Alan WALTER
Avocat au Barreau de Paris

Tél : 06 20 42 53 33 – E-mail : alan.walter@runbox.com
73 rue de Courcelles – 75008 Paris – Palais D 1891

A : **Stéphane Lubiarz / Jean-Paul Smets**

OBJET : **Cloud et sécurité des données**

DATE : 16 janvier 2015

Bien avant les premières révélations d'Edward Snowden en juin 2003 et le scandale « Prism » qui éclata en juin 2013, le souci de la confidentialité des données a toujours constitué une question de premier plan les utilisateurs de l'internet.

Après les premiers virus informatiques de grande envergure[1] et depuis le début des années 2000, point de départ de la généralisation massive de l'internet auprès du grand public, ont émergé les préoccupations liées à la sécurité informatique, la cybercriminalité, la cryptographie…

En ce début d'année, après les attentats survenus à Paris, il est désormais question d'un « *Patriot Act* » à la française, jugeant que la loi de lutte contre le terrorisme adoptée en octobre 2014[2] ne fournirait pas suffisamment de moyens aux services de renseignement.

Indépendamment des questions relatives à la lutte contre le terrorisme, ces préoccupations ont pu se renforcer pour tous les usages d'outils informatiques avec l'arrivée du Cloud Computing : des infrastructures lourdes qui promettent de simplifier les usages d'Internet et de réduire les coûts d'exploitation pour les entreprises grâce à l'automatisation et à la centralisation des traitements de données dans un nombre restreint de centres de données géants. Le Cloud se targue en outre de pouvoir répondre aux exigences de sécurisation de ses clients grâce à la centralisation des politiques de sécurité par du personnel compétent.

Mas le passage d'une informatique physique aux serveurs répartis et identifiés par l'utilisateur à une informatique virtualisée aux serveurs sous contrôle du fournisseur n'a fait qu'opacifier les mesures et processus mis en œuvre, complexifier les questions et, *in fine*, aggraver la situation.

Et pour cause ! L'informatique « individuelle » reposait sur une architecture simple : les données étaient stockées dans un serveur physique détenu par une entité unique, implantée dans un seul pays et soumise à un droit homogène et identifiable. La sécurité des données était alors assurée, celles-ci n'étant mises en risques que lorsqu'elles transitaient sur les réseaux.

A l'inverse, dans le Cloud, en dépit d'une concentration indéniable du marché des prestataires, les données sont réparties sur plusieurs infrastructures techniques, potentiellement opérées par des prestataires distincts, dans plusieurs pays, sous l'empire de corpus législatifs disparates.

Au surplus, ces infrastructures lourdes et complexes n'étant mise en œuvres et commercialisées que par des géants de l'industrie, ces derniers ont toute latitude pour imposer leurs conditions aux utilisateurs.

Ainsi, indépendamment des aspects techniques, le Cloud ne semble pas aujourd'hui en mesure d'offrir à ses utilisateurs les garanties satisfaisantes au regard de la sécurité et de la confidentialité de leurs données.

Les développements ci-après ont pour objet l'analyse des principaux obstacles réglementaires et contractuels qui contredisent l'impression de sécurité que confèrent les offres de Cloud aujourd'hui disponibles.

1Notamment l'apparition de « Jérusalem » en 1987.

2Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme.

1 LA « SÉCURITÉ » N'EST PAS NÉCESSAIREMENT SYNONYME DE « SÉCURITÉ DES DONNÉES »

« *La sécurité est un droit fondamental* », proclamait l'article 1er de la loi relative à la sécurité quotidienne jusqu'à son abrogation[3].

Mais quelle sécurité ?

Probablement celle des personnes mais certainement pas celle des données.

Depuis la signature de la Convention sur la cybercriminalité à Budapest le 23 novembre 2001, les pays membres du G8 ont décidé de se doter d'un arsenal juridique leur permettant de lutter contre la criminalité informatisée et la criminalité informatique, toutes deux désignées comme la « cybercriminalité »[4].

A la suite des évènements du 11 septembre 2001, les pays membres du G8 ont formulé un certain nombre de recommandations visant à renforcer leur présence sur le réseau et à étendre leurs facultés d'intervention.

