôle des exportations et des règlements susceptibles de limiter le transfert de certains logiciels ou informations vers certains pays. Elles peuvent aussi découler d'engagements contractuels, comme des **licences de propriété intellectuelle** prévoyant par exemple que le contenu sous licence doit être stocké sur les serveurs sécurisés de l'utilisateur. La **localisation des données** peut en outre être privilégiée à des fins purement pratiques, par exemple pour diminuer le **temps de latence**, ce qui est surtout important pour les opérations en temps réel comme le négoce en bourse.

11. Dans ses conditions générales, le fournisseur peut expressément se réserver le droit de stocker les données client dans tout pays dans lequel lui-même ou ses sous-traitants exercent des activités. Le plus souvent, une telle pratique sera suivie même en l'absence d'un droit contractuel explicite, car il est clair que les **services d'informatique en nuage** sont, de par leur nature, généralement fournis à partir de plusieurs endroits (par exemple, la sauvegarde et la protection antivirus peuvent être assurées à distance, et l'assistance être offerte depuis le monde entier, en fonction des fuseaux horaires disponibles (modèle « **follow the sun** »). Le client qui doit satisfaire à certaines exigences en matière de **localisation des données** devra se faire confirmer par le fournisseur qu'il est possible d'y satisfaire. Lorsqu'il est possible de négocier un contrat d'informatique en nuage, on pourra y inclure des garanties contractuelles, comme l'interdiction de transférer des données en dehors de l'endroit prévu ou l'obligation, pour le fournisseur, de demander l'autorisation préalable du client en vue d'un tel transfert [lien de renvoi].

- *Exigences concernant le fournisseur*

12. Le choix d'un fournisseur adéquat par le client peut être limité, outre par les conditions du marché, par des exigences légales. Ainsi, il peut être interdit par la loi de conclure un contrat d'informatique en nuage avec un fournisseur étranger, un fournisseur dans certains pays ou un fournisseur non accrédité/certifié auprès des autorités publiques compétentes. La loi peut exiger qu'un fournisseur étranger constitue une coentreprise avec un fournisseur national ou acquière des licences et autorisations locales, y compris des autorisations d'exportation, pour fournir des **services**

d'informatique en nuage dans un pays donné. Les exigences en matière de **localisation des données** [lien de renvoi] peuvent aussi influencer le choix d'un fournisseur. Par ailleurs, le client pourra aussi tenir compte des obligations légales auxquelles le fournisseur pourrait être soumis pour ce qui est de divulguer les données client et d'autres contenus aux autorités d'autres États, ou de leur fournir un accès à ces données ou contenus.

B. Évaluation précontractuelle des risques

13. Les dispositions de droit impératif peuvent exiger qu'il soit procédé à une évaluation des risques avant la conclusion d'un contrat d'informatique en nuage. Même en l'absence d'exigences légales, les parties à un éventuel contrat peuvent décider de procéder à une telle évaluation en vue de définir une stratégie appropriée de réduction des risques, y compris la négociation de clauses contractuelles adéquates.

14. Tous les risques inhérents à un contrat d'informatique en nuage ne sont pas spécifiquement liés au nuage. Certains devront être abordés en dehors d'un éventuel contrat d'informatique en nuage (par exemple, les risques liés à une interruption de la connectivité) et tous ne pourront pas être réduits à un coût acceptable (par exemple, une atteinte à la réputation). De plus, l'évaluation des risques ne se résume pas à une étape unique avant la conclusion d'un contrat. Elle peut se poursuivre pendant la durée d'existence du contrat, et ses résultats peuvent entraîner la modification, voire la résiliation du contrat.

- *Vérification des informations relatives au fournisseur retenu*

15. Les informations suivantes pourront aider le client à identifier certains risques liés à un fournisseur particulier :

a) La politique du fournisseur en matière de protection de l'information, de confidentialité et de sécurité, en particulier en ce qui concerne la prévention des accès non autorisés, l'utilisation, l'altération ou la destruction des données du client pendant leur traitement, leur transit ou leur transfert vers le système du fournisseur, ou à partir de celui-ci ;

b) Les garanties concernant l'accès continu du client aux **métadonnées**, aux journaux d'audit et à d'autres journaux attestant des mesures de sécurité ;

c) Le plan existant de reprise après sinistre et les obligations de notification en cas d'atteinte à la sécurité ou de dysfonctionnement du système ;

d) L'assistance proposée par le fournisseur lors de la migration vers le nuage et de la cessation des services et ses garanties en matière d'**interopérabilité** et de **portabilité** ;

e) Les mesures existantes pour contrôler les antécédents des employés, sous-traitants et autres tiers impliqués dans la fourniture des services d'informatique en nuage, ainsi que les former ;

f) Des statistiques relatives aux incidents de sécurité et des informations relatives à la performance passée des procédures de reprise après sinistre ;

g) La certification de conformité aux normes techniques par un tiers indépendant ;

h) Des preuves attestant de la régularité et de la portée des audits effectués par un organe indépendant ;

i) La situation financière ;

j) Les polices d'assurance ;

k) D'éventuels conflits d'intérêts ; et

l) Le volume des **services d'informatique en nuage en couches** et sous-traités.

- *Tests d'intrusion, audits et inspections physiques*

16. Les lois et règlements qui sont d'application impérative pour le client peuvent exiger la tenue d'**audits**, de tests d'intrusion et l'inspection physique des centres de données impliqués dans la fourniture des services d'informatique en nuage, afin en particulier de déterminer si leur emplacement satisfait bien aux exigences légales en matière de **localisation des données**. Le client et le fournisseur devront convenir des conditions relatives à ces vérifications, notamment en ce qui concerne le moment où elles seront entreprises, la répartition des coûts et l'indemnisation en cas de dommage causé au fournisseur.

- *Risque d'atteinte à la propriété intellectuelle*

17. Il peut exister un risque d'atteinte à la propriété intellectuelle lorsque, par exemple, le fournisseur n'est ni le propriétaire ni le concepteur des ressources fournies à ses clients, qu'il utilise en vertu d'un contrat de **licence de propriété intellectuelle** conclu avec un tiers. Un tel risque peut aussi survenir lorsque le client est tenu, pour l'exécution du contrat, d'autoriser le fournisseur à utiliser le contenu qu'il souhaite placer dans le nuage. Dans certains pays, le stockage de contenu dans le nuage, même à des fins de sauvegarde, peut être qualifié de reproduction et exiger une autorisation préalable du propriétaire des droits de propriété intellectuelle.

18. Il est de l'intérêt des deux parties de s'assurer au préalable que l'utilisation des services d'informatique en nuage ne portera pas atteinte aux droits de propriété intellectuelle et ne constituera pas un motif de retrait des licences de propriété intellectuelle qui leur auront été accordées. Le coût d'une atteinte à la propriété intellectuelle peut être très élevé. Il faudra peut-être prévoir le droit de conclure une sous-licence, ou conclure un contrat de licence direct avec le tiers concerné, qui conférera le droit de gestion des licences du tiers. Pour pouvoir utiliser des logiciels ou autres contenus libres, il peut être nécessaire d'obtenir au préalable le consentement des tiers concernés et de divulguer le code source avec toute modification apportée au logiciel ou autre contenu libre.

- *Risque de verrouillage*

19. L'une des considérations les plus importantes peut-être pour le client sera la possibilité d'éviter ou de limiter le risque de **verrouillage**. Celui-ci découle en particulier du manque d'**interopérabilité** et de **portabilité**. En effet, la législation n'exigera pas nécessairement du fournisseur qu'il garantisse celles-ci. Il peut appartenir entièrement au client de créer des routines d'exportation compatibles, à moins que le contrat n'en dispose autrement.

20. Le contrat pourra en particulier contenir les garanties du fournisseur quant à l'**interopérabilité** et à la **portabilité**. Il pourra exiger l'utilisation de formats d'exportation de données et autres contenus qui soient normalisés ou interopérables et couramment utilisés, ou autoriser le client à choisir parmi les formats disponibles. Le contrat pourra aussi évoquer le droit du client à des produits communs et aux applications ou logiciels du fournisseur, sans lesquels l'utilisation des données et autres contenus dans un autre nuage ou dans le nuage du fournisseur pourra être impossible [lien de renvoi]. Le contrat pourra aussi prévoir l'obligation du fournisseur d'apporter son assistance pour le rapatriement des données du client ou leur exportation vers un autre fournisseur à la fin du contrat [lien de renvoi]. Le client devra aussi examiner de près les incidences de la durée du contrat : le risque de verrouillage pourra être plus important avec un contrat à long terme et avec un contrat à court ou moyen terme automatiquement renouvelable [lien de renvoi].

21. Le client pourra envisager de tester au préalable si les données et autres contenus peuvent être exportés vers un autre fournisseur ou rapatriés et utilisés sur place. Il devra peut-être aussi assurer la synchronisation entre le nuage et les plateformes internes et la reproduction de ses données en un autre lieu. Pour limiter le risque de **verrouillage**, il peut être judicieux de négocier avec plusieurs fournisseurs et de retenir une combinaison de divers types de **services d'informatique en nuage**, avec leur **modèle de**

déploiement (sources d'approvisionnement multiples), même si cela peut entraîner des coûts et d'autres conséquences pour le client.

- *Risques concernant la continuité des opérations*

22. Le client se préoccupera des risques concernant la continuité des opérations en vue non seulement de la fin programmée du contrat, mais aussi d'une éventuelle résiliation anticipée, notamment si l'une ou l'autre partie cesse ses activités. De tels risques peuvent aussi survenir en cas de suspension, par le fournisseur, de la fourniture des services. Le client peut être tenu, de par la loi, de prévoir une stratégie appropriée pour assurer la continuité des opérations et éviter les incidences négatives de la cessation ou de la suspension des services sur les utilisateurs finaux. L'élaboration de clauses contractuelles pourra aider le client à limiter les risques en la matière, en particulier en cas d'insolvabilité du fournisseur [lien de renvoi] ou de suspension ou de cessation unilatérale des services d'informatique en nuage [lien de renvoi].

- *Stratégies de retrait*

23. Le client devra déterminer à l'avance le contenu à retirer (par exemple, uniquement les données qu'il aura entrées dans le nuage ou aussi les **données dérivées de l'informatique en nuage**). Il devra aussi s'assurer qu'il pourra accéder, le moment venu, aux clefs de déchiffrement détenues par le fournisseur ou des tiers. De plus, il devra penser aux modifications qu'il conviendra d'apporter aux **licences de propriété intellectuelle** pour lui permettre de continuer à utiliser les données et autres contenus en dehors du système du fournisseur. Si le client a conçu des programmes pour échanger directement avec les interfaces de programmation applicative (API) du fournisseur, il devra peut-être les réécrire pour les adapter à l'API du nouveau fournisseur. Les clients **SaaS** dotés d'une large base utilisateurs risquent d'encourir des frais particulièrement élevés en cas de migration vers un autre fournisseur **SaaS**, car les utilisateurs finaux devront être formés à nouveau.

24. Au moment de négocier les clauses contractuelles relatives à la fin du contrat, il faudra tenir compte de tous ces facteurs, ainsi que du temps qui sera nécessaire pour exporter toutes les données client et autres contenus en vue de les rapatrier ou de les importer dans le système d'un autre fournisseur de manière à ce qu'ils soient pleinement utilisables [lien de renvoi].

C. Autres questions précontractuelles

- *Divulgation d'informations*

25. La loi applicable peut exiger des parties à un éventuel contrat qu'elles se fournissent mutuellement les informations nécessaires pour décider en toute connaissance de cause si elles souhaitent ou non conclure ledit contrat. Dans certains pays, l'absence de communication à l'autre partie d'informations permettant de satisfaire à cette obligation avant la conclusion d'un contrat peut entraîner la nullité, en tout ou en partie, du contrat ou fonder la partie lésée à réclamer des dommages-intérêts.

26. Dans certains pays, les informations précontractuelles peuvent être considérées comme faisant partie intégrante du contrat. Dans ce cas, les parties devront veiller à ce que celles-ci soient correctement enregistrées et que toute incohérence entre ces informations et le contrat même soit évitée. Elles devront aussi se préoccuper des incidences de ces informations divulguées avant la conclusion du contrat en matière de flexibilité et d'innovation pendant la phase d'exécution du contrat.

- *Confidentialité*

27. Certaines des informations divulguées avant la conclusion du contrat peuvent être jugées confidentielles (par exemple, sécurité, identification et authentification requises par le client ou offertes par le fournisseur, informations sur les sous-traitants et sur l'emplacement et le type de centres de données, celles-ci pouvant permettre d'identifier le type de données qui y sont enregistrées et l'accès dont peuvent bénéficier les autorités

publiques, y compris celles d'États étrangers). Les éventuelles parties pourront devoir s'entendre sur le caractère confidentiel des informations à divulguer avant la conclusion du contrat. Des engagements écrits de confidentialité ou des accords de non-divulgation pourront également être exigés des tiers impliqués dans le contrôle diligent précontractuel (par exemple, auditeurs).

- *Migration vers le nuage*

28. Avant d'effectuer la migration vers le nuage, le client devra généralement classer les données à migrer et les protéger en fonction de leur caractère sensible ou critique, et indiquer au fournisseur le niveau de protection exigé pour chaque type de données. Il devra peut-être aussi lui communiquer d'autres informations nécessaires pour la fourniture de services (par exemple, le calendrier de conservation et d'élimination de ses données, les mécanismes de gestion des identités et des accès et les procédures d'accès, le cas échéant, aux clefs de déchiffrement).

29. Outre le transfert des données et autres contenus depuis le client ou son ancien fournisseur vers le nuage du nouveau fournisseur, la migration vers le nuage peut aussi impliquer des opérations d'installation, de configuration, de chiffrement, des tests et la formation du personnel et des autres utilisateurs finaux. Le fournisseur pourra accepter d'apporter son assistance au client, contre rémunération ou non, aux termes soit du contrat passé avec lui, soit d'un accord distinct conclu avec lui ou un tiers agissant en son nom (par exemple, un **intégrateur de système**). Les parties impliquées dans la migration devront s'entendre sur leurs rôles et responsabilités respectifs dans l'installation et la configuration, le format dans lequel les données et autres contenus seront migrés vers le nuage, le calendrier de la migration, une procédure d'acceptation pour attester de sa bonne exécution et d'autres détails relatifs au plan de migration.

Deuxième partie. Rédaction d'un contrat

A. Considérations générales

- *Liberté contractuelle*

30. Le principe de la liberté contractuelle, largement reconnu dans les relations commerciales, permet aux parties de conclure un contrat et d'en déterminer le contenu. Cette liberté peut être restreinte par la législation relative aux conditions non négociables applicable à certains types de contrats ou par des règles qui sanctionnent l'abus de droits et les atteintes à l'ordre public, à la moralité, etc. Les conséquences du non-respect de ces restrictions peuvent aller du caractère non exécutoire de tout ou partie d'un contrat à une responsabilité civile, administrative ou pénale. Le caractère exécutoire de contrats qui n'ont pas été librement négociés, surtout lorsqu'ils imposent des conditions abusives à la partie ayant un pouvoir de négociation plus faible [lien de renvoi], peut être sujet à caution, surtout dans les pays qui attendent des parties qu'elles respectent les principes de bonne foi et de loyauté commerciale.

