Alan WALTER
*Avocat au Barreau de Paris*

Tél : 01 45 01 45 01 – Fax : 01 45 01 45 00 – E-mail : alan.walter@runbox.com
51, rue Dumont d’Urvil e – 75116 Paris – Palais P 449

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

OBJET  :
**Cloud et sécurité des données**
DATE  :
13 septembre 2013

Bien  avant  les  révélations  d’Edward  Snowden  et  le  scandale  « Prism »,  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  envergure1  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…
Revenant  aux  principes  mêmes  de  l’internet  en  allant  jusqu’à  appliquer  la  logique  de  réseau
décentralisé  aux  infrastructures  elles-mêmes,  le  Cloud  se  targue  de  pouvoir  répondre  aux
exigences de sécurisation de ses clients.
Néanmoins,  le  passage  d’une  informatique  aux  serveurs  physiques  et  identifiés  à  une
informatique  dans  les  nuages  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 « centralisée » reposait sur une architecture simple : les données
étaient  détenues  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  morcelées  sur  plusieurs  infrastructures  techniques,  potentiellement  opérées
par  des  prestataires  distincts,  dans  plusieurs  pays,  sous  l’empire  de  corpus  législatifs
divergents.
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  confère  les  offres  de  Cloud
aujourd’hui disponibles.

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


**1**
**LA « SECURITE » N’EST PAS NECESSAIREMENT SYNONYME DE « SECURITE DES DONNEES »**
« *La  sécurité  est  un  droit  fondamental* »,  proclamait  l’article  1er  de  la  loi  relative  à  la  sécurité
quotidienne jusqu’à son abrogation2.
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 »3.
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  (**1.1**),  imposant
aux prestataires techniques une obligation de conservation (**1.2**).
**1.1**
**Le régime d’accès aux données par les administration 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, dans le cadre des perquisitions et saisies, l’article 97 du code de procédure
pénale 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* ».
Néanmoins, 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.4
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* »5.

2 Article 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).
3 Convention consultable à l’adresse <http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm>.
4 Article 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 L 83 du Livre des procédures fiscales.
Alan WALTER
2 / 10
  *13 septembre 2013*


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* »6.
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.
**2 -**Toutefois,  les  administrations  ne  sont  pas  seules  à  pouvoir  accéder  légalement  aux
données stockées par un tiers.
En  effet,  en  matière  d’atteinte  aux  droits  de  propriété  intellectuelle,  par  le  biais  de  la  saisie-
contrefaçon7, ou bien, dans toutes les autres matières, par le biais de la procédure *in futurum*8,
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* »9.
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* »10.
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.
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 -**Tel  qu’exposé  précédemment,  les  données  stockées  par  les  prestataires  techniques  de
l’économie numérique peuvent donc être l’objet d’intrusions légales par les autorités judiciaires
et/ou administratives.

5 On 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.
6 Directive 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* »).
7 Selon 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.
8 Cf. Article 145 et suivants du code de procédure civile.
9 Extrait de l’article L 343-2 du code de la propriété intellectuelle.
10 Article 145 du code de procédure civile.
Alan WALTER
3 / 10
  *13 septembre 2013*


S’agissant des ordonnances rendues sur requête, il s’agit bien entendu d’un point ayant trait à
la force exécutoire des décisions de justice et au 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, s’agissant de ces procédures engagées devant les juridictions civiles, le
saisi bénéficie d’une forme de protection du fait du contrôle 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* »11.
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.
**1.2**
**L’obligation de conservation des données imposée aux prestataires techniques**
L’universalité de la faculté d’accès constatée, il est nécessaire de s’interroger sur la nature des
données ainsi accessibles.
**1 -**L’article  6  II  de  la  loi  pour  la  confiance  dans  l’économie  numérique  (« **LCEN**»)12  prévoit
que « *les* [fournisseurs d’accès à internet13] *et* [hébergeurs14] *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.
**Erreur ! Source du renvoi introuvable.**).
**2 -**L’article 6 II de la LCEN est complété par les dispositions d’un décret *ad hoc*15, l’article 1 2°
duquel précise que les hébergeurs doivent conserver :
« *a) L'identifiant de la connexion à l'origine de la communication ;*
*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 ;*