S'en suivirent, en France, un certain nombre de textes législatifs visant à assurer à l'Etat un accès rapide et permanent aux données informatiques des personnes privées (**Error: Reference source not found**), imposant aux prestataires techniques une obligation de conservation (**Error: Reference source not found**).

1. Procédures de droit commun permettant l'accès aux données d'un tiers : les procédures sur requête

1. En matière d'atteinte aux droits de propriété intellectuelle, par le biais de la saisie-contrefaçon[5], ou bien, dans toutes les autres matières, par le biais de la procédure *in futurum*[6], toute personne peut requérir du juge que soient mises en œuvre des mesures d'instruction.

En matière de propriété intellectuelle et/ou industrielle, ces dispositions légales permettent donc, à celui qui pourra démontrer avoir un intérêt et la qualité pour agir, de voir ordonnées « *toute mesure urgente destinée à prévenir une atteinte aux droits [...] ou à empêcher la poursuite d'actes portant prétendument atteinte à ceux-ci* »[7].

De la même façon, dans toute autre matière, notamment dans le cadre d'un contentieux civil ou commercial, « *S'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé* »[8].

2. Ainsi, dès lors que la compétence des juridictions françaises sera reconnue, toute donnée hébergée pourra être extraite et copiée en application d'une ordonnance rendue au visa de l'un de ces textes.

Il convient de préciser que, sous réserve de justifier de sa demande auprès du magistrat compétent, le demandeur pourra agir sur requête, c'est-à-dire en dérogeant au principe du contradictoire.

3Article 1er de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité introduit par la loi **n**° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et abrogé par l'ordonnance n° 2012-351 du 12 mars 2012 - art. 19 (V).

4Convention consultable à l'adresse <http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm>.

5Selon que l'affaire concerne de la contrefaçon de droit d'auteur, de marque, de brevet, de logiciel et/ou de base de données, les textes applicables diffèrent mais restent similaires.

6Cf. Article 145 et suivants du code de procédure civile.

7Extrait de l'article L 343-2 du code de la propriété intellectuelle.

8Article 145 du code de procédure civile.

Dans une telle hypothèse, ni le propriétaire ni le détenteur des données ne seront informés de la mise en œuvre d'une telle procédure.

Si le détenteur des données (le plus souvent l'hébergeur) sera informé de la mesure d'instruction lors de sa mise en œuvre, celui qui en est le propriétaire, quant à lui, pourra ne jamais être informé d'un tel accès à ses données.

3. S'agissant des ordonnances rendues sur requête, la problématique principale est celle du respect des droits de la défense. En effet, dans une telle hypothèse, celui dont les données sont saisies dispose bien entendu de voies de recours, sous réserve qu'il ait été informé de l'identité du saisissant, ce qui peut ne pas toujours être le cas.

En tout état de cause, aucune de ces saisies ne saurait intervenir sans un contrôle préalable exercé par le juge : la requête aux fins de saisie doit être examinée et validée par un juge, ce dernier étant tenu de s'assurer, lors dudit examen, que la dérogation au principe du contradictoire est justifiée et que la mesure d'instruction sollicitée ne pourra être « *un moyen détourné pour obtenir des informations confidentielles de son concurrent sur son activité, sa clientèle ou son savoir-faire* »[9].

Dans de telles conditions, aucune donnée stockée sur un cloud auprès d'un prestataire soumis à la législation française n'est réellement sécurisée : le prestataire ne pourra refuser de communiquer les informations requises sous peine d'engager sa responsabilité pénale.

2. Le régime d'accès aux données dans les enquêtes de police et par les administrations françaises

Devant la généralisation de la cybercriminalité, le pouvoir judiciaire s'est doté de la possibilité d'intervenir sur les outils informatiques dans le cadre de toute enquête.

1 - A cette fin, l'article 56 du code de procédure pénale dispose que :

> « *Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, **données informatiques** ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal* ».