- *Formation du contrat*

31. Les concepts d'offre et d'acceptation de l'offre sont traditionnellement utilisés pour déterminer si et à quel moment les parties se sont entendues sur leurs droits et obligations respectifs, qui les lieront pendant toute la durée du contrat. La loi applicable peut exiger que certaines conditions soient remplies pour que la proposition de conclusion du contrat constitue une offre définitive et irrévocable (par exemple, cette proposition doit indiquer de manière suffisamment précise les services d'informatique en nuage couverts et les conditions de paiement).

32. Le contrat est conclu lorsque l'acceptation de l'offre devient effective. Il peut exister divers mécanismes d'acceptation (par exemple, le client coche une case sur une page Web, il s'enregistre en ligne pour un service d'informatique en nuage, ou il commence à utiliser un service ou à payer une commission ; le fournisseur commence ou continue à fournir des services ; les deux parties signent un contrat en ligne ou sur papier). Lorsque des modifications importantes sont apportées à l'offre (par exemple, concernant les responsabilités, la qualité et la quantité de services à fournir ou les conditions de paiement), cela peut constituer une contre-offre, qui devra dans certains cas être acceptée par l'autre partie pour que le contrat soit conclu.

33. Les **solutions d'informatique en nuage normalisées pour multiabonnés** sont généralement offertes par le biais d'applications interactives (par exemple, accords par clic). Dans ce cas, il y aura souvent très peu, voire pas, de marge de manœuvre pour négocier et ajuster l'offre standard. Pour conclure un tel contrat, il suffit de cliquer sur la mention « J'accepte », « OK » ou « Je suis d'accord ». Lorsqu'un contrat est négocié, la formation du contrat peut résulter d'une série d'étapes, notamment l'échange préliminaire d'informations, les négociations, la remise et l'acceptation d'une offre et la préparation du contrat.

- *Forme du contrat*

34. Les contrats d'informatique en nuage sont généralement conclus en ligne. Ils peuvent s'intituler différemment (accords de services d'informatique en nuage, accords-cadres de services, ou conditions de service) et comprendre un ou plusieurs documents, comme une **politique d'utilisation acceptable**, un **accord de niveau de service**, un accord de traitement des données ou une politique de protection des données, une politique en matière de sécurité et un accord de licence.

35. Les règles législatives applicables aux contrats d'informatique en nuage peuvent exiger que le contrat soit conclu par **écrit**, surtout lorsqu'il implique le **traitement de données personnelles**, et que tous les documents qui y sont mentionnés soient joints au contrat-cadre. Même lorsque la forme **écrite** n'est pas requise, les parties peuvent décider, par souci de commodité, de clarté et d'exhaustivité, ainsi qu'afin d'assurer

l'exécution et l'efficacité du contrat, de conclure celui-ci par **écrit**, en lui incorporant tous les accords accessoires.

36. La loi applicable peut exiger la signature du contrat sur papier, par exemple, pour des raisons fiscales dans certains pays.

- *Définitions et terminologie*

37. Compte tenu de la nature des **services d'informatique en nuage**, les contrats y relatifs contiendront nécessairement de nombreux termes techniques. On pourra inclure le glossaire dans le contrat, ainsi que des définitions des principaux termes qui y sont utilisés, afin d'éviter toute ambiguïté dans leur interprétation. Les parties voudront peut-être envisager d'utiliser la terminologie établie à l'échelle internationale pour assurer la cohérence et la clarté juridique du texte.

- *Contenu minimal du contrat*

38. Un contrat devra normalement : a) désigner les parties contractantes ; b) définir son objet et sa portée ; c) préciser les droits et obligations des parties, y compris les conditions de paiement ; d) établir la durée du contrat et les conditions de résiliation et de renouvellement ; et e) prévoir des recours en cas de rupture du contrat et des exemptions de responsabilité. Il contient aussi généralement des clauses relatives au règlement de litiges et au choix de la loi et du for.

B. Désignation des parties contractantes

39. La désignation correcte des parties au contrat peut avoir des incidences directes sur la formation et l'exécution du contrat. Le nom de la personne morale, sa forme juridique, son numéro d'immatriculation (s'il existe) et le siège statutaire ou l'adresse commerciale, ainsi que les documents statutaires de cette personne morale constituent généralement une base suffisante pour déterminer la personnalité juridique d'une entité commerciale (entreprise ou particulier) et sa capacité de conclure un contrat contraignant. La législation pourra exiger des renseignements supplémentaires, par exemple un numéro d'identification fiscal ou une procuration pour déterminer la capacité d'une personne physique de signer et de s'engager pour le compte d'une personne morale.

40. La vérification de l'identité d'une personne morale peut être effectuée de différentes manières, soit directement par les parties, soit par l'intermédiaire d'un tiers. Les parties sont généralement libres de déterminer une méthode d'identification, à moins que la loi applicable n'en dispose autrement. La présence physique d'un représentant autorisé de la personne morale pourra être exigée, à moins que la présence à distance par le biais de moyens d'identification électronique jugés acceptables par les parties ne soit suffisante. Le choix des parties dans ce domaine sera généralement dicté par plusieurs facteurs, y compris les risques associés à une transaction contractuelle particulière. Dans certains cas, la législation exigera ou reconnaîtra certaines méthodes d'identification uniquement, surtout pour la délivrance d'une procuration. Elle peut aussi exiger du fournisseur qu'il communique l'identité de ses clients aux autorités publiques compétentes, conformément aux normes applicables.

C. Définition de l'objet et de la portée du contrat

41. Les contrats d'informatique en nuage varient sensiblement, de par le type et la complexité de leur objet, compte tenu de la diversité des services concernés. Cet objet peut changer au cours de la durée d'un contrat : certains services pourront être annulés et d'autres ajoutés. Il peut prévoir la fourniture de services de base, auxiliaires et optionnels.

42. L'indication de l'objet du contrat contiendra une description du type de services d'informatique en nuage (**SaaS, PaaS, IaaS** ou combinaison de ceux-ci), de leur **modèle de déploiement** (**public,** communautaire**, privé** ou **hybride**), de leurs caractéristiques

techniques, en termes de qualité et de performance et de toute norme applicable. Plusieurs documents qui constituent le contrat peuvent entrer en ligne de compte pour en déterminer l'objet [lien de renvoi].

- *Accord de niveau de service*

43. L'**accord de niveau de service** définit les **paramètres de performance** à l'aide desquels la fourniture des services par le fournisseur sera mesurée. Il constitue par conséquent un outil utile pour déterminer la portée des obligations contractuelles et identifier, le cas échéant, une rupture du contrat par le fournisseur. Les accords standard ne contiendront pas nécessairement d'obligation de résultat précise, mais plutôt des déclarations d'intention non contraignantes (par exemple, « le fournisseur fera [tout] son possible pour garantir une disponibilité des services élevée », « le fournisseur s'efforcera de rendre les services disponibles 24 heures sur 24 et 7 jours sur 7 [ou d'atteindre un temps de disponibilité de 99 %] (mais ne le garantit pas) »). Dans ce genre de contrat, le client ne disposera peut-être d'aucune voie de recours, car il sera parfois difficile de prouver une violation des dispositions relatives aux meilleurs efforts. Pour éviter ce genre de situations, le client pourra souhaiter inclure, dans l'**accord de niveau de service**, des paramètres de performance quantitatifs et qualitatifs, avec des mesures spécifiques, des assurances qualité et une méthodologie de mesure de la performance.

Exemples de paramètres de performance quantitatifs

Capacité	– capacité X de stockage de données – quantité X de mémoire disponible pour le programme en cours
Disponibilité	– **temps de disponibilité** en pourcentage (par exemple, 99,9 %) – formule détaillée pour le calcul du **temps de disponibilité** – dates ou jours et heures spécifiques pendant lesquels il est essentiel d'assurer la disponibilité du service (100 %) – disponibilité d'une application particulière (100 %)
Temps d'arrêt ou pannes	– 10 pannes de 6 minutes – 1 panne d'une heure – temps nécessaire pour rétablir les données à la suite d'une panne
Élasticité et extensibilité	– dans quelle mesure et à quelle vitesse les services peuvent être augmentés ou réduits, par exemple, ressources maximales disponibles pendant une période minimum
Temps de latence	– inférieur à X millisecondes
Chiffrement	– valeur X bit pour les données au repos, en transit et en utilisation
Services d'assistance	– 24 h sur 24 et 7 jours sur 7 – heures de bureau habituelles du client

Plans de gestion des incidents et des sinistres et plans de reprise	– temps maximum de résolution des incidents – **temps** maximum **de réaction initiale** – **objectif de point de reprise** – **objectif de délai de reprise** – dates ou jours et heures spécifiques pendant lesquels il est essentiel de rétablir les données dans un délai de X
Pérennité des données stockées	– données intactes/(données intactes + données perdues pendant un délai de X (par exemple, un mois calendaire)). Il faudra définir le type de données (par exemple, fichiers, bases de données, codes, applications) et l'unité de mesure (nombre de fichiers, bits, longueur).

Exemples de paramètres de performance qualitatifs

Portabilité des données	– le client peut récupérer ses données par le biais d'un seul lien de téléchargement ou d'une API bien documentée – le format de données est structuré et documenté de manière suffisante pour permettre au client de le réutiliser ou de le restructurer dans un nouveau format s'il le désire
Exigences en matière de **localisation des données**	– les données du client (y compris toute copie, **métadonnée** et sauvegarde) sont exclusivement stockées dans des centres de données physiquement situés dans les pays indiqués dans le contrat et détenus et exploités par des entités établies dans ces pays – elles ne doivent jamais sortir du pays X, doivent être copiées dans le pays Y et ailleurs mais en aucun cas dans le pays Z
Sécurité	– les services fournis au titre du contrat sont certifiés une fois par an au moins par un auditeur indépendant à l'aune de la norme de sécurité prévue dans le contrat
Chiffrement	– le fournisseur assure le chiffrement des données chaque fois qu'elles transitent par un réseau de communication public comme Internet, tant entre le client et le fournisseur qu'entre les centres de données utilisés par le fournisseur, ainsi que lorsqu'elles se trouvent au repos dans ces centres – le fournisseur a mis en œuvre une politique de gestion des clefs conforme à une norme internationale définie dans le contrat
Protection des données/confidentialité	– les services fournis au titre du contrat sont certifiés une fois par an au moins par un auditeur indépendant à l'aune de la norme en matière de protection des données/confidentialité prévue dans le contrat

Suppression des données	– le fournisseur veille à ce que les données du client soient effectivement, irrévocablement et définitivement supprimées à la demande du client dans un certain délai prévu dans le contrat et conformément à la norme ou technique définie dans le contrat

44. Le contrat pourra inclure des mécanismes pour faciliter l'introduction de changements demandés par le client. Autrement, il faudra, à chaque fois que ses exigences évoluent, entamer un processus de négociation qui peut prendre beaucoup de temps.

Mesure de la performance

45. Le contrat pourra préciser la méthode et les procédures de mesure choisies, en particulier la période de référence choisie pour mesurer les services (quotidienne, hebdomadaire, mensuelle), les mécanismes de suivi de la fourniture des services (fréquence et forme), les rôles et responsabilités des parties et le point de mesure. Les parties pourront s'entendre sur un mécanisme indépendant de mesure de la performance et la répartition des frais y relatifs.

46. Le client s'intéressera surtout aux mesures effectuées pendant les heures de pointe, c'est-à-dire au moment où les services sont le plus nécessaire. Il pourra peut-être mesurer – ou vérifier les mesures fournies par le fournisseur ou un tiers – les données chiffrées reflétant la performance du système au moment de la consommation, mais pas celles reflétant la performance au moment de la fourniture des services. Il pourra peut-être évaluer ces dernières à partir des rapports sur la performance communiqués par le fournisseur ou un tiers. Le fournisseur pourra accepter de fournir de tels rapports à la demande du client, à un rythme régulier (quotidien, hebdomadaire, mensuel, etc.) ou à la suite d'un incident. Il pourra aussi autoriser le client à examiner ses données relatives à l'évaluation du niveau de service. Certains fournisseurs autorisent leurs clients à consulter les données relatives à la performance du service en temps réel.

47. Le contrat pourra obliger l'une des parties, voire les deux, à conserver les données relatives à la fourniture et à la consommation de services pendant une certaine durée. Ces informations peuvent être utiles pour négocier tout changement à apporter au contrat ou en cas de litige.

- *Politique d'utilisation acceptable*

48. La **politique d'utilisation acceptable** définit les conditions de l'utilisation, par le client et ses utilisateurs finaux, des services d'informatique en nuage visés par le contrat. Elle entend protéger le fournisseur contre toute responsabilité découlant de la conduite de ses clients et de leurs utilisateurs finaux. Tout client potentiel devra accepter cette politique, qui fera partie du contrat passé avec le fournisseur. La grande majorité des politiques standard interdisent toute une série d'activités dont les fournisseurs considèrent qu'elles constituent une utilisation abusive ou illégale des **services d'informatique en nuage**. Dans certains cas, il peut être justifié de supprimer certaines de ces interdictions pour tenir compte des besoins spécifiques du client.

49. Les conditions générales du fournisseur prévoient habituellement que les utilisateurs finaux du client doivent aussi observer la **politique d'utilisation acceptable** et que le client doit déployer ses meilleurs efforts ou des efforts commercialement raisonnables pour en assurer le respect. Certains fournisseurs peuvent exiger des clients qu'ils empêchent activement tout usage non autorisé ou abusif par des tiers des services d'informatique en nuage offerts au titre du contrat. Le client pourra préférer limiter son obligation de communiquer la **politique d'utilisation acceptable** aux utilisateurs finaux connus et ne pas autoriser, ou permettre en connaissance de cause, de tels usages, en plus de notifier au fournisseur tout usage non autorisé ou abusif dont il aura connaissance.

- *Politique en matière de sécurité*

50. La sécurité du système, y compris celle des données du client, implique un partage des responsabilités entre le fournisseur et le client. Le contrat précisera les rôles et responsabilités de chaque partie dans ce domaine, en tenant compte des obligations qui peuvent leur être imposées par les dispositions de droit impératif.

51. Il est habituel que le fournisseur suive sa propre politique en matière de sécurité. Dans certains cas, il pourra être possible, mais pas dans les **solutions d'informatique en nuage normalisées pour multiabonnés**, de négocier qu'il suive la politique du client en la matière. Le contrat pourra prévoir des mesures de sécurité précises (par exemple, exigences de nettoyage ou de suppression des données dans un support endommagé, stockage de paquets de données séparés à différents endroits, stockage des données du client sur du matériel spécifique qui lui est propre). Les parties devront toutefois évaluer le risque que représente la divulgation excessive d'informations concernant la sécurité dans le contrat.

