Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES

TELEDOC 792
BATIMENT NECKER
120, RUE DE BERCY
75572 PARIS CEDEX 12

N° 2018/08/RR

Juin 2020

La responsabilité des fournisseurs de systèmes numériques

Rapport à

Monsieur le Vice-président
du Conseil Général de l'Economie

établi par

Mario CASTELLAZZI
Ingénieur général des Mines

Claudine DUCHESNE-JEANNENEY
Contrôleur général économique et financier

Ivan FAUCHEUX
Ingénieur général des Mines

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

SOMMAIRE

SYNTHESE **4**

TABLE DES RECOMMANDATIONS **7**

1 Introduction **8**

2 Le cadre juridique existant **13**

2.1 Des contrats à l'avantage des fournisseurs 13

2.1.1 Notre lecture de contrats et autres CGU/CGV 13

2.1.2 Nos rencontres avec les acteurs du monde professionnel 15

2.2 Des dispositifs juridiques existent pour contenir le déséquilibre 15

2.2.1 Code civil 16

2.2.2 Code de la Consommation 16

2.2.3 Code de Commerce 17

2.3 Peu d'actions en justice 17

3 Des pistes d'évolution pour rééquilibrer les rapports contractuels **19**

3.1 Recueillir des cas concrets de dysfonctionnement/litige 19

3.2 Instaurer une responsabilité sans faute pour les contrats de service en ligne 20

3.2.1 Instaurer par la loi des obligations accessoires aux contrats de service en ligne 22

3.2.2 Instaurer une responsabilité sans faute des fournisseurs de service en ligne 23

3.3 Etendre la protection du Code de la Consommation aux « petits professionnels profanes ». 26

3.4 Tenir compte du droit local dans l'expression des clauses d'exonération/limitation de responsabilité/indemnisation dans les contrats destinés aux particuliers et aux petits professionnels 28

3.5 Spécialiser une juridiction sur les litiges relatifs à la responsabilité des fournisseurs de systèmes numériques 28

4 Des pistes d'évolution pour une meilleure prise en compte de la sécurité **29**

4.1 Une prise de conscience grandissante de la nécessité d'une meilleure prise en compte de la sécurité 30

4.2 Nos recommandations 31

4.2.1 Imposer une sécurité par défaut 32

4.2.2 Instaurer la gratuité des mises à jour de sécurité 32

4.2.3 Obliger à la fourniture des mises à jour de sécurité bien après la fin de commercialisation du produit 32

5 Quels impacts pour ces pistes d'évolution ? **34**

5.1 Vers une augmentation du prix des produits/services numériques ? 34

5.2 Un frein à l'innovation ? 34

ANNEXES **36**

Annexe 1 : Lettre de mission 37
Annexe 2 : Liste des personnes rencontrées ou interrogées 39
Annexe 3 : Les contrats et CGU/CGV examinés par la mission 43
Annexe 4 : Glossaire 45

SYNTHESE

Par lettre du 5 octobre 2018, le vice-président du conseil général de l'économie (CGE) a lancé une mission d'étude portant sur la responsabilité des fournisseurs de systèmes numériques.

Ces fournisseurs jouent un rôle de plus en plus important dans la vie économique. Les systèmes numériques qu'ils commercialisent sont sujets à des dysfonctionnements ou à des attaques dont les effets peuvent être très préjudiciables pour leurs clients. Dans le même temps, ils entretiennent avec ces derniers des relations déséquilibrées (contrats d'adhésion, clauses limitatives de responsabilité,…).

Dans ce contexte, la mission s'est efforcée de déterminer dans quelle mesure peuvent être mis en place un régime de responsabilité plus impliquant pour les fournisseurs ainsi que des règles de sécurité plus protectrices des clients.

La définition d'un système numérique est très vaste puisqu'elle englobe aussi bien une montre connectée, un dispositif de surveillance dans une habitation constitué par un ensemble de capteurs et d'actionneurs, une baie de stockage dans un data center, un micro-ordinateur ou un smartphone, un robot spécialisé dans l'accueil des visiteurs, un logiciel de trading ou d'assistance chirurgicale, la fourniture de musique ou de vidéo en ligne, le stockage de photos dans le nuage, les services de partage de données (FaceBook, Youtube,…) que l'accès à son logiciel de comptabilité par un artisan.

Ces différents types de systèmes numériques relèvent, quant à la responsabilité de leur fournisseur en cas de dysfonctionnement, de différents régimes juridiques. Le dysfonctionnement d'un bien matériel est, par exemple, bien couvert par différents dispositifs juridiques (garantie légale de conformité, garantie contre les vices cachés et régime de responsabilité du fait des produits défectueux) qui sont autant d'outils pour instaurer une relation équilibrée entre clients et fournisseurs.