De la même façon, l'article 60-1 de ce code autorise le procureur de la République et les officiers de police judiciaire à contraindre toute personne (privée ou publique) à leur remettre des informations dans le cadre d'une enquête de flagrance.[10]

Egalement, dans le cadre des perquisitions et saisies, l'article 97 du même code dispose qu'il est possible de procéder à :

> « *la **saisie des données informatiques nécessaires à la manifestation de la vérité** en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition* ».

4. Par ailleurs, sous couvert d'extension de la lutte contre la cybercriminalité, cette faculté a été étendue, par le biais de l'article 62 de la loi de finances rectificative pour 2001, aux agents du trésor public, des douanes et de l'AMF.[11]

9TC Châteauroux, 24 jan. 2007, RG : 2006/882, à rapprocher de Cour d'appel de Paris – Pôle 1 Chambre 4 – 11 mars 2010 n°0 913 381 s'agissant d'un huissier qui excède les limites de sa mission et ainsi aggrave le risque d'atteinte à la confidentialité des données informatiques copiées.

10Sur la modification de ce texte et le remplacement du terme « *documents* » par le terme « *informations* », cf. infra 1.3.

11Article 62 de la loi n° 2001-1276 du 28 décembre 2001 de Finances rectificative pour 2001 qui a modifié l'article 65 du Code des douanes, l'article L 621-10 du Code monétaire et financier et l'article

Depuis lors, chaque agent de ces administrations dispose de la faculté d'exiger la communication de toute information et documents auprès des « *opérateurs de télécommunication* »[12].

Il convient alors de s'interroger sur la définition, très large, de l'« *opérateur de télécommunication* », à savoir « *une entreprise qui fournit ou est autorisée à fournir un réseau de communications public ou une ressource associée* »[13].

Face à la rédaction de cette définition et en particulier de la référence à une « *ressource associée* », force est de constater que tout acteur de l'internet, qu'il soit fournisseur d'accès, hébergeur ou même fournisseur de *caching* se verra soumis à ces dispositions qui permettent un accès par diverses administrations.

3. Sécurité intérieure, programmation militaire et lutte contre le terrorisme : des possibilités d'accès accrues

1 - Le code de la sécurité intérieur, qui prévoit le régime des interceptions de sécurité et de l'accès administratif aux données de connexion, a été complété par la loi de programmation militaire de 2013.[14]

Désormais, les articles L 246-1 de ce code autorise :

> « *le recueil, auprès des opérateurs de communications électroniques* [, des hébergeurs et des fournisseurs d'accès] *des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications* ».

Outre les données en elle-même, ce sont également les informations relatives à l'utilisateur (les métadonnées), en ce compris les données de géolocalisation, qui peuvent être demandées par des « *agents individuellement désignés et dûment habilités des services relevant des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget* ».[15]

Il convient de relever que le champ de mise en œuvre de telles interceptions est des plus larges, dans la mesure où l'interception réalisée sur le fondement du code de la sécurité intérieure peut avoir lieu pour « *rechercher des renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous* ».

A la lecture de cet article, force est de constater que ce régime d'interception n'a pas vocation à s'appliquer en matière militaire mais également en matière économique ou, plus généralement, pour la prévention « *de la criminalité et de la délinquance organisées* ».

L 83 du Livre des procédures fiscales.

12On notera l'absence de mise à jour de cette disposition qui fait encore référence non seulement au terme « télécommunications » alors que celui-ci a depuis plusieurs années été remplacé par l'expression « *communications électronique* » mais aussi à des articles abrogés.

13Directive 2002/19/CE du Parlement Européen et du Conseil du 7 mars 2002 relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion (directive « *accès* »).

14Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

15Article L 246-2 du code de la sécurité intérieure.

5. Depuis 2012, le code de la sécurité intérieur prévoit même une obligation à la charge des prestataires de cryptographie, lesquels seront contraints, sur demande des agents autorisés, « *de remettre [...] les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies* ».

Dans une telle hypothèse, sauf à démontrer qu'il est techniquement dans l'impossibilité d'y parvenir, le prestataire en cause pourra même être contraint de procéder lui-même au décryptage des données qui auront été cryptées au moyen du système qu'il aura fourni.