52. Certaines mesures de sécurité ne nécessitent pas la contribution de l'autre partie et portent exclusivement sur ses activités habituelles, notamment les inspections, effectuées par le fournisseur, du matériel sur lequel les données sont stockées et les services sont fournis, et la prise de mesures efficaces pour assurer un accès contrôlé à celui-ci. Dans d'autres cas, l'autre partie pourra être amenée à intervenir car elle sera autorisée à s'acquitter de ses tâches ou à évaluer et contrôler la qualité des mesures de sécurité mises en œuvre. Le client, par exemple, devra mettre à jour la liste des identifiants des utilisateurs et de leurs droits d'accès et communiquer tout changement au fournisseur en temps utile pour garantir le bon fonctionnement des mécanismes de gestion des identités et des accès. Il devra aussi indiquer au fournisseur le niveau de sécurité à attribuer à chaque catégorie de données.

53. Certaines menaces à la sécurité peuvent être extérieures au cadre contractuel entre le client et le fournisseur et exiger l'alignement des conditions du contrat d'informatique en nuage sur d'autres contrats passés par le fournisseur et le client (par exemple, avec des fournisseurs de services Internet).

- *Intégrité des données*

54. Les contrats standard du fournisseur peuvent contenir une clause de non-responsabilité générale prévoyant que la responsabilité finale en ce qui concerne la préservation de l'intégrité des données incombe au client. Le fournisseur peut ne prendre que l'engagement non contraignant de faire tout son possible pour protéger les données du client.

55. Certains fournisseurs accepteront peut-être de prendre un engagement concernant l'intégrité des données (par exemple par le biais de sauvegardes régulières), éventuellement moyennant paiement. Indépendamment de l'arrangement contractuel passé avec le fournisseur, le client pourra se demander s'il serait utile de garantir l'accès à une copie utilisable au moins de ses données placée hors du contrôle, de la portée et de l'influence du fournisseur et de ses sous-traitants, et n'impliquant pas leur participation.

- *Clause de confidentialité*

56. Dans certains cas, le fournisseur n'offre pas de clause de confidentialité ou de non-divulgation, ou alors ces clauses ne sont pas suffisantes pour garantir le respect de la confidentialité des données client. Certains fournisseurs peuvent même écarter expressément toute obligation de confidentialité en la matière, et transférer l'entière responsabilité de la préservation de la confidentialité des données au client, par exemple, à travers le chiffrement. Ils peuvent accepter d'assumer uniquement la responsabilité de la confidentialité des données communiquées par le client lors de la négociation du contrat, et non des données traitées dans le cadre de la fourniture des services. La bonne volonté du fournisseur en la matière dépendra de la nature des services qu'il fournit au client en vertu du contrat et, en particulier, de la question de savoir s'il aura besoin d'avoir un accès non chiffré aux données pour fournir lesdits services.

57. Dans la plupart des cas, le client souhaitera que le fournisseur assure la confidentialité de l'ensemble de ses données placées dans le nuage et prenne un engagement de confidentialité plus élevé pour certaines données sensibles (avec un régime de responsabilité distinct en cas de violation de la confidentialité de ces dernières). Il pourra en particulier s'inquiéter de la protection de ses secrets commerciaux, de son savoir-faire et des informations dont il doit assurer la confidentialité conformément à la législation ou à des engagements pris auprès de tiers.

58. Lorsqu'un degré de protection supplémentaire est nécessaire, il pourra être judicieux de limiter l'accès aux données du client à un nombre limité de membres du personnel du fournisseur et d'exiger de ce dernier qu'il obtienne des engagements de confidentialité auprès de ces personnes, en particulier de celles exerçant une fonction à risque (par exemple, administrateurs de système, auditeurs et personnes s'occupant des dispositifs de détection des intrusions et de la réponse aux incidents). Il appartiendra au client d'indiquer clairement au fournisseur les informations confidentielles, le niveau de protection requis, toute loi ou exigence contractuelle applicable et tout changement concernant ces informations, y compris tout changement apporté à la législation applicable.

59. Dans certains cas, la divulgation des données du client sera nécessaire aux fins de l'exécution du contrat. Dans d'autres, elle sera exigée par la loi, par exemple au titre de l'obligation de fournir des informations aux autorités publiques compétentes [lien de renvoi]. Il sera alors nécessaire de prévoir des exceptions appropriées aux clauses de confidentialité.

60. Le fournisseur pourra, de son côté, imposer au client l'obligation de ne pas divulguer d'informations au sujet de ses mesures de sécurité, ni d'autres détails concernant les services fournis au client aux termes du contrat ou de la loi.

- *Protection des données/politique de confidentialité ou accord de traitement des données*

61. Les **données personnelles** font l'objet d'une protection particulière en vertu de la loi dans de nombreux pays. La législation applicable au **traitement** de ces données peut différer de la loi applicable au contrat et prévaudra sur toute clause contractuelle non conforme.

62. Le contrat peut contenir une clause relative à la protection des données ou à la confidentialité ou un accord de traitement des données ou autre type d'accord similaire, même si certains fournisseurs s'engageront uniquement de manière générale à respecter la législation applicable en matière de protection des données. Dans certains pays, un tel engagement général sera peut-être insuffisant et le contrat devra énoncer au minimum l'objet, la durée, la nature et l'objectif du **traitement**, le type de **données personnelles** et les catégories de **personnes concernées**, et les droits et obligations de **l'agent chargé du contrôle des données** et de **l'agent chargé du traitement des données**. Lorsqu'il n'est pas possible de négocier une clause de protection des données dans le contrat, le client devra peut-être au moins examiner les conditions générales pour déterminer si les dispositions lui donnent des garanties suffisantes quant au **traitement** licite **des données personnelles** et prévoient des recours en dommages-intérêts adéquats.

63. Le client jouera probablement le rôle de **contrôleur des données** et assumera la responsabilité du respect de la législation relative à la protection des données en ce qui concerne les **données personnelles** réunies et traitées dans le nuage. Il devra peut-être rechercher des clauses contractuelles obligeant le fournisseur à appuyer ses efforts visant à observer les règles applicables en matière de protection des données, y compris les demandes liées aux **droits des personnes concernées**. Des recours distincts pourraient être négociés en cas de violation de cette obligation par le fournisseur, y compris la possibilité, pour le client, de résilier unilatéralement le contrat et d'obtenir une indemnisation du fournisseur.

64. Les contrats standard prévoient généralement que le fournisseur n'assume aucun rôle de **contrôle des données**. Habituellement, il agira uniquement en tant qu'**agent chargé du traitement des données** lorsqu'il traite les données du client conformément à ses instructions aux seules fins de la fourniture des services d'informatique en nuage. Il pourra toutefois être considéré comme assumant un rôle de **contrôle des données**, indépendamment des clauses contractuelles, lorsqu'il traite plus avant les données à ses propres fins ou selon les instructions des autorités publiques [lien de renvoi]. Il assumera alors l'entière responsabilité de la protection des **données personnelles** dans le cadre de ce **traitement** supplémentaire.

- *Obligations découlant d'une violation des données et d'autres incidents de sécurité*

65. Les parties peuvent être tenues, de par la loi ou les dispositions contractuelles, voire les deux, de se notifier mutuellement tout incident de sécurité ayant un lien avec le contrat ou tout soupçon en la matière qui vient à leur connaissance. Cette obligation peut s'ajouter à l'obligation générale, qui peut être prévue par la loi, de notifier tout incident de sécurité aux parties prenantes concernées, y compris les **personnes concernées**, les assureurs et les autorités publiques, afin de prévenir les incidents ou d'en minimiser l'impact.

66. Les parties peuvent convenir d'un délai de notification (par exemple, un jour après la prise de connaissance, par la partie, de l'incident ou de la menace), de la forme et du contenu de la **notification de l'incident de sécurité** et des **mesures post-incident** à prendre, qui peuvent varier en fonction des catégories de données stockées dans le nuage. Toute exigence en matière de notification devrait tenir compte de la nécessité de ne pas divulguer d'informations sensibles susceptibles de nuire au système, aux opérations ou au réseau de la partie affectée.

67. Le client voudra peut-être se réserver le droit de résilier le contrat en cas d'incident de sécurité grave entraînant, par exemple, la perte de ses données.

D. Droit d'accéder aux données client et à d'autres contenus

- *Droit du fournisseur d'accéder aux données client pour la fourniture des services*

68. Les fournisseurs se réservent généralement le droit d'accéder aux données client conformément au principe du « besoin d'en connaître ». Avec une telle disposition, les employés, sous-traitants et autres tiers (par exemple, auditeurs) peuvent accéder aux données du client lorsqu'ils en ont besoin pour fournir les services d'informatique en nuage (y compris à des fins de maintenance, d'assistance et de sécurité) ou pour vérifier le respect de la **politique d'utilisation acceptable**, d'un **accord de niveau de service** ou de **licences de propriété intellectuelle** et d'autres documents contractuels. Les clients pourront souhaiter limiter les circonstances dans lesquelles l'accès sera autorisé et exiger des mesures permettant d'assurer la confidentialité et l'intégrité de leurs données.

69. On peut considérer que le client octroie implicitement au fournisseur certains droits d'accès à ses données lorsqu'il demande qu'un certain service lui soit fourni. Sans ces droits, le fournisseur ne pourra en effet pas fournir le service en question. Par exemple, si le fournisseur a pour instruction de sauvegarder régulièrement les données, il devra pour s'acquitter de cette tâche se voir conférer le droit de copier les données. De même, si des sous-traitants doivent traiter des données du client, le fournisseur doit être en droit de les leur transférer.

70. Le contrat peut préciser les droits liés aux données requises pour l'exécution du contrat que le client confère au fournisseur, la mesure dans laquelle ce dernier est autorisé à transférer ces droits à des tiers (par exemple, à ses sous-traitants) et la portée spatio-temporelle des droits accordés de manière implicite ou explicite. Les restrictions géographiques peuvent être particulièrement importantes pour le client si celui-ci

souhaite empêcher la sortie des données d'une région ou d'un pays particulier. Le contrat précisera souvent aussi si le client peut retirer un droit accordé de manière implicite ou explicite, et à quelles conditions. Étant donné que la capacité de fournir des services, au niveau de qualité exigé, peut dépendre des droits accordés par le client, le retrait de certains droits peut avoir pour conséquence d'entraîner la modification ou la fin du contrat.

- *Utilisation à d'autres fins des données client par le fournisseur*

71. Le fournisseur pourra demander d'utiliser les données du client à d'autres fins que la fourniture des services d'informatique en nuage prévus dans le contrat (par exemple, à des fins publicitaires, pour l'établissement de statistiques, de rapports analytiques ou prévisionnels ou pour d'autres pratiques d'extraction de données). Dans ce contexte, le client voudra notamment se poser les questions suivantes : a) quelles informations le concernant lui ou ses utilisateurs finaux seront réunies, ainsi que les raisons et le but de cette collecte et de leur utilisation par le fournisseur ; b) si ces informations seront partagées avec d'autres organisations, entreprises ou particuliers et, le cas échéant, pour quelles raisons, et si ce partage se fera avec ou sans son consentement ; et c) comment le respect des politiques en matière de confidentialité et de sécurité sera assuré si le fournisseur partage ces informations avec des tiers. Si l'utilisation par le fournisseur des données du client concerne des **données personnelles**, les parties devront en outre évaluer soigneusement leurs obligations en matière de respect des règlements au titre de la législation applicable relative à la protection des données.

72. De manière générale, le contrat devra peut-être indiquer que le fournisseur n'acquiert aucun droit automatique d'utiliser les données du client à ses propres fins. Il pourra énumérer les motifs légitimes d'utilisation autres que la fourniture de services. Ainsi, il pourra autoriser le fournisseur à utiliser des données, à ses propres fins, sous forme de données ouvertes rendues anonymes, ou de données agrégées et désidentifiées, pendant la durée du contrat ou au-delà. Dans de tels cas, le contrat pourra prévoir des obligations en ce qui concerne l'anonymisation des données client pour garantir le respect de toute réglementation relative à la protection des données ou autre réglementation applicable. Il pourra aussi imposer des limites à la reproduction des contenus et à leur communication au public.

- *Utilisation par le fournisseur du nom, du logo et de la marque du client*

73. Les conditions générales du fournisseur peuvent lui accorder le droit d'utiliser le nom, le logo et la marque du client à des fins publicitaires. Le client pourra négocier la suppression ou la modification de telles dispositions. Ainsi, il pourra exiger du fournisseur qu'il demande son approbation au préalable pour l'utilisation de son nom, de son logo ou de sa marque, ou limiter cette utilisation à son nom.

- *Mesures prises par le fournisseur à l'égard des données client sur ordre de l'État ou aux fins du respect des règlements*

74. Les conditions générales du fournisseur peuvent conférer à celui-ci une grande latitude pour divulguer des données client aux autorités publiques ou leur donner accès à ces dernières (par exemple, avec une formule du type « lorsque cela sert au mieux les intérêts du fournisseur »). Le client pourra souhaiter limiter les circonstances dans lesquelles cela sera possible, par exemple lorsque le fournisseur reçoit l'ordre d'un tribunal ou d'une autre autorité publique de donner un accès aux données ou de supprimer ou modifier celles-ci (par exemple, pour mettre en œuvre le **droit** à l'oubli **de la personne concernée**). Le fournisseur insistera toutefois peut-être sur son droit de supprimer ou de bloquer immédiatement les données du client dans d'autres circonstances, indépendamment d'un ordre donné par l'État, par exemple s'il prend connaissance d'un contenu illégal, afin d'éviter toute responsabilité prévue par la loi (procédure « de notification et de retrait » [lien de renvoi]).

75. Le contrat pourra, au minimum, obliger le fournisseur à notifier immédiatement au client tout ordre reçu de l'État, ou ses propres décisions concernant les données du client, en précisant les données concernées, à moins qu'une telle notification ne soit

contraire à la loi. Lorsqu'une notification préalable et l'intervention du client ne sont pas possibles, le contrat peut exiger du fournisseur qu'il adresse une notification *ex post* immédiate au client contenant les mêmes informations. Il peut obliger le fournisseur à conserver le journal de tous les ordres, requêtes et autres activités concernant les données du client, et à fournir à ce dernier un accès à ces informations.

- *Droits relatifs aux données dérivées des services en nuage*

76. Le contrat devra peut-être traiter des droits du client relatifs aux **données dérivées des services en nuage** et de la manière dont ces droits peuvent être exercés pendant la relation contractuelle et au terme du contrat.

- *Clause de protection des droits de propriété intellectuelle*

77. Certains types de contrats d'informatique en nuage peuvent entraîner la création d'objets de droits de propriété intellectuelle, soit conjointement par le fournisseur et le client (par exemple, améliorations du service proposées par le client) soit par le client uniquement (nouvelles applications, nouveaux logiciels et autres œuvres originales). Le contrat pourra contenir une clause expresse relative à la propriété intellectuelle, qui déterminera la partie au contrat qui jouira des droits de propriété intellectuelle sur divers objets déployés ou développés dans le nuage et l'utilisation que les parties pourront faire de ces droits. Lorsqu'il n'existe pas de possibilité de négociation dans ce domaine, le client pourra au moins examiner toute clause relative à la propriété intellectuelle pour déterminer si le fournisseur lui offre des garanties suffisantes et des moyens appropriés pour protéger ses droits et en jouir, et éviter tout risque de **verrouillage** [lien de renvoi].