Par contre, l'offre de services en ligne (cloud computing), qui est une tendance lourde de l'industrie informatique, est le siège d'une relation déséquilibrée entre clients et fournisseurs où la négociation n'a pas sa place et où la mise en cause de la responsabilité du fournisseur est impossible compte tenu du type de contrat (engagement de moyens). Aussi, ce champ des services en ligne fera l'objet des principales recommandations de la mission.

Au préalable, la conviction qu'a la mission d'une relation déséquilibrée entre clients et fournisseurs devra être documentée par le recueil d'informations précises sur des cas concrets de différend entre les deux parties. Actuellement, ces informations ne sont pas disponibles car les différends, soit ne se règlent pas par lassitude des clients, soit se règlent par une transaction plutôt que de faire appel aux tribunaux. Dans l'hypothèse, fort probable, où ce recueil des faits montrera factuellement le déséquilibre existant entre fournisseurs de service en ligne et clients, la mission formule ici quelques recommandations pour rééquilibrer ces relations.

Ainsi, la loi pourrait imposer quelques obligations accessoires (existence d'un accord de niveau de service par exemple) aux contrats de service en ligne pour rééquilibrer les relations client-fournisseur. Mais il apparaît préférable, compte tenu de l'évolution constante du droit, d'instaurer une responsabilité sans faute pour les contrats de service en ligne, qui permettra au client de rechercher

plus facilement la responsabilité de son fournisseur dans une action judiciaire. Sans cette mesure, une telle action, qui nécessite de prouver en premier lieu la faute du fournisseur, est vaine car cette preuve est impossible à établir pour le client du fait, notamment, de la technicité de la prestation.

Parmi les clients, les « petits professionnels profanes[1] » doivent faire l'objet d'une protection renforcée. La proposition est d'étendre la protection du Code de la Consommation sur les clauses abusives à cette population, compte tenu du fait que cette catégorie de professionnels n'a pas nécessairement les connaissances juridiques et techniques suffisantes pour bien appréhender les conséquences d'un contrat et que l'achat d'un service en ligne est désormais indispensable à l'exercice d'une activité professionnelle.

Pour des contrats plus facilement compréhensibles par les consommateurs et les petits professionnels, l'expression des contrats doit être faite en droit local. Il s'agit de bannir des contrats les rédactions commençant par « Sous réserve du droit applicable… », car ce type d'expression permet alors au rédacteur d'introduire toute une série d'exclusions limitant sa responsabilité ou le droit à indemnisation du consommateur ou du petit professionnel, même lorsque le droit français interdit une telle exclusion, sans que cette rédaction soit pour autant contestable devant un tribunal. L'effet recherché par le rédacteur d'une telle formulation, excessive et compliquée, est sans doute de dissuader le co-contractant d'agir en justice.

Enfin, la spécialisation d'une juridiction sur les litiges relatifs à la responsabilité des fournisseurs de systèmes numériques permettra de réduire la variabilité de la jurisprudence et de donner ainsi plus de visibilité aux justiciables sur l'issue probable d'une action en justice.

Il n'existe pas, aujourd'hui, de droit européen unifié des contrats ni de règles couvrant les spécificités de ces services numériques. Aussi, les propositions ci-dessus se rapportent au droit français sans contrevenir au droit européen. Mais, les pratiques de nombreux fournisseurs du numérique étant a priori identiques dans les autres pays européens, elles gagneront à être proposées au niveau de l'Union européenne, pour créer un cadre unique plus vertueux économiquement et plus équilibré entre gros éditeurs et utilisateurs, entreprises comme ménages.

Lors des échanges de la mission avec les parties prenantes, les entreprises utilisatrices, bien que peu disertes sur leurs différends avec leurs fournisseurs, ont vu d'un bon œil toute mesure susceptible de rééquilibrer leurs relations avec ces derniers. Pour les fournisseurs, le dispositif juridique existant était jugé suffisant. Quant aux consommateurs, ils appellent de leurs vœux des amendes réellement dissuasives pour les éditeurs de logiciels contrevenants.

La sécurité de fonctionnement des dispositifs numériques est une préoccupation grandissante des organisations utilisatrices bien sûr, mais aussi, progressivement, des fournisseurs et des Etats.

Dans le sillage de cette prise de conscience, la mission formule trois recommandations.

[1] Le « petit professionnel » est la PME de moins de 20 salariés. Le « professionnel profane » est celui pour lequel le contrat n'entre pas dans le champ de son activité principale (par exemple le bijoutier qui achète un service de comptabilité en ligne).