6. La Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a pour sa part étendu les pouvoirs d'investigations de la police durant les enquêtes de flagrance, en remplaçant, à l'article 60-1 du code de procédure pénale le terme « *documents* » par le terme « *informations* », aboutissant à la rédaction suivante :

   « *Le procureur de la République ou l'officier de police judiciaire peut, par tout moyen, requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des informations intéressant l'enquête, y compris celles issues d'un système informatique ou d'un traitement de données nominatives, de lui remettre ces informations, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel.[...]* ».

La nouvelle rédaction de ce texte contraint donc tout prestataire informatique établi en France à fournir toute information, quelle que soit sa nature, lorsque la demande lui en faîte dans le cadre d'une enquête de flagrance, y compris lorsque ladite enquête ne sera pas en lien direct avec des activités terroristes.

2 L'OBLIGATION DE CONSERVATION DES DONNÉES IMPOSÉE AUX PRESTATAIRES TECHNIQUES

L'universalité de la faculté d'accès aux données constatée, il est nécessaire de s'interroger sur la possibilité d'obtenir les données d'identification d'un internaute et d'autres métadonnées afférentes.

1 - Avant même la promulgation de la loi de lutte contre le terrorisme, l'article 6 II de la loi pour la confiance dans l'économie numérique (« **LCEN** »)[16] prévoit que « *les* [fournisseurs d'accès à internet[17]] *et* [hébergeurs[18]] *détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires* ».

Dans le même esprit que la définition des opérateurs de communications électroniques, la définition des hébergeurs est suffisamment large pour englober non seulement les hébergeurs de sites web mais également tous les hébergeurs de solutions en ligne, cloud compris.

Cette obligation de conservation assure bien entendu l'efficacité des dispositions précitées (cf. supra).

7. Cet article 6 II de la LCEN est complété par les dispositions d'un décret *ad hoc*[19], l'article 1 2° duquel précise que les hébergeurs doivent conserver :

   « *a) L'identifiant de la connexion à l'origine de la communication ;*

16Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

17Définis comme « *Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* » (Article 6 I 1° de la LCEN).

18Définis comme « *Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* » (Article 6 I 2° de la LCEN).

19Décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

b) L'identifiant attribué par le système d'information au contenu, objet de l'opération ;

c) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ;

d) La nature de l'opération ;

e) Les date et heure de l'opération ;

f) L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni ».

Au surplus, l'article 1 3° de ce décret, afin de s'assurer de la capacité à identifier le propriétaire des informations détenues, impose également aux hébergeurs, lors de la souscription du contrat, de recueillir :

« *a) Au moment de la création du compte, l'identifiant de cette connexion ;*

b) Les nom et prénom ou la raison sociale ;

c) Les adresses postales associées ;

d) Les pseudonymes utilisés ;

e) Les adresses de courrier électronique ou de compte associées ;

f) Les numéros de téléphone ;

g) Le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour ».

On remarquera bien entendu en particulier les stipulations de l'alinéa g) qui imposent que soient conservés le mot de passe ainsi que les moyens de le modifier et/ou de la vérifier.

Sur ce point, la conservation de la « question secrète » ne pose pas question. Toutefois, il n'en va pas de même pour la conservation du mot de passe en lui-même. Cette conservation pose en effet un double problème : d'abord de capacité technique mais aussi et surtout de respect de la vie privée.

Sur le plan de la vie privée, il apparaît parfaitement choquant qu'un prestataire technique conserve, en clair, le mot de passe de ses utilisateurs et, pis encore, soit contraint de le communiquer si la demande lui en était faite.

La pertinence de cette disposition peut être discutée dans la mesure où, sur réquisition, tout prestataire est tenu de fournir les données qu'il détient. Ainsi, quelle peut être l'utilité de la conservation des mots de passe, si ce n'est leur éventuelle utilisation pour accéder à des services qui seraient hors du champ d'action des dispositions légales permettant un accès aux données fondé ?

8. En tout état de cause, il est par ailleurs précisé par l'article 3 de ce même décret que les données sont conservées pendant une durée d'un an.