- *Extraction de données à des fins judiciaires*

78. Les clients pourront avoir à rechercher des données placées dans le nuage sous leur forme initiale à des fins judiciaires, notamment dans le cadre d'une procédure judiciaire. Les documents électroniques en particulier pourront devoir répondre à des normes d'audit et d'enquête. Certains fournisseurs pourront offrir une assistance aux clients en vue de l'extraction de données dans le format requis par la loi à des fins judiciaires. Dans ce cas, le contrat devra peut-être définir exactement la nature de l'assistance que le client pourra demander au fournisseur pour répondre aux demandes des autorités compétentes.

- *Suppression de données*

79. La question de la suppression des données pourra se poser pendant la durée du contrat, mais surtout à la fin de ce dernier. Ainsi, certaines données devront peut-être être supprimées conformément au plan de conservation du client. Les données sensibles devront peut-être être détruites à un moment donné (par exemple, par le biais de la destruction des disques durs à la fin de la durée de vie des supports ayant stocké ces données). Les données devront peut-être aussi être détruites pour répondre à une demande de suppression émanant des services de police ou en raison d'un cas confirmé d'atteinte à une propriété intellectuelle [lien de renvoi].

80. Les conditions générales du fournisseur peuvent ne contenir que des déclarations non contraignantes concernant la suppression occasionnelle des données client. Le client pourra souhaiter obliger le fournisseur à supprimer immédiatement, effectivement, irrévocablement et définitivement des données, sauvegardes et **métadonnées**, conformément au calendrier de conservation et d'élimination ou à une autre forme d'autorisation ou de requête qu'il aura communiqué au fournisseur. Le contrat pourra définir les délais et autres conditions relatifs à la suppression des données, y compris l'obligation du fournisseur d'adresser une confirmation au client une fois la suppression terminée et de lui donner accès aux journaux d'audit y relatifs.

81. Des normes ou techniques de suppression particulières pourront être définies, en fonction de la nature et du caractère sensible des données (par exemple, la suppression pourra être requise dans différents lieux et sur divers supports, y compris sur les systèmes des sous-traitants et d'autres tiers, avec des niveaux de suppression différents, allant du nettoyage des données pour en assurer la confidentialité jusqu'à leur

suppression complète, voire la destruction du matériel). Une suppression plus sûre impliquant la destruction, plutôt que le redéploiement du matériel, risque d'être plus coûteuse et n'est pas toujours possible (par exemple si les données d'autres clients du fournisseur sont stockées sur le même support). Il faudra prendre en compte ces aspects dans la négociation du contrat, par exemple en exigeant que le fournisseur utilise une infrastructure isolée pour stocker les données les plus sensibles du client.

E. Audits et suivi

- *Activités de suivi*

82. Les parties pourront devoir surveiller leurs activités respectives pour assurer le respect des règlements et des obligations contractuelles (par exemple, respect par le client et ses utilisateurs finaux de la **politique d'utilisation acceptable** et des **licences de propriété intellectuelle**, et respect par le fournisseur de l'**accord de niveau de service**, de la politique de protection des données, etc.). Certaines activités de suivi, liées notamment au **traitement des données personnelles**, peuvent être exigées par la loi.

83. Le contrat devrait préciser les activités régulières ou périodiques de suivi et la partie qui sera chargée de les exécuter, ainsi que l'obligation de l'autre partie de faciliter ce suivi. Il pourra aussi anticiper toute activité de suivi exceptionnelle et prévoir les modalités d'exécution y relatives. Enfin, il pourra aussi prévoir l'obligation de communiquer des informations à ce sujet à l'autre partie, ainsi que tout engagement de confidentialité en relation avec ces activités de suivi.

84. Un suivi excessif peut avoir des conséquences négatives sur la performance et augmenter le coût des services. Pour ceux qui requièrent une performance en temps quasi réel, le client voudra peut-être chercher à obtenir le droit de demander au fournisseur d'arrêter temporairement ou définitivement le suivi si celui-ci porte gravement atteinte à la performance des services.

- *Audits et tests de sécurité*

85. Les audits et tests de sécurité sont courants, surtout ceux que le fournisseur fait réaliser pour contrôler l'efficacité des mesures de sécurité. Certains peuvent être exigés par la loi. Le contrat peut inclure des clauses relatives aux droits en matière d'audit des deux parties, à la portée et au rythme de ces audits, ainsi qu'aux formalités et coûts y relatifs. Il peut aussi obliger les parties à partager les résultats des audits ou tests de sécurité qu'elles font réaliser. Il faudra peut-être mentionner dans le contrat, outre les droits contractuels ou obligations légales en matière d'audits et de tests de sécurité, l'obligation de l'autre partie de faciliter l'exercice de ces droits ou l'exécution de ces obligations (par exemple, en donnant accès aux centres de données concernés).

86. Les parties pourront convenir que les audits et les tests de sécurité peuvent uniquement être réalisés par des organisations professionnelles, ou que le fournisseur ou le client peuvent choisir de les confier à une telle organisation. Le contrat pourra prévoir les qualifications requises du tiers concerné et les conditions de son engagement, y compris la répartition des coûts. Les parties pourront convenir de dispositions particulières concernant la réalisation d'audits ou de tests de sécurité à la suite d'un incident, en fonction de la gravité et du type d'incident (par exemple, la partie responsable de l'incident pourra être tenue de rembourser partiellement ou intégralement les coûts).

F. Conditions de paiement

- *Paiement à l'usage*

87. Le prix est une condition essentielle du contrat, et l'absence de prix ou de mécanisme de fixation du prix peut entraîner la nullité du contrat.

88. Dans un système d'informatique en nuage caractérisé par le **libre-service à la demande**, la facturation se fera généralement **à l'usage**. Il arrive couramment que le contrat précise le prix à l'unité pour le volume convenu de services fournis (par exemple, pour un nombre défini d'utilisateurs, d'utilisations ou en fonction du temps utilisé). Les barèmes ou autres ajustements de prix, y compris les rabais de volume, peuvent être conçus comme des mesures incitatives ou dissuasives pour l'une ou l'autre des parties. Les essais gratuits sont courants, de même que la fourniture de certains services à titre gracieux. S'il peut y avoir de nombreuses options en matière de calcul des prix, une clause claire et transparente dans ce domaine, bien comprise par les deux parties, permettra peut-être d'éviter des conflits et des litiges ultérieurement.

- *Frais de licence*

89. Le contrat devrait préciser clairement si le coût des services d'informatique en nuage englobe les frais pour toute licence que le fournisseur peut accorder au client en relation avec ces services. Les contrats de type **SaaS**, en particulier, prévoient souvent l'utilisation, par le client, de logiciels donnés en licence par le fournisseur.

90. Les frais de licence peuvent être calculés par poste ou par instance et varier en fonction de la catégorie d'utilisateurs (par exemple, les utilisateurs professionnels, par opposition aux utilisateurs non professionnels, pourront entrer dans l'une des catégories les plus chères). Le client devra examiner les incidences des diverses structures de paiement. Ainsi, les frais de licence d'un client peuvent considérablement augmenter si le logiciel est facturé par instance, chaque fois qu'une nouvelle machine est reliée, même si le client utilise le même nombre d'instances de machines pour la même durée. Il sera aussi important, pour le client, de préciser dans le contrat non seulement le nombre d'utilisateurs potentiels d'un logiciel couvert par l'accord de licence, mais aussi le nombre d'utilisateurs dans chaque catégorie (par exemple, employés, entrepreneurs indépendants, fournisseurs) et les droits à accorder à chaque catégorie. Il souhaitera aussi que le contrat précise les droits d'accès et d'utilisation qui entreront dans la portée de la licence, et ceux qui, sortant du cadre de cette licence, entraîneront une hausse des frais de licence.

- *Coûts supplémentaires*

91. Le prix peut comprendre également les coûts non récurrents (par exemple, pour la configuration et la migration vers le nuage). On peut également envisager des services supplémentaires non compris dans le contrat relatif à la fourniture de services informatiques de base, mais qui sont proposés par le fournisseur et facturés séparément (par exemple, assistance après les heures de bureau, facturée au temps passé ou pour un prix fixe). Les parties devraient également examiner l'aspect fiscal, car les services d'informatique en nuage peuvent ou non, selon le cas, entrer dans la catégorie des biens ou services imposables.

- *Modification du prix*

92. Les conditions générales du fournisseur donnent souvent le droit à celui-ci de modifier unilatéralement le prix ou les barèmes de prix. Le client pourra souhaiter limiter ce droit. Les parties peuvent convenir de définir dans le contrat la méthode de fixation des coûts (par exemple, la fréquence et l'ampleur des éventuelles augmentations). Les prix peuvent être liés à un indice des prix à la consommation particulier, limités à un pourcentage défini ou fixés selon le barème de prix du fournisseur à un moment donné. Le client peut exiger du fournisseur qu'il lui notifie au préalable toute hausse de prix et prévoir dans le contrat les conséquences d'une non-acceptation de sa part d'une telle hausse.

- *Autres conditions de paiement*

93. Les conditions de paiement devront peut-être prévoir les modalités de facturation (par exemple, facturation électronique), ainsi que la forme et le contenu des factures, aux fins notamment du respect des réglementations fiscales. Les autorités fiscales de certains pays pourront ne pas accepter les factures électroniques, ou exiger qu'elles se

présentent sous une forme particulière, et notamment qu'elles indiquent séparément les taxes applicables aux services d'informatique en nuage.

94. Le contrat pourra aussi préciser les échéances de paiement, la monnaie, le taux de change applicable, les modalités de paiement, les sanctions en cas de retards de paiement et les procédures de règlement de tout litige relatif à une demande de paiement.

G. Modification des services

95. Les **services d'informatique en nuage** sont par nature souples et variables. Le contrat peut contenir de nombreuses options que le client peut utiliser pour les adapter à l'évolution de ses besoins commerciaux. De plus, le fournisseur peut se réserver le droit d'ajuster son portefeuille de services à sa discrétion. Des régimes contractuels différents peuvent se justifier selon que les changements concernent les services de base ou les services auxiliaires et les aspects relatifs au soutien. Ils peuvent également se justifier pour des changements qui pourraient avoir une incidence négative sur les services par opposition à des améliorations des services (par exemple, le passage d'une offre classique à une offre améliorée comportant des niveaux de sécurité plus élevés ou des délais de réponse plus courts).

- *Mises à jour*

96. Si elles peuvent être dans l'intérêt du client, les mises à jour peuvent également perturber la disponibilité des services d'informatique en nuage, car elles peuvent se traduire par des **temps d'arrêt** relativement longs pendant les heures ouvrables normales, même si le service doit être fourni 24 heures sur 24 et 7 jours sur 7. Elles peuvent également avoir d'autres effets négatifs, par exemple exiger des modifications des applications ou des systèmes informatiques des clients ou nécessiter la formation des utilisateurs.

97. Aux termes du contrat, le fournisseur peut être tenu d'aviser le client bien à l'avance des mises à jour prévues et de leurs implications. Il peut avoir l'obligation de prévoir les mises à niveau pendant des périodes de faible demande ou d'absence de demande pour le client. Lorsque des modifications importantes sont apportées à une version en cours d'utilisation, les parties peuvent convenir que les ancienne et nouvelle versions doivent être maintenues en parallèle pendant une période convenue, afin d'assurer au client la continuité de ses activités commerciales. Il faudra peut-être que les parties s'entendent sur des procédures pour signaler et pour résoudre les problèmes éventuels. Le contrat peut également préciser l'assistance due par le fournisseur en cas de modification des applications ou des systèmes informatiques des clients et, le cas échéant, sur la formation des utilisateurs finaux du client. Les parties peuvent aussi devoir s'entendre sur la répartition des coûts découlant des mises à jour.

- *Dégradation ou interruption des services*

98. Les développements technologiques, la pression concurrentielle et d'autres raisons peuvent entraîner la dégradation ou l'interruption de certains services d'informatique en nuage, avec ou sans remplacement par d'autres services. Dans le contrat, le fournisseur peut se réserver le droit d'adapter son offre, par exemple en mettant fin à une partie des services. L'abandon de certains services par le fournisseur peut toutefois engager la responsabilité du client vis-à-vis de ses utilisateurs finaux.

99. Le contrat peut devoir comporter des clauses assurant au client une protection adéquate pour de tels cas, incluant par exemple le droit à la notification préalable de tels changements, le droit de résilier le contrat en cas de changements inacceptables ainsi qu'un délai de conservation suffisant pour garantir la **réversibilité** en temps utile des données ou d'autres contenus concernés du client. Il peut interdire toute modification susceptible d'affecter négativement la nature, l'étendue ou la qualité des services fournis, ou limiter le droit du fournisseur d'introduire uniquement des « modifications commercialement raisonnables ». Le client ne serait toutefois pas nécessairement toujours le mieux à même de juger du caractère raisonnable des modifications apportées

aux services fournis et pourrait devoir s'appuyer à cet égard sur les conseils d'experts indépendants.

- *Suspension des services à la discrétion du fournisseur*

100. Aux termes de leurs conditions générales, les fournisseurs peuvent être en droit de suspendre les services à tout moment, à leur discrétion. Le client peut souhaiter restreindre ce droit inconditionnel en autorisant la suspension uniquement dans des cas clairement circonscrits (par exemple en raison d'une violation fondamentale du contrat par le client, notamment en cas du non-paiement de sommes dues). Pour justifier la suspension unilatérale des services, les fournisseurs invoquent souvent des « événements imprévisibles », qui sont généralement définis de manière large et englobent tous les obstacles échappant au contrôle du fournisseur, y compris les défaillances de sous-traitants, de sous-prestataires et d'autres tiers impliqués dans la fourniture à la clientèle des services d'informatique en nuage, notamment les fournisseurs de réseaux Internet.

101. Le client peut envisager de subordonner le droit de suspension en raison d'événements imprévisibles à la bonne mise en œuvre par le fournisseur d'un plan de continuité des opérations et de reprise des activités à la suite d'un sinistre. Le contrat peut exiger que ce plan contienne des mesures de protection contre les facteurs qui menacent le plus fréquemment la prestation des services d'informatique en nuage et qu'il soit soumis aux commentaires et à l'approbation du client. Les mesures de protection peuvent comprendre l'existence d'un site de reprise après sinistre se trouvant dans un emplacement géographique distinct du site sinistré, une transition sans heurt ainsi que l'utilisation d'une alimentation électrique ininterrompue et de générateurs de secours.

- *Notification des modifications*

102. Aux termes de leurs conditions générales, les fournisseurs n'ont parfois aucune obligation d'informer le client des modifications des termes de service. Ainsi, il peut appartenir aux clients de vérifier régulièrement eux-mêmes s'il y a effectivement eu des modifications dans les documents contractuels publiés sur le ou les site(s) Web du fournisseur. Ces documents contractuels peuvent être nombreux ; certains peuvent renvoyer à des conditions et politiques contenues dans d'autres documents, qui peuvent à leur tour renvoyer à d'autres conditions et politiques, qui peuvent toutes faire l'objet de modifications unilatérales de la part du fournisseur. Il pourrait donc être difficile pour le client de repérer des modifications apportées par le fournisseur.