11  TC  Châteauroux,  24  jan.  2007,  RG :  2006/882,  à  rapprocher  de  Cour  d’appel  de  Paris  –  Pôle  1  Chambre  4  –  11  mars  2010
n°0913381 s’agissant d’un huissier qui excède les limites de sa mission et ainsi aggrave le risque d’atteinte à la confidentialité des
donnés informatiques copiées.
12 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.
13 Définis 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).
14 Définis 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).
15 Décret 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.
Alan WALTER
4 / 10
  *13 septembre 2013*


*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 ?
**3 -**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.
**4 -**Par ces dispositions, fortement critiquées lors de leur adoption, les pouvoirs public 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.
Alan WALTER
5 / 10
  *13 septembre 2013*


**2**
**CLAUSE  CONTRACTUELLES  ET  SECURITE  DES  DONNEES  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 prise16.
Une  analyse  de  ces  contrats  permet  aisément  de  démontrer  que  le  prestataire  n’offre  aucune
garantie,  en  particulier  au  regard  de  la  conservation  des  données  (**2.1**)  et  exclut  autant  que
possible  sa  responsabilité  (**2.2**),  ce  que  les  tribunaux  français  ont  été  amenés  à  valider  dans
certaines conditions (Erreur ! Source du renvoi introuvable.).
**2.1**
**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.
*2.1.1  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.
**2 -**“*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  professionnel17,  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*»18.
En  excluant  cette  garantie,  le  prestataire  édulcore  son  obligation  d’information,  limitant  ainsi
les possibilités de recours pour les clients.
**3 -**“*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 ».

16 Il 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* ».
17 La 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.
18 Cass. com., 5 janv. 1999 ; pourvoi n° 96-16521.
Alan WALTER
6 / 10
  *13 septembre 2013*


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.
**4 -**“*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.
**5 -**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  matériel  associés),  ce  qui  empêche  de  qualifier  le  contrat  de
« vente », la jurisprudence admet que la présence de « bugs » est inhérente à la matière19.
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 valables, laissant le client à la merci d’une action corrective du prestataire.
*2.1.2  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*” ;
-  “*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***” ;
-  “***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*” ;

19 CA Paris 5e Ch. 7-2-1986, Caisse de retraite des notaires c/ MAP Informatique : Expertises 1986 n°87 p.235.
Alan WALTER
7 / 10
  *13 septembre 2013*


-  “***Any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or***
***failure to store any of your content or other data***” ;
-  “*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’aucun garantie n’est prise et que toute
responsabilité  est  exclue  relativement  à  ses  données,  il  ne  pourra  que  très  difficilement
recherché 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 terme de qualité de services.
**2.2**
**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.
**2 -**Quelques exemples parmi les plus parlants :
-  « *the immediately preceding month in which the event (or first in a series of connected events)*
*occurred*” ;
-  “*The service offerings are provided “as is”*.” ;
-  “*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)*” ;
-  “*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.
**3 -**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 irrésistible20.

20 Article 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 l’exigence du caractère d’extériorité, voir : Cass. Civ. , 30 oct. 2008 : Bull. Civ. I, n°243.
Alan WALTER
8 / 10
  *13 septembre 2013*


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
démontrés21.
Dans une telle hypothèse, un prestataire pourrait ainsi exclure sa responsabilité.
*2.2.1  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  commun  accord  entre  les  parties22,  sauf  dans  certaines  circonstances,
limitativement énumérées par la loi et la jurisprudence :
-  le  dol23.  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 ;
-  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* »24 ;
-  les dommages aux personnes, qui, de jurisprudence constante, rend nulle toute clause
de limitation ou d’exclusion de la responsabilité25.
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 contracté26.
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
responsabilité27.

21 Cass. Com. 25 novembre 1997, jursidata: 1997-004692.
22 Cass. Crim. 12 décembre 1946, JCP 1947, II, 3621, note R. Rodière.
23 Cf. 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* ».
24 Cass. Civ. 1er mai 1983: D. 1983 IR p. 256.
25 CA Toulouse, 23 octobre 1931 : D. 1935 II p.49 note L. Mazaud.
26 Voir sur ce point les décisions « Chronopost », en particulier Cass. Com. 22 octobre 1996, Contrats conc. consom. 19987, p. 0 note
anonyme.
27 Cass. civ. 1e , 24 février 1993
Alan WALTER
9 / 10
  *13 septembre 2013*


\*
\*
\*
\*
\*
Alan WALTER
10 / 10
  *13 septembre 2013*