9. Par ces dispositions, fortement critiquées lors de leur adoption, les pouvoirs publics se sont assurés, tant pour les personnes privées que pour les administrations d'Etat, de la possibilité de saisir tout contenu accessible en ligne et de pouvoir en identifier l'auteur.

Cette obligation qui pèse sur les hébergeurs, couplée aux facultés d'accès aux données qui sont ouvertes tant aux personnes publiques qu'aux personnes privées permettent de douter avec force de la sécurité réellement possible s'agissant de l'accès par des tiers aux données hébergées dans un cloud.

3 CLAUSE CONTRACTUELLES ET SÉCURITÉ DES DONNÉES OU « COMMENT NE RIEN PROMETTRE »

Il est usuel dans le milieu de l'informatique de négocier ses différents contrats, étant entendu que tant le client que le prestataire tenteront chacun de protéger leurs intérêts au mieux, sans pour autant nuire à l'équilibre général de la relation contractuelle.

Dans le domaine du cloud, nombre de contrats se révèlent être contrats d'adhésion sur lesquels le client n'a pas de prise[20].

Une analyse de ces contrats permet aisément de démontrer que le prestataire n'offre pas ou peu de garanties (**Error: Reference source not found**) et limite, voire exclut, autant que possible sa responsabilité en cas de défaillance du service (**Error: Reference source not found**).

4. Exclusions de garantie

Une analyse des conditions générales de services des principaux prestataires de Cloud permet de relever que les garanties fournies en standard sont quasi-inexistantes.

1. *Exclusion générale de toutes les garanties non prévues au contrat*

Il convient de constater que, parmi les contrats analysés, la totalité exclu les garanties suivantes :

1 - "*merchantability*", généralement usitée dans les seuls contrats de droit anglo-saxon, cette garantie vise les qualités du produit et leur respect des standards en vigueur permettant sa mise sur le marché.

L'exclusion de cette garantie pourra permettre au prestataire, dans l'hypothèse où son produit ne serait pas jugé conforme aux standards du marché, d'exclure tout ou partie de sa responsabilité vis-à-vis du client.

10. "*fitness for [a particular] purpose*" qui protégé le prestataire dans l'hypothèse où le service fourni ne serait pas en adéquation avec les besoins du client.

De manière générale, le vendeur professionnel[21], en tant que « *sachant* », est tenu à une obligation de conseil. En effet, la jurisprudence constante considère que : « *tout vendeur doit, afin que la vente soit conclue en connaissance de cause, s'informer des besoins de l'acheteur et informer ensuite celui-ci des contraintes techniques de la chose vendue et de son aptitude à atteindre le but recherché* »[22].

En excluant cette garantie, le prestataire édulcore son obligation d'information, limitant ainsi les possibilités de recours pour les clients.

11. "*satisfactory quality*", probablement l'exclusion la plus surprenante, par laquelle le prestataire indique, sans ambiguïté, que son service pourrait ne pas être d'une qualité jugée « satisfaisante ».

Il convient ici de renvoyer à la notion d'obligations essentielles. En effet, si le prestataire venait, par le truchement de cette clause, à vider le contrat de se substance de sorte qu'il ne serait plus tenu à aucun engagement, le droit français tendrait à l'annulation de cette stipulation.

Néanmoins, dans l'hypothèse de l'application d'un droit étranger, il ne peut être préjuge de la validité ou de l'invalidité d'une telle clause, laquelle pourrait s'avérer dévastatrice pour un client qui souhaiterait engager une action à l'encontre de son prestataire.

20Il a été procédé à l'analyse des conditions générales des services suivants : « *Cloud Terms of Service RackSpace US* » ; « *CloudSigma Terms of Service* » et « *Amazon Web Services Customer Agreement* ».

21La notion de « vendeur » est ici entendue au sens large et pas seulement dans son acception stricte de « *transfert de propriété* ». Ainsi, l'obligation de conseil pourra être invoquée dans le cadre d'une licence de logiciel ou bien d'un contrat de prestation de services.

22Cass. com., 5 janv. 1999 ; pourvoi n° 96-16 521.

12. "*quiet enjoyment*" et "*non-infringement*" : il s'agit ici de la garantie d'éviction et de son pendant en matière de propriété intellectuelle ; la garantie de contrefaçon.