103. La poursuite de l'utilisation des services par le client étant réputée valoir acceptation des conditions modifiées, le client peut souhaiter faire obligation au fournisseur, dans le contrat, de l'informer des changements destinés à être apportés aux conditions de service dans un délai suffisant avant leur date d'entrée en vigueur. Aux termes du contrat, le fournisseur peut également être tenu de laisser le client accéder à des pistes d'audit relatives à l'évolution des services. Le client peut également souhaiter conserver toutes les conditions convenues et obliger le fournisseur à définir les services par référence à une version mise à jour ou à une version finale particulière.

H. Sous-traitants, sous-fournisseurs et externalisation

- *Identification de la chaîne de sous-traitance*

104. **L'informatique en nuage** fait fréquemment appel à la sous-traitance, aux **services d'informatique en nuage en couches** et à l'externalisation. Dans leurs conditions générales, les fournisseurs peuvent se réserver explicitement le droit d'avoir recours à des tiers pour la prestation des services en nuage au client ou ce droit peut être implicite du fait de la nature des services à fournir. Le fournisseur peut souhaiter conserver autant de latitude que possible à cet égard.

105. L'identification dans le contrat des tiers intervenant dans la fourniture des services d'informatique en nuage au client peut être exigée par la loi ou être dans l'intérêt du client à des fins de vérification. Le client voudrait en particulier avoir des garanties concernant le respect par les tiers des exigences législatives ou contractuelles en matière notamment de sécurité, de confidentialité et de protection des données, l'absence de conflits d'intérêts et les risques de non-exécution du contrat par le fournisseur en raison de défaillances des tiers. Sans être toujours en mesure d'identifier tous les tiers impliqués dans la prestation des services d'informatique en nuage au client, le fournisseur devrait être en mesure d'indiquer ceux qui jouent des rôles clefs.

- *Modifications de la chaîne de sous-traitance*

106. Le contrat peut interdire toute modification ultérieure de la chaîne de sous-traitance sans le consentement du client et prévoir que ce dernier sera en droit d'une part de contrôler tout nouveau tiers intervenant dans la fourniture des services d'informatique en nuage qui font l'objet du contrat et, d'autre part, d'opposer son veto à l'intervention d'un tel tiers. Une autre solution est d'inclure dans le contrat une liste de tiers préalablement approuvés par le client au sein de laquelle le fournisseur peut choisir en cas de besoin.

107. Le fournisseur peut toutefois insister sur son droit d'apporter des modifications unilatérales à sa chaîne de sous-traitance en en notifiant ou non le client. Le client peut souhaiter se réserver le droit d'autoriser le fournisseur à mettre en œuvre des modifications sous réserve qu'il les approuve par la suite. Il pourrait être convenu qu'en l'absence d'une telle approbation du client, les services devraient se poursuivre avec le tiers précédent ou un autre tiers préapprouvé, voire avec un autre tiers dont le choix devrait être convenu entre les parties, faute de quoi le contrat serait résiliable. La législation impérative peut prévoir des circonstances dans lesquelles des modifications de la chaîne de sous-traitance d'un fournisseur peuvent entraîner la résiliation du contrat.

- *Alignement des conditions du contrat avec celles des contrats liés*

108. Bien qu'ils puissent être listés dans le contrat, les tiers qui jouent un rôle essentiel dans l'exécution du contrat d'informatique en nuage ne sont pas eux-mêmes parties au contrat entre le fournisseur et le client. Les obligations qu'ils sont tenus d'exécuter sont celles qui découlent de leurs propres contrats avec le fournisseur. Néanmoins, divers mécanismes sont susceptibles de garantir que les conditions du contrat entre le client et le fournisseur lient ces tiers. En particulier, il peut être prévu dans le contrat que le fournisseur en aligne les conditions sur celles des contrats liés existants ou futurs. Le contrat peut également exiger du fournisseur qu'il fournisse au client des copies des contrats liés, à des fins de vérification.

109. Le client peut choisir de conclure un accord directement avec les tiers qui interviennent dans l'exécution du contrat d'informatique en nuage, en particulier en ce qui concerne des questions sensibles telles que la confidentialité et le **traitement des données personnelles**. Il peut également souhaiter négocier avec les tiers les plus importants une obligation d'intervenir si le fournisseur n'exécute pas le contrat comme il le doit (notamment si ce dernier devient insolvable).

- *Responsabilité des sous-traitants, des sous-fournisseurs et d'autres tiers*

110. Conformément au contrat ou à la loi applicable, le fournisseur peut être tenu responsable envers le client de tout problème relevant de la responsabilité de tout tiers qu'il a fait intervenir aux fins de l'exécution du contrat. En particulier, la coresponsabilité du fournisseur et de ses sous-traitants peut être établie par la loi pour tout problème lié au **traitement des données personnelles**, en fonction de l'étendue de la participation des sous-traitants à ce traitement.

111. Le contrat pourrait obliger le fournisseur à créer des droits de tiers bénéficiaires au profit du client dans le cadre de contrats liés ou à faire du client une partie à des contrats liés. Ces deux solutions permettraient au client d'exercer un recours direct contre le tiers en cas d'inexécution de ses obligations dans le cadre d'un contrat lié.

I. Responsabilité

- *Répartition des risques et des responsabilités*

112. Dans les opérations entre entreprises, les parties sont libres de répartir les risques et les responsabilités comme elles le jugent approprié, sous réserve des dispositions impératives de la loi applicable, le cas échéant. Des facteurs tels que les risques liés à la fourniture des services d'informatique en nuage (que ceux-ci soient fournis à titre onéreux ou non) et le montant facturé par le fournisseur pour ces services sont tous pris en compte dans la négociation de la répartition des risques et des responsabilités. Bien que les parties tendent généralement à exclure ou à limiter leur responsabilité en ce qui concerne les facteurs sur lesquels leur contrôle est limité ou inexistant (par exemple, le comportement des utilisateurs finaux, les actions ou les omissions des sous-traitants), le niveau de contrôle n'est pas toujours une considération décisive. Une partie peut être prête à assumer les risques et la responsabilité à l'égard de certains éléments qu'elle ne contrôle pas afin de se distinguer sur le marché. Il est néanmoins probable que les risques et les responsabilités de la partie augmentent progressivement en proportion des éléments qu'elle contrôle.

113. Par exemple, dans les modèles **SaaS** impliquant l'utilisation d'un logiciel de bureautique standard, il est probable que le fournisseur serait responsable de la quasi-totalité des ressources fournies au client et que sa responsabilité pourrait être engagée à chaque fois que les ressources ne seraient pas fournies ou qu'elles présenteraient des dysfonctions. Néanmoins, même dans ces cas, le client pourrait rester responsable de certains aspects des services, tels le chiffrement ou la sauvegarde des données sous son contrôle. En cas de perte de données, le client n'ayant pas effectué les sauvegardes de rigueur pourrait être privé de son droit de recours contre le fournisseur. Dans les modèles **IaaS** et **PaaS**, le fournisseur pourrait n'être responsable que de l'infrastructure ou des plateformes fournies (comme le matériel informatique, les systèmes d'exploitation ou les logiciels médiateurs) tandis que le client assumerait la responsabilité de tous les éléments lui appartenant (comme les applications exécutées en utilisant l'infrastructure ou les plateformes fournies et les données qu'elles contiennent).

- *Exclusion ou limitation de responsabilité*

114. Les conditions générales des fournisseurs peuvent exclure toute responsabilité conformément au contrat et faire valoir que les clauses de responsabilité ne sont pas négociables. Selon une autre possibilité, le fournisseur peut accepter la responsabilité (même illimitée) pour des violations qu'il est en mesure de contrôler (comme une violation des licences de propriété intellectuelle concédées au fournisseur par le client) mais pas pour des violations qui peuvent survenir pour des raisons indépendantes de sa volonté (incidents de sécurité, événements imprévisibles ou fuites de données confidentielles, entre autres). Les conditions générales des fournisseurs excluent généralement toute responsabilité pour des pertes ou des préjudices indirects (comme la perte d'occasions d'affaires suite à l'indisponibilité du service d'informatique en nuage).

115. Lorsque la responsabilité est acceptée de façon générale ou pour certains cas précis, les conditions générales des fournisseurs limitent souvent le montant des pertes qui seront couvertes (par incident, par série d'incidents ou par période de temps). En outre, les fournisseurs fixent souvent un plafond global de responsabilité conformément au contrat, qui peut être lié aux recettes attendues en vertu du contrat, au chiffre d'affaires du fournisseur ou à la couverture d'assurance.

116. Le client peut souhaiter négocier une responsabilité illimitée ou un dédommagement plus élevé pour certains types définis de dommages résultant d'un acte ou d'une omission de la part du fournisseur ou de son personnel. La capacité de ce faire peut dépendre, entre autres facteurs, du **modèle de déploiement** [lien croisé]. La perte ou l'utilisation abusive de données du client, les violations de la protection des données personnelles et la violation des droits de propriété intellectuelle en particulier pourraient entraîner une responsabilité potentiellement élevée du client à l'égard de tiers ou donner lieu à des amendes réglementaires. Il peut donc se justifier d'imposer au fournisseur un

régime de responsabilité plus strict lorsque de tels problèmes résultent d'une faute qu'il a commise ou de sa négligence. La législation peut également imposer la responsabilité illimitée du fournisseur face à certains types de défauts (par exemple lorsque les matériels ou les logiciels sont défectueux).

117. Les conditions générales des fournisseurs rendent généralement le client responsable en cas de non-respect de la **politique d'utilisation acceptable**. Le client peut toutefois souhaiter limiter sa responsabilité découlant d'une violation de cette **politique** due notamment à des actions de ses utilisateurs finaux qu'il ne saurait contrôler.

118. Pour être exécutoires, les clauses de non-responsabilité et les limitations de responsabilité peuvent devoir figurer dans le corps du contrat et être communiquées de manière appropriée à l'autre partie.

- *Assurance responsabilité*

119. Le contrat peut comporter des obligations en matière d'assurance visant l'une des deux parties ou toutes les deux, notamment en ce qui concerne les exigences de qualité que les compagnies d'assurance doivent remplir et le montant minimal de la couverture d'assurance demandée. Il peut également préciser que les parties doivent s'aviser mutuellement de toutes modifications apportées à la couverture d'assurance ou se fournir des copies des polices d'assurance en vigueur.

- *Exigences légales*

120. Si la plupart des systèmes juridiques reconnaissent généralement le droit des parties contractantes de répartir les risques et la responsabilité et de limiter ou d'exclure la responsabilité par le biais de dispositions contractuelles, ce droit est habituellement soumis à diverses limitations et conditions. Ainsi, le rôle que chaque partie assume en ce qui concerne les **données personnelles** placées dans le nuage constitue un facteur important pour la répartition des risques et de la responsabilité dans le cadre du **traitement des données personnelles**. Dans de nombreux pays, la législation sur la protection des données impose une plus grande responsabilité aux **agents chargés du contrôle des données** qu'aux **agents chargés du traitement des données personnelles**. Nonobstant les dispositions contractuelles, c'est le maniement de fait de ces données qui déterminera généralement le régime juridique auquel la partie serait soumise en vertu du droit applicable. Les **personnes concernées** qui ont subi un préjudice résultant du traitement illicite de **données personnelles** ou de tout acte incompatible avec les dispositions nationales relatives à la protection des données peuvent avoir droit à une indemnisation due directement par l'**agent chargé du contrôle des données**.

121. En outre, dans de nombreux pays, l'exclusion totale de la responsabilité due au fait personnel n'est pas admissible ou est sujette à des limitations. Il est parfois impossible d'exclure totalement la responsabilité liée aux dommages corporels (y compris la maladie et le décès) et à la négligence grave, aux dommages intentionnels, aux défauts, à la violation des obligations essentielles du contrat ou au non-respect des exigences réglementaires applicables. Par ailleurs, si les conditions du contrat ne sont pas librement négociées, mais plutôt imposées ou préétablies par l'une des parties (« contrats d'adhésion »), certains types de clauses limitatives peuvent être considérés comme « abusifs » et donc invalides [lien croisé].

122. La législation peut limiter la capacité qu'ont les institutions publiques d'assumer certaines responsabilités ou leur imposer d'obtenir l'approbation préalable d'un organe compétent de l'État pour ce faire. Il peut aussi leur être interdit d'accepter l'exclusion ou la limitation de la responsabilité des fournisseurs soit de manière générale soit en ce qui concerne des omissions ou des actes définis dans la législation.

123. D'autre part, la législation applicable peut prévoir une exonération de responsabilité si certains critères sont remplis par une partie dont la responsabilité risquerait autrement d'être engagée. Par exemple, en vertu de la procédure dite de notification et de retrait qui a cours dans certains pays, le fournisseur sera dégagé de toute responsabilité relative à l'hébergement d'un contenu illicite sur son infrastructure

dans le nuage s'il supprime ce contenu lorsqu'il prend conscience de son existence [lien croisé].

J. Recours en cas de violation du contrat

- *Types de recours*

124. Les parties sont libres de choisir des recours, dans les limites prévues par la législation applicable. Ces recours peuvent inclure des mesures en nature visant à fournir à la partie lésée le même avantage ou un avantage équivalent à l'avantage censé découler de l'exécution du contrat (entre autres le remplacement du matériel défectueux), des mesures pécuniaires (par exemple des crédits de service) ou la résiliation du contrat. Le contrat pourrait établir une distinction entre les types de violation et préciser des recours correspondants.

- *Suspension ou résiliation des services*

125. La suspension ou la résiliation de la prestation des services d'informatique en nuage au client constitue un recours habituel du fournisseur en cas de rupture de contrat de la part du client ou de violation de la **politique d'utilisation acceptable** par les utilisateurs finaux du client. Le client souhaitera sans doute disposer de garanties contractuelles contre des droits étendus de suspension ou de résiliation. Par exemple, le droit du fournisseur de suspendre ou de résilier la prestation des services informatiques en nuage au client pourrait être limité aux cas de violations fondamentales du contrat par le client et de menaces sérieuses pour la sécurité ou l'intégrité des systèmes du fournisseur. Le droit du fournisseur de suspendre ou de résilier les services pourrait aussi être limité aux services affectés par la violation, lorsque cette possibilité existe.