Ces garanties permettent au client d'avoir un recours dans l'hypothèse où les éléments qui lui sont fournis (i.e. services, logiciels, documentation…) en application du contrat porteraient atteinte aux droits de tiers (e.g. contrefaçon, concurrence déloyale…). Même si elle n'a pas directement trait aux données des utilisateurs, elle permet d'assurer une continuité de service dans l'éventualité visée ci-avant.

En l'absence d'une telle garantie, le client n'aura que très peu de recours à sa disposition dans l'hypothèse d'une action dirigée par un tiers qui considèrerait que le produit en cause porte atteinte à ses droits.

13. De la même façon, il est généralement indiqué que le service ne sera pas ininterrompu et/ou exempt de bugs et erreurs.

Lorsque la prestation concerne la seule délivrance d'un logiciel (à l'exclusion de toute autre prestation ou fourniture de matériels associés), ce qui empêche de qualifier le contrat de « vente », la jurisprudence admet que la présence de « bugs » est inhérente à la matière[23].

Ainsi, sauf à démontrer que le contrat pouvait être qualifié de vente ou bien à invoquer un engagement contractuel spécifique, une exclusion de garantie relative à la subsistance de bugs reste valable, laissant le client à la merci d'une action corrective du prestataire.

2. Exclusion de toute garantie relative aux données

De manière bien plus spécifique, il convient de relever que les contrats étudiés excluent de manière systématique toute obligation relative aux données.

Quelques exemples de clause permettent d'appréhender l'étendue de ces exclusions :

- "*to be* ***solely and entirely responsible for maintaining at least one current backup copy outside of CloudSigma's network of all data*** *(including but not limited to operating systems, content and programs) stored on CloudSigma's network to ensure that the potential for losses is mitigated*" ;

1. "*We make no representations or warranties that the Services will be […] secure or that* ***data stored using the Services will be secure or otherwise safe from loss or damage***" ;

2. "***You are responsible for*** *properly configuring and using the Service Offerings and* ***taking your own steps to maintain appropriate security, protection and backup of Your Content****, which may include the use of encryption technology to protect Your Content from unauthorized access and routine archiving Your Content*" ;

3. "***Any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of your content or other data***" ;

4. "*You acknowledge that* ***there are risks inherent in Internet connectivity that could result in the loss of your privacy, Customer Data, Confidential Information****, and property*".

Le client étant informé dès la conclusion du contrat qu'aucune garantie n'est prise et que toute responsabilité est exclue relativement à ses données, il ne pourra que très difficilement rechercher la responsabilité du prestataire de ce fait.

L'insertion de cette clause rend nulle ou difficilement applicable tout autre engagement pris par le prestataire en termes de qualité de services.

23CA Paris 5e Ch. 7-2-1986, Caisse de retraite des notaires c/ MAP Informatique : Expertises 1986 n°87 p.235.

5. Limitation de responsabilité

1 - Les prestataires n'hésitent pas à limiter voire exclure totalement leur responsabilité aux termes des différents contrats.

Pour ce faire, ils peuvent (i) exclure leur responsabilité en cas de survenance de certains dommages listés au contrat, (ii) prévoir que le service est fourni « en l'état », excluant ainsi totalement la mise en jeu de leur responsabilité ; ou bien (iii) en limitant par avance le montant des dommages et intérêts qu'ils sont susceptibles de verser en cas de condamnation.

14. Quelques exemples parmi les plus parlants :

5. « *the immediately preceding month in which the event (or first in a series of connected events) occurred*" ;

6. "*The service offerings are provided "*as is*"*." ;

7. "*we and our affiliates or licensors will not be liable to you for any direct, indirect, incidental, special, consequential or exemplary damages (including damages for loss of profits, goodwill, use, or data)*" ;

8. "*our and our affiliates' and licensors' aggregate liability under this agreement will be limited to the amount you actually pay us under this agreement for the service that gave rise to the claim during the 12 months preceding the claim*".

En choisissant voir cumulant ce type de formulations, le prestataire se met donc à l'abri de nombreuses difficultés.