- *Crédits de service*

126. Le système des crédits de service est un mécanisme souvent utilisé pour indemniser le client lorsque le fournisseur ne remplit pas ses obligations. Ces crédits se présentent sous la forme d'une baisse du coût des services à fournir conformément au contrat au cours de la période mesurée suivante. Un barème dégressif peut s'appliquer, à savoir qu'un pourcentage de la réduction des frais peut dépendre de la mesure dans laquelle les performances du fournisseur en vertu du contrat sont inférieures aux paramètres définis dans l'**accord de niveau de service** ou dans d'autres parties du contrat. Un plafond global en matière de crédits de service peut également s'appliquer. Les fournisseurs peuvent limiter les circonstances dans lesquelles des crédits de service sont accordés, par exemple aux cas où les défaillances sont dues à des aspects qu'ils contrôlent, ou limiter les délais dans lesquels les clients peuvent utiliser ces crédits. Certains fournisseurs peuvent aussi être disposés à rembourser des frais déjà payés ou à fournir un forfait de services amélioré au cours de la période mesurée suivante (comportant par exemple un soutien informatique gratuit). S'il existe un éventail d'options, les conditions générales des fournisseurs précisent généralement que toute solution en cas d'inexécution de la part du fournisseur sera laissée au choix de ce dernier.

127. Le client devrait évaluer au cas par cas le bienfondé du fait que le contrat désigne les crédits de service comme étant le seul et unique recours contre un fournisseur qui ne remplit pas ses obligations contractuelles. En effet, ce régime peut limiter les droits qu'aurait le client de se prévaloir d'autres recours, y compris des actions en réparation ou pour résilier le contrat. Le client pourrait souhaiter que le contrat prévoie d'autres mesures d'atténuation des risques de non-exécution de la part du fournisseur, ainsi que des incitations suffisantes que ce dernier remplisse correctement ses obligations conformément au contrat et qu'il améliore ses services. L'imposition de pénalités, par exemple, pourrait avoir un impact financier plus important sur le fournisseur que l'obligation de fournir des crédits de service. En outre, en cas de résiliation du contrat, il ne servirait vraisemblablement à rien d'offrir des crédits de service sous forme d'une baisse des frais ou d'un forfait de services amélioré au cours de la période mesurée suivante. Enfin, des crédits de service excessifs pourraient ne pas être exécutoires s'ils

ont été considérés comme une approximation déraisonnable du préjudice à la formation du contrat.

- *Formalités à observer en cas de violation du contrat*

128. Le contrat peut comporter des formalités à respecter en cas de violation, par exemple exiger d'une partie qu'elle notifie l'autre partie lorsque des clauses sont considérées comme étant violées et qu'elle lui donne l'occasion de remédier à cette éventuelle violation. Des délais de recours peuvent également être fixés.

K. Durée et résiliation du contrat

- *Date d'entrée en vigueur du contrat*

129. Le contrat devrait préciser clairement sa date d'entrée en vigueur, qui peut différer de la date de signature, de la date d'acceptation de l'offre ou de la date d'acceptation de la configuration et d'autres actions requises pour que le client migre vers le nuage. On peut considérer que la date d'entrée en vigueur du contrat est celle à laquelle le fournisseur met les services informatiques en nuage à la disposition du client (même si ce dernier ne les utilise pas effectivement). Il est également possible de considérer que le contrat entre en vigueur le jour où le client effectue le premier paiement correspondant aux services d'informatique en nuage (même si le fournisseur ne les lui a pas encore procurés).

- *Durée du contrat*

130. Le contrat peut être de courte, moyenne ou longue durée. Dans le cadre des **solutions d'informatique en nuage normalisées pour multiabonnés**, il est fréquent de prévoir une durée initiale fixe (courte ou moyenne), avec des renouvellements automatiques à moins de résiliation par l'une ou l'autre des parties. Le client peut contraindre le fournisseur à le notifier de l'expiration prochaine de la durée du contrat et de la nécessité de prendre une décision quant à son renouvellement. Ce mécanisme peut s'avérer utile pour que les clients évitent les risques de **verrouillage** et ne ratent pas des offres plus intéressantes.

- *Résiliation anticipée*

131. Le contrat devrait aborder les circonstances dans lesquelles il pourrait être résilié autrement qu'à l'expiration de sa durée fixe, par exemple pour des raisons de commodité ou de violation. Il pourrait devoir prévoir des modalités de résiliation anticipée, y compris l'obligation d'un préavis suffisant, la **réversibilité** et d'autres engagements en matière de fin des services [lien de renvoi].

Résiliation pour raisons de commodité

132. En particulier dans le cadre des **solutions d'informatique en nuage normalisées pour multiabonnés**, les fournisseurs se réservent généralement le droit, dans leurs conditions standard, de résilier le contrat à tout moment sans qu'il y ait défaillance du client. Le client pourrait souhaiter limiter les circonstances dans lesquelles un tel droit pourrait s'exercer et contraindre le fournisseur à lui signifier un préavis de résiliation suffisamment long.

133. Le droit du client de résilier le contrat pour convenance (c'est-à-dire sans qu'il y ait de défaillance du fournisseur) est très courant dans les contrats publics. Le cas échéant, le fournisseur peut exiger le paiement d'indemnités de résiliation anticipée, que la législation peut par ailleurs limiter dans le cas des entités publiques. Dans les contrats à durée indéterminée, les fournisseurs peuvent être plus enclins à accepter la résiliation par le client pour de simples raisons de commodité sans compensation, mais cela peut également entraîner une hausse des tarifs conformément au contrat.

Résiliation pour violation

134. La violation fondamentale du contrat en justifie généralement la résiliation. Afin d'éviter toute ambiguïté, les parties peuvent définir dans le contrat des événements qu'elles considéreront comme des violations fondamentales. Du point de vue du client, il peut s'agir de la perte ou de l'utilisation abusive de données, d'infractions à la protection des données personnelles, d'incidents de sécurité récurrents (à savoir plus de X fois durant n'importe quelle période mesurée), de violations de confidentialité et d'indisponibilité des services à certains moments ou pendant certaines périodes de temps. Le défaut de paiement et la violation par le client ou ses utilisateurs finaux de la **politique d'utilisation acceptable** sont les motifs les plus fréquents de résiliation du contrat par le fournisseur. Le droit des parties de résilier le contrat peut être subordonné à une notification préalable, à la tenue de consultations de bonne foi, à l'offre de mesures visant à remédier à la situation et à l'engagement de restaurer l'exécution du contrat dans un certain délai suivant la prise de mesures correctives.

135. Le contrat peut devoir tenir compte des engagements du fournisseur en matière de fin des services qui survivraient à la violation fondamentale du contrat par le client. Le client pourrait souhaiter garantir, au minimum, la **réversibilité** de ses données et autres contenus [lien de renvoi].

Résiliation pour cause de modifications inacceptables du contrat

136. La résiliation peut se justifier par des modifications inacceptables ou commercialement déraisonnables ou si des modifications unilatérales sensiblement préjudiciables aux intérêts de l'autre partie sont apportées au contrat. Il peut s'agir de changements portant sur les exigences en matière de **localisation des données** ou sur les conditions de sous-traitance. Il est possible que le contrat doive préserver de manière spécifique le droit qu'a le client de le résilier dans son intégralité si des modifications découlant de la restructuration du portefeuille de services du fournisseur entraînent la cessation ou le remplacement de certains services [lien de renvoi].

Résiliation pour cause d'insolvabilité

137. Un client insolvable peut devoir continuer à utiliser les services informatiques en nuage pendant qu'il résout ses difficultés financières. Il peut donc souhaiter limiter le droit du fournisseur d'invoquer l'insolvabilité du client comme seul motif de résiliation du contrat en l'absence, par exemple, de tout défaut de paiement du client conformément au contrat.

138. Les risques d'insolvabilité du fournisseur pourraient être détectés au cours de l'évaluation des risques. Au terme du contrat, le fournisseur pourrait devoir communiquer aux clients des rapports périodiques sur sa situation financière et prévoir le droit de ces derniers de résilier le contrat sans autre obligation ou responsabilité s'il venait à ne pas avoir les capacités financières voulues pour exécuter intégralement le contrat.

139. Les clients courent un risque important de ne pas pouvoir récupérer leurs données et autres contenus hébergés dans l'infrastructure infonuagique du fournisseur lorsque des craintes relatives à la situation financière du fournisseur provoquent des sorties et des retraits de contenus à grande échelle. Le fournisseur insolvable ou un **représentant de l'insolvabilité** peuvent limiter les quantités de contenus (données et code applicatif) susceptibles d'être retirées dans un délai donné. Il pourrait également être décidé de remplir les engagements en matière de fin de service en fonction de l'ordre d'arrivée des clients (« premiers venus, premiers servis »). Le client pourrait donc souhaiter disposer de mécanismes contractuels lui garantissant qu'il pourra récupérer ses données détenues par le fournisseur insolvable. Il pourrait demander le séquestre des clefs ou des codes sources qui seraient ensuite automatiquement libérés pour autoriser l'accès aux données et aux autres contenus du client en cas d'insolvabilité du fournisseur. Cependant, les dispositions impératives de la législation sur l'insolvabilité pourraient l'emporter sur des engagements contractuels.

Résiliation en cas de changement de contrôle

140. Le changement de contrôle peut impliquer, par exemple, un changement de propriété ou des changements dans la capacité de déterminer, directement ou indirectement, les politiques opérationnelles et financières du fournisseur, ce qui peut entraîner des modifications du portefeuille de services de ce dernier. Il peut également entraîner la cession ou la novation du contrat, avec transfert à un tiers soit des droits et des obligations soit uniquement des droits découlant du contrat. En conséquence, une des parties d'origine du contrat peut être remplacée par une autre partie ou certains aspects du contrat, par exemple les paiements, peuvent devoir faire intervenir un tiers.

141. Aux termes du contrat, le fournisseur peut avoir l'obligation de donner un préavis de tout changement de contrôle à venir et de son incidence prévue sur la continuité des services. Le client pourrait souhaiter se réserver le droit contractuel de résilier le contrat si, du fait du changement de contrôle, le fournisseur ou le contrat sont repris par un concurrent du client ou si l'acquisition entraîne l'abandon ou la transformation du portefeuille des services. La législation applicable pourrait imposer la résiliation du contrat si, du fait du changement de contrôle, il devient impossible de remplir certaines dispositions législatives impératives (concernant notamment les exigences en matière de localisation des données ou l'interdiction de traiter avec certaines entités parce qu'elles sont soumises à des régimes de sanctions internationaux ou pour des raisons de sécurité nationale). Les contrats publics en particulier peuvent être affectés par des limitations réglementaires en matière de changement de contrôle.

Disposition relative à l'inactivité du compte

142. L'absence d'activité de la part du client pendant une période précisée dans le contrat peut justifier la résiliation unilatérale de ce dernier par le fournisseur. Ceci étant, les contrats portant sur des services d'informatique en nuage d'entreprise à entreprise payants comportent très rarement de telles clauses relatives à l'inactivité du compte, voire jamais.

L. Engagements en matière de fin des services

143. Les engagements en matière de fin des services peuvent soulever des questions non seulement contractuelles mais également réglementaires. Le contrat devrait parvenir à un équilibre entre les intérêts du client pour ce qui est d'avoir un accès constant à ses données et autres contenus (notamment pendant la période de transition) et ceux du fournisseur, à qui il importe de mettre fin à toutes ses obligations à l'égard de l'ancien client le plus rapidement possible.

144. Les engagements en matière de fin des services peuvent être les mêmes quelle que soit la cause de résiliation du contrat, ou ils peuvent être différents selon que la résiliation découle de la violation du contrat ou d'autres raisons. Diverses questions peuvent devoir être abordées par les parties, notamment :

- *Délais d'exportation*

145. Le client souhaiterait disposer d'une période suffisamment longue pour lui permettre d'effectuer la bonne migration de ses données et autres contenus vers un autre fournisseur ou vers ses infrastructures internes.

- *Accès du client aux contenus faisant l'objet de l'exportation*

146. Le contrat devrait préciser les données et autres contenus qui sont susceptibles d'être exportés ainsi que les modalités d'accès des clients à ces données, y compris les éventuelles clefs de décryptage qui pourraient être détenues par le fournisseur ou des tiers. Les parties peuvent convenir d'un séquestre pour assurer au client un accès automatique à toutes les caractéristiques requises pour l'exportation. Dans la mesure du possible, le contrat devrait également préciser les options d'exportation (notamment les formats et les processus), tout en reconnaissant la possibilité qu'elles changent au fil du temps.

- *Aide à l'exportation apportée par le fournisseur*

147. L'étendue de la participation du fournisseur à l'exportation des données du client soit vers ses infrastructures internes soit vers un autre fournisseur de son choix, les procédures qui seraient employées et les délais nécessaires pourraient devoir être précisés dans le contrat. Le fournisseur pourrait exiger que les frais relatifs à l'assistance à l'exportation soient réglés séparément. Dans ce cas, les parties pourraient fixer le montant de ce paiement dans le contrat ou convenir de se reporter à la liste des tarifs du fournisseur à un moment donné. Une autre solution serait que les parties conviennent qu'une telle assistance fait partie des frais prévus dans le contrat et que le client ne se verra facturer aucun frais supplémentaire si la résiliation du contrat découle d'une violation par le fournisseur.

- *Suppression des données de l'infrastructure infonuagique du fournisseur*

148. Le contrat pourrait devoir préciser les règles qui seront mises en œuvre pour supprimer les données et autres contenus du client de l'infrastructure infonuagique du fournisseur lors de l'exportation ou à l'expiration de la période prévue dans le contrat pour l'exportation. Les données peuvent être supprimées automatiquement par le fournisseur ou bien à la demande et suivant les instructions spécifiques du client. Le contrat peut faire obligation au fournisseur d'avertir le client avant la suppression des données et de lui confirmer la suppression des données, des sauvegardes et des **métadonnées**. Le fournisseur peut être tenu de communiquer au client une attestation, un rapport ou une déclaration confirmant que les données ont été supprimées, notamment des systèmes des tiers.

- *Conservation de données après la fin du contrat*

149. Le fournisseur pourrait avoir une obligation légale de conservation des données des clients, en particulier en vertu de la législation sur la protection des données (qui pourrait également préciser une durée de conservation). En outre, le client peut autoriser le fournisseur à conserver certaines données spécifiques ou il peut souhaiter que celui-ci s'engage par contrat en ce qui concerne la conservation des données après la résiliation du contrat pour des raisons liées à la réglementation, au règlement des différends ou à d'autres motifs juridiques qui lui sont propres. Moyennant des frais supplémentaires, certains fournisseurs peuvent permettre aux clients de choisir une période pendant laquelle leurs données seront conservées après la fin du contrat.

150. Il peut être nécessaire d'établir des exigences particulières (par exemple pour anonymiser les renseignements personnels) à l'égard des données qui ne sont pas ou ne peuvent pas être retournées au client et dont la suppression ne serait pas possible. Le contrat devrait préciser le format dans lequel ces données doivent être conservées après la résiliation du contrat. Il peut s'agir d'un format approuvé par le client (chiffré ou non) ou le contrat peut stipuler de façon générale que les données doivent être conservées dans un format utilisable et interopérable pour permettre leur extraction si besoin est. Le contrat devrait préciser les responsabilités des parties en ce qui concerne la conservation des données dans le format spécifié après la fin du contrat.

- *Clause de confidentialité après la fin du contrat*

151. Les parties peuvent convenir d'une clause de confidentialité qui restera en vigueur après la fin du contrat. Les obligations de confidentialité peuvent survivre au contrat pendant un certain temps (par exemple pendant cinq à sept ans après sa résiliation) ou se poursuivre indéfiniment, en fonction de la nature des données et autres contenus des clients qui ont été placés dans l'infrastructure infonuagique du fournisseur.

- *Audits après la fin du contrat*

152. Les audits à réaliser après la fin du contrat peuvent être convenus par les parties ou imposés par la loi. Le contrat devrait préciser leurs modalités d'exécution, y compris le calendrier et la répartition des coûts.

- *Reliquats de compte*

153. Les parties peuvent être amenées à s'entendre sur les conditions de restitution au client du reliquat de son compte ou sur la déduction du montant de ce reliquat des sommes qui resteraient éventuellement dues au fournisseur, notamment pour les activités de fin de service ou pour régler des dommages-intérêts.

M. Règlement des litiges

- *Méthodes de règlement des litiges*

154. Il est souhaitable que les parties conviennent à l'avance du mode de règlement des éventuels litiges qui pourraient découler du contrat, par exemple la négociation, la médiation, la conciliation, l'arbitrage ou les procédures judiciaires. Différents types de différends peuvent justifier la mise en œuvre de différentes procédures de règlement. Ainsi, les litiges portant sur des questions financières et techniques peuvent être soumis à la décision contraignante d'un tiers expert (qu'il s'agisse d'un particulier ou d'un organisme) tandis que des négociations directes entre les parties peuvent s'avérer plus efficaces pour résoudre d'autres types de différends. Certaines législations peuvent imposer aux parties d'épuiser les ressources liées à divers mécanismes de règlement extrajudiciaire avant de pouvoir soumettre leur litige à un tribunal national.

- *Procédures arbitrales*

155. Si les parties en sont convenues, les différends qui ne sont pas réglés à l'amiable peuvent être soumis à l'arbitrage. Les parties devraient cependant vérifier l'arbitrabilité des questions soumises à l'arbitrage (c'est-à-dire vérifier si l'État ne réserve pas les questions devant être tranchées par l'arbitrage à des procédures judiciaires à mener devant des tribunaux nationaux). Si les parties ont opté pour l'arbitrage, il est souhaitable qu'elles s'entendent sur un ensemble de règles d'arbitrage destinées à régir toute procédure arbitrale. Le contrat peut comprendre une clause type faisant référence à l'utilisation de règles internationalement reconnues pour la conduite des procédures de règlement des différends (par exemple, le Règlement d'arbitrage de la CNUDCI). À défaut d'une telle précision, la procédure arbitrale est normalement régie par le droit procédural de l'État où l'arbitrage se déroule ou, si une institution arbitrale est choisie par les parties, par le règlement de cet organisme. Les parties peuvent opter pour un mécanisme de règlement des litiges en ligne doté de ses propres règles.

- *Actions en justice*

156. Si des procédures judiciaires devaient avoir lieu, la nature des **services d'informatique en nuage** est telle que plusieurs États pourraient se déclarer compétents. Dans la mesure du possible, les parties peuvent convenir d'une clause attributive de compétence en vertu de laquelle elles sont tenues de soumettre leurs litiges à un tribunal particulier [lien croisé].

- *Conservation des données*

157. Le contrat devrait aborder les questions de conservation pendant une période de temps raisonnable des données et autres contenus du client, et d'accès du client à ceux-ci, quelle que soit la nature du litige. Cela peut être important pour le client, non seulement en raison de la nécessité d'assurer la continuité des opérations mais aussi parce que l'accès aux données, y compris les **métadonnées** et d'autres **données dérivées des services en nuage**, peut être vital pour les procédures de règlement des différends elles-mêmes (par exemple pour étayer une demande ou une demande reconventionnelle).

- *Délais de prescription pour les demandes*

158. Les parties peuvent être amenées à s'entendre sur les délais de prescription applicables aux demandes. Les fournisseurs peuvent avoir tendance à imposer aux clients des délais de prescription relativement courts pour introduire des demandes relatives aux services. Ces dispositions peuvent être inapplicables si elles violent les délais de prescription obligatoires prévus par la législation applicable.

N. Dispositions relatives au choix de loi et à l'élection de for

159. La liberté contractuelle permet habituellement aux parties de choisir la loi qui sera applicable à leur contrat ainsi que la juridiction ou le for où les différends seront traités. La législation impérative (sur la protection des données, par exemple) peut cependant l'emporter sur le choix de la loi applicable et les clauses d'élection de for convenus par les parties contractantes, selon l'objet du litige. En outre, indépendamment du choix de loi et de l'élection de for, plusieurs lois impératives (loi sur la protection des données, loi sur l'insolvabilité, par exemple) peuvent être applicables au contrat.

- *Considérations relatives au choix de loi et à l'élection de for*

160. Le choix de la loi applicable et les clauses d'élection de for sont liés. La question de savoir si la loi choisie par les parties s'appliquera en fin de compte dépendra du for où la clause de choix de loi sera présentée à un tribunal ou à un autre organe juridictionnel, par exemple un tribunal arbitral. C'est la loi de ce for qui déterminera si la clause est valide et si le for respectera le choix de la loi applicable fait par les parties. En raison de l'importance de la loi du for pour la clause de choix de loi, tout contrat comportant une telle clause comporte généralement aussi une clause d'élection de for.

161. Pour choisir le for, les parties tiennent habituellement compte de l'incidence de la loi choisie ou autrement applicable et de la mesure dans laquelle une décision judiciaire rendue dans ce for serait reconnue et exécutoire dans les pays où l'exécution serait probablement demandée. Il peut être important de préserver la souplesse des options d'exécution, en particulier dans les environnements d'**informatique en nuage** où il peut y avoir une certaine incertitude quant à la localisation des actifs intervenant dans la prestation des services, du fournisseur et du client ainsi qu'à d'autres facteurs que les parties prennent généralement en compte pour choisir la loi applicable et déterminer les clauses d'élection de for.

- *Loi et for obligatoires*

162. La loi et le for d'un pays donné peuvent être obligatoires pour divers motifs, par exemple :

a) Le fait que les services d'informatique en nuage soient accessibles sur le territoire d'un État donné peut être suffisant pour que s'applique la législation de cet État en matière de protection des données ;

b) La nationalité ou le lieu de résidence de la **personne concernée** ou des parties contractantes, en particulier de l'**agent chargé du contrôle des données**, peuvent déclencher l'application de la loi dont relève cette partie ou la **personne concernée** ; et

c) La législation du lieu d'origine de l'activité (l'emplacement du matériel) ou du lieu vers lequel l'activité est dirigée aux fins d'en tirer des avantages peut déclencher l'application de la loi de ce lieu. L'utilisation du nom de domaine géographique associé à un lieu particulier, la langue locale utilisée par le fournisseur pour la conception de son site Web, la tarification en monnaie locale et les points de contact locaux sont autant de facteurs qui peuvent être pris en compte pour cette détermination.

- *Loi et for du lieu d'établissement du fournisseur ou du client*

163. Les contrats relatifs à des **solutions d'informatique en nuage normalisées pour multiabonnés** précisent souvent qu'ils sont régis par le droit du lieu où le fournisseur a son établissement principal ou bien du lieu où il est implanté. En règle générale, ils accordent aux tribunaux de ce pays la compétence exclusive pour connaître de tous les litiges qui pourraient découler du contrat. Le client peut préférer préciser la loi et la compétence de son propre pays. La capacité d'institutions publiques de consentir à l'application de la loi et à la compétence de pays étrangers serait généralement très limitée. Les fournisseurs qui sont actifs dans de nombreux pays peuvent faire preuve de souplesse s'agissant de choisir la loi et le for du pays où le client est situé.

- *Options multiples*

164. Les parties peuvent également préciser diverses options pour différents aspects du contrat. Elles peuvent aussi opter pour la juridiction du défendeur afin d'éliminer l'avantage dont bénéficie le demandeur quand le for est celui de son pays de domicile et de favoriser ainsi le règlement informel des différends.

- *Absence de choix de loi ou d'élection de for*

165. Certaines parties peuvent préférer que leur contrat ne précise pas de loi applicable et ne comporte pas de clause attributive de compétence, laissant la question ouverte en vue d'être tranchée ultérieurement le cas échéant. Dans certains cas, il pourrait s'agir de la seule solution viable.

O. Notifications

166. Les clauses de notification porteraient sur la forme, la langue, le destinataire et les moyens de notification, ainsi que sur le moment d'entrée en vigueur de la notification (lors de la remise, de l'expédition ou conformément à l'accusé de réception). En l'absence de dispositions législatives contraignantes, les parties peuvent convenir de formalités de notification qui pourraient être uniformes ou varier en fonction du degré d'importance, de l'urgence et d'autres considérations. Des exigences plus strictes que pour les notifications de routine se justifieraient notamment en cas de suspension ou de résiliation unilatérale du contrat. Dans de tels cas, les délais devraient permettre la **réversibilité** et la continuité des activités du client. Le contrat peut contenir des références aux notifications et délais imposés par la loi.

167. Les parties peuvent opter pour que les notifications **écrites** soient remises à l'adresse physique ou électronique des correspondants indiqués dans le contrat. Le contrat peut préciser les conséquences juridiques d'un manquement à l'obligation de notification et d'une absence de réponse à une notification exigeant une réponse.

P. Dispositions diverses

168. Les parties regroupent souvent sous l'intitulé « divers » les dispositions qui ne relèvent pas d'autres parties du contrat. Certaines d'entre elles peuvent contenir un texte normalisé figurant dans tous les types de contrats commerciaux (en quelque sorte des « dispositions standard »). Il peut s'agir, par exemple, d'une clause de sauvegarde permettant de supprimer les dispositions invalides du reste du contrat ou d'une clause linguistique identifiant une certaine version linguistique du contrat comme faisant foi en cas de conflit d'interprétation entre différentes versions linguistiques. Le fait de placer des clauses contractuelles au sein de ces dispositions n'enlève rien à leur signification juridique. Certaines d'entre elles devront peut-être être soigneusement examinées par les parties à la lumière des spécificités de l'informatique en nuage.

Q. Modification du contrat

169. L'une ou l'autre des parties pourrait vouloir apporter des modifications au contrat, conformément à la procédure à suivre indiquée dans le contrat pour introduire des modifications et les rendre effectives. Le contrat peut également devoir aborder les conséquences du rejet des modifications par l'une ou l'autre des parties.

170. Compte tenu de la nature de **l'informatique en nuage**, il pourrait être difficile de distinguer les changements qui modifieraient le contrat de ceux qui ne le feraient pas. Par exemple, l'utilisation par le client de n'importe quelle option mise à sa disposition dès l'entrée en vigueur du contrat ne constituerait pas nécessairement une modification du contrat initial, pas plus que des changements des services qui résulteraient de l'entretien ordinaire et d'autres activités du fournisseur prises en compte dans le contrat. L'ajout d'éléments non couverts dans les conditions initialement convenues et justifiant

ainsi des modifications de prix peut, en revanche, constituer une modification du contrat. Toute mise à jour entraînant des changements importants des conditions et politiques convenues antérieurement peut également constituer une modification du contrat. Des modifications substantielles des conditions matérielles du contrat initialement conclu (par exemple, l'arrêt de certains services d'informatique en nuage) peuvent effectivement conduire à un nouveau contrat.

171. L'ampleur des modifications susceptibles d'être apportées aux contrats publics peut être limitée par les règles de passation des marchés publics, qui restreignent généralement la liberté des parties de renégocier les clauses d'un marché ayant fait l'objet d'une procédure d'adjudication publique.

172. Compte tenu des modifications fréquentes des conditions initialement convenues, chaque partie peut souhaiter conserver sa propre copie de l'ensemble de ces conditions initialement convenues et leurs modifications.

Glossaire

Accord de niveau de service – Partie du contrat d'informatique en nuage entre le fournisseur et le client où sont indiqués les services d'informatique en nuage couverts par le contrat et les modalités de la prestation (les **paramètres de performance**) [lien de renvoi].

Agent chargé du contrôle des données – Personne qui décide de l'objet et des moyens du traitement des **données personnelles**.

Agent chargé du traitement des données – Personne qui traite les données pour le compte de **l'agent chargé du contrôle des données**.

Audit – Processus consistant à examiner le respect des prescriptions légales et contractuelles. Il peut couvrir des aspects techniques (tels que la qualité et la sécurité du matériel et des logiciels) ; le respect de toute norme sectorielle applicable ; et l'existence de mesures appropriées, y compris l'isolement, pour empêcher l'accès non autorisé au système et son utilisation et pour garantir l'intégrité des données. L'audit peut être interne (réalisé par le fournisseur de services), externe (réalisé par le client) ou indépendant (mené par un tiers indépendant nommé par le fournisseur ou par le client, ou par les deux parties).

Données dérivées des services en nuage – Données qui sont dérivées des services d'informatique en nuage proposés par un fournisseur et que celui-ci contrôle. Il s'agit notamment des **métadonnées** et de toutes autres données contenues dans les journaux tenus par les fournisseurs indiquant l'identité des utilisateurs des services, les dates et heures d'utilisation des services, les fonctions et les types de données mis en œuvre. Elles peuvent également englober des renseignements sur les utilisateurs autorisés, leurs identifiants, et les configurations, personnalisations et modifications éventuelles.

Données personnelles – Données qui peuvent servir à identifier la personne physique à laquelle elles se rapportent. Dans certains pays, la définition des données à caractère personnel peut englober toutes les données ou informations directement ou indirectement liées ou relatives à une personne identifiée ou identifiable (la **personne concernée**).

Droits des personnes concernées – Droits associés aux **données personnelles** des personnes concernées. En fonction des législations, les personnes concernées peuvent bénéficier du droit qu'on leur communique toutes les informations importantes relatives à leurs données personnelles, notamment l'emplacement de ces données, leur utilisation par des tiers, d'éventuelles fuites et autres violations. S'agissant de ces données personnelles, elles peuvent également disposer du droit d'accès à tout moment, du droit à l'effacement (par suite du droit à l'oubli), du droit d'en limiter le **traitement** et du droit à la **portabilité**.

Écrit ou **par écrit** – Informations qui doivent être accessibles de façon à pouvoir être utilisées pour s'y référer ultérieurement. Le terme s'applique à la fois aux informations en format papier et contenues dans une communication électronique. Le mot « accessible » implique que les informations se présentant sous la forme de données informatisées doivent être lisibles et interprétables et que le logiciel qui pourrait être nécessaire pour assurer leur lisibilité doit être conservé. Le terme « être utilisées » englobe à la fois l'usage par des personnes et le traitement informatique.

Exigences en matière de localisation des données – Exigences relatives à l'emplacement des données et d'autres contenus, des centres de données ou des fournisseurs. Elles peuvent interdire que certaines données (notamment des **métadonnées** et leurs sauvegardes) soient stockées dans certains territoires ou pays, ou y entrent ou en sortent, ou exiger pour ce faire l'autorisation préalable d'une instance publique compétente. Elles sont fréquemment énoncées dans des lois et règlements relatifs à la protection des données, lesquels sont susceptibles d'interdire en particulier que les **données personnelles** soient stockées ou passent dans des pays qui ne respectent pas certaines normes en matière de protection des **données personnelles**.