15. De manière indirecte, en prévoyant généralement des définitions extensives de la "force majeure", les prestataires se réservent par-là la possibilité d'exclure leur responsabilité en cas de virus informatique.

En effet, pour être qualifié de cas de force majeure et ne pas engager la responsabilité des parties en cas d'inexécution, l'évènement en cause doit remplir trois critères cumulatifs, à savoir être extérieure aux parties (même si ce dernier critère n'est plus retenu de manière aussi absolue), imprévisible et irrésistible[24].

Même si la jurisprudence est rare sur cette question, certaines décisions nous renseignent sur la question de la responsabilité de celui qui transmettrait un virus.

En l'état actuel de la jurisprudence, même si le virus informatique est « un risque connu dans le domaine informatique », rien n'empêche que son caractère imprévisible (par son ampleur ?) et irrésistible (faute de moyen pour combattre efficacement un nouveau virus ?) pourrait être démontrés[25].

Dans une telle hypothèse, un prestataire pourrait ainsi exclure sa responsabilité.

1. *Le plafonnement voir l'exclusion de responsabilité, même rédigés de manière très large, peuvent être valables*

Laissé à la libre appréciation des parties en raison de la liberté contractuelle, l'aménagement de la responsabilité est de droit.

Contrairement à la responsabilité délictuelle (lorsque la faute à l'origine du dommage est constitutive d'une infraction), la responsabilité contractuelle peut donc être encadrée, limitée ou exclue, d'un

24Article 1148 du Code civil et, pour la définition des trois critères, Cass. Soc. 16 mai 2013, pourvoir n° : 10-17.726. S'agissant d'un certain relâchement quant à l'exigence du caractère d'extériorité, voir : Cass. Civ. , 30 oct. 2008 : Bull. Civ. I, n°243.

25Cass. Com. 25 novembre 1997, jursidata : 1997-004 692.

commun accord entre les parties[26], sauf dans certaines circonstances, limitativement énumérées par la loi et la jurisprudence :

9. le dol[27]. Si le dol est prouvé, la convention se trouve annulée, faisant perdre toute efficacité aux clauses qu'elle contient. Dès lors, toute limitation ou exclusion ne peut plus trouver à s'appliquer ;

10. la faute lourde, qui entraîne l'inefficacité de la clause de responsabilité, car elle est la faute grossière, quasi-inexcusable, la « *négligence grossière que l'homme le moins averti ne commettrait pas dans la gestion de ses propres affaires* »[28] ;

11. les dommages aux personnes, qui, de jurisprudence constante, rendent nulle toute clause de limitation ou d'exclusion de la responsabilité[29].

Pendant longtemps, les tribunaux français ont hésité sur le sort à réserver aux clauses qui aménagent la responsabilité des parties en cas de manquement à une obligation essentielle.

En effet, comment ne pas considérer qu'un tel manquement, s'il n'est pas (ou peu) réparé, reviendrait à vider de sa substance le contrat en permettant aux parties de ne pas se soumettre aux obligations qu'elles ont contracté[30].

Toutefois, cette position des juridictions des juridictions françaises s'est depuis lors infléchi, considérant qu'il peut ressortir de l'équilibre général du contrat une limitation des engagements du prestataire, lequel peut valablement aménager, limiter et/ou exclure sa responsabilité[31].

** *

* *

26Cass. Crim. 12 décembre 1946, JCP 1947, II, 3621, note R. Rodière.

27Cf. article 1116 du code civil : « *Le dol est une cause de nullité de la convention lorsque les manœuvres pratiquées par l'une des parties sont telles, qu'il est évident que, sans ces manœuvres, l'autre partie n'aurait pas contracté* ».

28Cass. Civ. 1er mai 1983 : D. 1983 IR p. 256.

29CA Toulouse, 23 octobre 1931 : D. 1935 II p.49 note L. Mazaud.

30Voir sur ce point les décisions « Chronopost », en particulier Cass. Com. 22 octobre 1996, Contrats conc. consom. 19 987, p. 0 note anonyme.

31Cass. civ. 1e, 24 février 1993