Exploitation des fuseaux horaires (« Follow-the-sun ») – Modèle dans lequel la charge de travail est répartie entre plusieurs sites géographiques de façon à mieux équilibrer les ressources et la demande. Ce modèle peut viser à fournir des services 24 heures sur 24 et à minimiser la distance moyenne entre les serveurs et les utilisateurs finaux pour essayer de limiter les **temps de latence** et de maximiser la vitesse de transmission des données entre appareils (taux de transfert des données ou débit).

IaaS (infrastructure en tant que service) – Types de **services d'informatique en nuage** par le biais desquels le client peut obtenir et utiliser des ressources liées au traitement, au stockage et aux réseaux. La gestion et le contrôle des ressources physiques ou virtuelles sous-jacentes ne relèvent pas du client mais ce dernier contrôle les systèmes d'exploitation, le stockage et les applications déployées qui font usage de ces ressources. Il peut également exercer un contrôle restreint sur certaines composantes des réseaux (par exemple les pare-feu hôtes).

Informatique en nuage – Offre et utilisation de **services d'informatique en nuage** par l'intermédiaire de réseaux ouverts ou fermés. Le système peut comporter les caractéristiques suivantes :

a) **Large accès au réseau** : possibilité d'accéder aux **services d'informatique en nuage** par l'intermédiaire du réseau à partir de tout endroit où celui-ci est disponible (par exemple par Internet), au moyen d'une gamme étendue d'appareils tels que téléphones mobiles, tablettes et ordinateurs portables ;

b) **Services mesurés** : Mesure des **services d'informatique en nuage** qui sont fournis, à l'instar de ce qui se fait dans les services publics (par exemple pour le gaz et l'électricité), ce qui permet de contrôler l'usage des ressources et de facturer en conséquence (**paiement à l'usage**) ;

c) **Architecture multilocataire** : Allocation des ressources physiques et virtuelles à de multiples utilisateurs dont les données sont conservées séparément et inaccessibles aux autres ;

d) **Libre-service à la demande** : Utilisation des **services d'informatique en nuage** par les clients selon leurs besoins, automatiquement ou avec un minimum d'interaction avec le fournisseur ;

e) **Élasticité et extensibilité** : Capacité d'adaptation rapide à la montée ou à la baisse de la consommation de **services d'informatique en nuage** selon les besoins des clients, notamment en ce qui concerne les tendances à grande échelle de l'usage de ressources (par exemple les variations saisonnières). L'élasticité et l'extensibilité portent non seulement sur les aspects quantitatifs du système mais aussi sur la qualité et la sécurité des mesures, susceptibles d'être adaptées aux différents niveaux de sensibilité des données stockées des clients ;

f) **Mutualisation des ressources** : Possibilité qu'a le fournisseur de regrouper les ressources physiques ou virtuelles pour servir un ou plusieurs clients, sans que ceux-ci contrôlent les processus en jeu ou en aient même connaissance.

Interopérabilité – Capacité de deux ou plusieurs systèmes ou applications à échanger des informations et à utiliser mutuellement les informations échangées.

Licences de propriété intellectuelle – Contrats conclus entre des titulaires de droits de propriété intellectuelle (donneurs de licence) et des personnes autorisées à utiliser ces droits (preneurs de licence). Ils imposent habituellement des restrictions et des obligations quant à la portée du contrat et à la manière dont le preneur de licence ou les tiers peuvent utiliser le bien sous licence. Par exemple, les logiciels et les contenus visuels (modèles, mises en page et images) peuvent faire l'objet d'une licence en vue d'une exploitation spécifique, ne permettant pas la copie, la modification ou l'amélioration, et être limités à un support donné. Les licences peuvent être limités d'un point de vue territorial (par exemple, marché national ou (sous-)régional), en ce qui concerne le nombre d'utilisateurs ou la durée du contrat. Les accords de sous-licence peuvent être interdits. Le donneur de licence peut exiger qu'il soit fait référence au titulaire des droits de propriété intellectuelle à chaque fois que ceux-ci sont utilisés.

Mesures post-incident – Mesures à prendre par le fournisseur, le client ou tous les deux, notamment en faisant intervenir un tiers, à la suite d'un incident de sécurité. Elles peuvent comprendre l'isolement ou la mise en quarantaine des zones touchées, l'analyse des causes profondes et l'élaboration d'un rapport d'analyse des incidents par la partie touchée, seule ou conjointement avec l'autre partie, ou par un tiers indépendant.

Métadonnées – Informations de base sur des données (comme l'auteur, la date de création, la date de modification et la taille du fichier). Elles contribuent à faciliter la recherche et l'utilisation des données et peuvent être requises pour garantir l'authenticité des archives au fil du temps. Elles peuvent être générées par le client ou par le fournisseur.

Modèles de déploiement – Différentes manières d'organiser l'informatique en nuage en fonction du contrôle et du partage des ressources physiques ou virtuelles :

a) **Nuage public** : Les **services informatiques en nuage** sont susceptibles d'être proposés à n'importe quel client et les ressources sont contrôlées par le fournisseur ;

b) **Nuage communautaire** : Les **services informatiques en nuage** sont mis à la disposition exclusive d'un groupe donné de clients liés les uns aux autres et ayant des exigences communes, et les ressources sont contrôlées par au moins un membre de ce groupe ;

c) **Nuage privé** : Les **services informatiques en nuage** sont mis à la disposition exclusive d'un seul client, qui contrôle les ressources ;

d) **Nuage hybride** : Solution intermédiaire faisant intervenir au moins deux modèles de déploiement différents.

Notification d'un incident de sécurité – Notification adressée aux parties concernées, aux autorités publiques ou au grand public au sujet d'un incident de sécurité. Elle peut indiquer les circonstances et la cause de l'incident, le type de données touchées, les mesures à prendre pour résoudre l'incident, le moment auquel l'incident devrait être résolu et tout plan d'urgence à mettre en œuvre pendant que l'incident est en cours de règlement. Elle peut également comporter des informations sur des violations n'ayant pas réussi, des attaques contre des cibles spécifiques (par utilisateur client, par application donnée, par appareil spécifique), des tendances et des statistiques.

Objectif de délai de reprise – Délai dans lequel tous les services d'informatique en nuage et les données doivent être rétablis à la suite d'une interruption imprévue.

Objectif de point de reprise – Durée maximale avant une interruption de service imprévue pendant laquelle les modifications des données peuvent être perdues par suite du rétablissement. Si le contrat précise un objectif de point de reprise équivalent à deux heures avant l'interruption des services, cela signifie que toutes les données devraient être accessibles après le rétablissement dans la forme où elles existaient deux heures avant l'interruption.

PaaS (plateforme en tant que service) – Types de **services d'informatique en nuage** par le biais desquels le client peut déployer, gérer et exploiter dans le nuage des applications ou des logiciels qu'il a créés ou acquis en mettant en œuvre un ou plusieurs langages de programmation et environnements d'exécution existants procurés par le fournisseur.

Paramètres de performance – Paramètres quantitatifs (liés à des objectifs, des indicateurs ou des fourchettes de performance chiffrés) ou qualitatifs (liés à l'assurance de la qualité des services). Ils peuvent être associés à la conformité aux normes applicables, y compris la date d'expiration de toute certification de conformité. Pour être significatifs, ils devraient viser à mesurer, de manière simple et vérifiable, les performances qui revêtent de l'importance pour le client. Ils peuvent varier en fonction des risques encourus et des besoins de l'entreprise (par exemple, la criticité de certains services, données ou applications et la priorité de restauration correspondante). Par exemple, un système non essentiel conçu pour utiliser le nuage à des fins d'archivage

n'aura pas besoin des mêmes conditions pour ce qui est des **temps de disponibilité** ou **d'autres accords de niveau de service** que des opérations essentielles ou en temps réel.

Partenaires de services d'informatique en nuage (notamment auditeurs de services en nuage, courtiers de services en nuage et intégrateurs de système) – Personnes qui mènent des activités de soutien ou auxiliaires à celles des fournisseurs, des clients ou des deux. Les auditeurs de services en nuage procèdent à des **audits** de la prestation et de l'utilisation de **services d'informatique en nuage**. Les courtiers de services en nuage apportent leur assistance aux parties à divers égards, par exemple pour trouver la meilleure solution en matière de nuage, négocier des conditions acceptables et organiser la migration du client vers le nuage.

Pérennité des données stockées – Probabilité que les données stockées dans le nuage ne soient pas perdues pendant la durée du contrat. Elle peut figurer dans le contrat comme une cible mesurable par rapport à laquelle le client évaluera les mesures prises par le fournisseur pour assurer la pérennité du stockage des données.

Politique d'utilisation acceptable – Partie du contrat d'informatique en nuage entre le fournisseur et le client où sont définies les limites de l'utilisation par le client et ses utilisateurs finaux des services d'informatique en nuage sur lesquels porte le contrat. Dans cette partie, il est précisé, par exemple, qu'il est interdit au client et à ses utilisateurs finaux de placer dans le nuage des contenus illicites ou autrement interdits et de les y utiliser [lien de renvoi].

Portabilité – Capacité de transférer facilement des données, des applications et d'autres contenus d'un système à l'autre (c'est-à-dire à faible coût, avec un minimum de perturbations et sans avoir à ressaisir les données, à réorganiser les processus ou à reprogrammer les applications). La portabilité peut exister s'il est possible de récupérer les données dans un format accepté dans un autre système ou par une transformation simple et directe à l'aide d'outils couramment disponibles.

Règlements sectoriels – Règlements sur les finances, la santé ou le secteur public, ou d'autres règlements sectoriels ou professionnels particuliers (par exemple en ce qui concerne le secret professionnel auquel sont tenus les avocats et les professionnels de santé) et règles relatives au traitement des informations classifiées (à savoir, au sens large, les informations auxquelles seules certaines catégories données de personnes ont accès de par la loi ou un règlement).

Représentant de l'insolvabilité – Personne ou organe habilité à administrer le redressement ou la liquidation des biens du fournisseur insolvable dans le cadre d'une procédure d'insolvabilité.

Réversibilité – Processus permettant au client d'extraire ses données, applications et autres contenus connexes du nuage, et au fournisseur de supprimer les données du client et autres contenus connexes après une période convenue.

SaaS (logiciels en tant que service) – Types de **services d'informatique en nuage** par le biais desquels le client peut utiliser les logiciels et applications du fournisseur dans le nuage.

Services d'informatique en nuage – Services fournis par l'intermédiaire de **l'informatique en nuage**. Ils varient et ils évoluent constamment. Il peut s'agir uniquement de connectivité et de services informatiques de base (comme le stockage, les courriers électroniques et des applications bureautiques). Les services peuvent toutefois inclure également la prestation et l'utilisation de la gamme entière des infrastructures physiques des technologies de l'information (comme les serveurs et les centres de données) et les ressources virtuelles requises pour créer des plateformes maison, ou déployer, gérer et exploiter des applications ou des logiciels créés ou acquis par les clients. L'infrastructure en tant que service (**Iaas**), la plateforme en tant que service (**PaaS**) et les logiciels en tant que service (**SaaS**) représentent différents types de services dans le nuage.

Services d'informatique en nuage en couches – Dans ce cadre, le fournisseur n'est propriétaire que d'une partie, voire d'aucune, des ressources informatiques qu'il utilise

pour fournir des services d'informatique en nuage à ses clients ; il est lui-même un client qui se fait fournir des **services d'informatique en nuage**, en tout ou en partie. Par exemple, le fournisseur de services de type **PaaS** ou **SaaS** peut utiliser les infrastructures de stockage et de serveur (centres de données, serveurs de données) dont une autre entité est propriétaire ou qu'elle fournit. Par conséquent, un ou plusieurs sous-traitants peuvent intervenir dans la prestation des services d'informatique en nuage au client. Ce dernier ne saura pas nécessairement quelles couches participent à la prestation de services à un moment donné, ce qui complique l'identification et la gestion des risques. Les **services d'informatique en nuage en couches** sont fréquents en particulier dans le modèle **SaaS**.

Solutions d'informatique en nuage normalisées pour multiabonnés – **Services d'informatique en nuage** fournis à un nombre illimité de clients en tant que ressource ou produit de masse, à des conditions standard non négociables déterminées par le fournisseur. De larges exclusions et des renonciations en matière de responsabilité du fournisseur sont courantes dans ce type de solution. Le client peut se renseigner et comparer différents fournisseurs et leurs contrats et choisir ceux qui correspondent le mieux à ses besoins, mais il ne pourra pas négocier son contrat.

Temps d'arrêt ou pannes – Périodes pendant lesquelles les clients n'ont pas accès aux services d'informatique en nuage. Ces périodes sont exclues du calcul du **temps de disponibilité** ou de fonctionnement sans interruption. On inclut généralement dans le temps d'arrêt les durées consacrées à la maintenance et aux mises à jour.

Temps de disponibilité – Durée pendant laquelle les services d'informatique en nuage sont accessibles et susceptibles d'être utilisés.

Temps de latence – Du point de vue du client, délai entre sa demande et la réponse du fournisseur. Ce temps de latence affecte l'exploitabilité pratique des **services d'informatique en nuage**.

Temps de réaction initiale – Délai qui s'écoule entre le moment où un client signale un incident et la première réaction du fournisseur.

Traitement [des données personnelles] – Collecte, enregistrement, organisation, stockage, adaptation ou altération, extraction, consultation, utilisation, divulgation par transmission, diffusion ou toute autre forme de mise à disposition, alignement ou combinaison, blocage, effacement ou destruction de données.

Verrouillage – Situation dans laquelle les coûts liés au changement de prestataire étant considérables, le client dépend d'un fournisseur unique. Dans ce contexte, la notion de coût s'entend au sens large comme englobant non seulement les dépenses monétaires, mais aussi l'effort, le temps et les aspects relationnels. Les risques de verrouillage des applications et des données peuvent être élevés dans les modèles **SaaS** et **PaaS**. Les données peuvent exister dans des formats spécifiques au système infonuagique du fournisseur et ne pas être utilisables dans d'autres systèmes. En outre, le fournisseur peut utiliser une application ou une technologie propriétaire pour organiser les données du client, d'où la nécessité d'ajuster les conditions de licence pour permettre l'exploitation en dehors du réseau du fournisseur. Dans le modèle **PaaS**, il pourrait aussi y avoir un verrouillage des logiciels d'exécution puisque ces derniers (à savoir les logiciels conçus pour permettre l'exécution de programmes informatiques créés avec un langage de programmation spécifique) sont souvent fortement customisés (par exemple pour des aspects tels que l'allocation ou la libération de mémoire, le débogage, etc.). Dans le modèle **IaaS**, si le verrouillage varie en fonction de la consommation spécifique des services d'infrastructure, le client peut également faire face au verrouillage des applications si le service dépend de certaines caractéristiques de la politique du fournisseur (par exemple, les contrôles d'accès) ou au verrouillage des données si de plus nombreuses données sont déplacées vers le nuage pour y être stockées.