En premier lieu, la sécurité par défaut doit devenir la règle dans la conception des produits. La mise en œuvre d'un niveau suffisant de sécurité pour déjouer les cyber-attaques connues ne doit pas nécessiter d'action explicite de l'utilisateur du produit ou service.

Pour que l'utilisateur n'ait pas à faire d'arbitrage prix versus sécurité qui, lorsqu'il est fait, tourne souvent en défaveur de la sécurité, les mises à jour de sécurité doivent être diffusées gratuitement, même en l'absence d'abonnement à des mises à jour fonctionnelles pour enrichir les fonctionnalités du produit ou du service.

Enfin, puisque la période d'usage d'un produit numérique ne s'arrête pas à la fin de sa commercialisation, la fourniture des mises à jour de sécurité doit être prolongée pour une période de [5, 10] ans après cette fin de commercialisation.

Pour les consommateurs et les petits professionnels, souvent insuffisamment sensibles aux sujets de sécurité, toute mesure élevant sans intervention et gratuitement le niveau de sécurité des produits est la bienvenue. Les fournisseurs, pour lesquels les mesures proposées complexifient la tâche, soulignent quant à eux le rôle que joue l'utilisateur dans le maintien en sécurité des systèmes numériques. Pour les entreprises utilisatrices, une disponibilité plus longue des mises à jour de sécurité leur ouvre un horizon plus large pour le renouvellement de leur système numérique et leur permet des réductions de coûts précieuses.

Compte tenu de la concurrence entre fournisseurs et du large niveau de diffusion de certains produits/services numériques, il n'est pas certain que ces propositions entraînent une hausse de prix. Une précédente mesure réglementaire[2] n'avait d'ailleurs pas eu d'effet inflationniste.

Le rééquilibrage des relations contractuelles par la mise en œuvre des recommandations ci-dessus accroît le risque, pour les fournisseurs du numérique, d'une mise en cause plus fréquente de leur responsabilité civile. Ce type de risque pourrait être couvert par une assurance, dont l'offre reste à construire. Aujourd'hui, le coût global de la défaillance potentielle d'un système informatique est totalement internalisé au niveau des clients.

*
* *

[2] En 2016, l'extension à 2 ans (au lieu de 6 mois) de la durée de présomption de conformité dans le cadre de la Garantie légale de conformité due au consommateur entraîne une prise en charge accrue de la réparation ou du remplacement des équipements en panne.

TABLE DES RECOMMANDATIONS

Avertissement : l'ordre dans lequel sont récapitulées ci-dessous les recommandations du rapport ne correspond pas à une hiérarchisation de leur importance mais simplement à leur ordre d'apparition au fil des constats et analyses du rapport.

Recommandation n° 1. Mettre en place une task force pour recueillir pendant 6 mois des cas concrets de différends entre les fournisseurs de service en ligne et leurs clients 19

Recommandation n° 2. Pour un ré-équilibrage des relations contractuelles, instaurer par la loi des obligations accessoires aux contrats de service en ligne 23

Recommandation n° 3. Pour une réparation plus facile du préjudice, instaurer une responsabilité sans faute du fournisseur dans les contrats de service en ligne..... 25

Recommandation n° 4. Etendre la protection de l'article L212-1 du Code de la consommation sur les clauses abusives aux « petits professionnels profanes » 26

Recommandation n° 5. Compléter l'article L211-1 du Code de la consommation par une disposition exigeant l'expression en droit local de toutes les clauses du contrat et étendre son champ d'application aux petits professionnels 28

Recommandation n° 6. Spécialiser une ou des juridictions territoriales des tribunaux judiciaires sur les litiges relatifs à la responsabilité des fournisseurs de systèmes numériques 29

Recommandation n° 7. Imposer une sécurité par défaut dans la mise en œuvre des produits et services numériques 32

Recommandation n° 8. Instaurer la gratuité des mises à jour de sécurité, même en l'absence d'abonnement aux évolutions fonctionnelles du produit ou du service numérique..... 32

Recommandation n° 9. Instaurer l'obligation de fournir pendant [5, 10] ans après la fin de commercialisation du produit numérique, les mises à jour de sécurité 33

1 INTRODUCTION

Les fournisseurs de systèmes numériques jouent un rôle de plus en plus important dans la vie économique. Ces systèmes sont sujets à des dysfonctionnements ou à des attaques dont les effets peuvent être très préjudiciables pour leurs clients. Dans le même temps, ils entretiennent avec ces derniers des relations déséquilibrées (contrats d'adhésion, clauses limitatives de responsabilité,…).

Dans ce contexte, l'objet de la présente mission est de déterminer dans quelle mesure peut être mis en place un régime de responsabilité plus étendu pour les fournisseurs ainsi que des règles de sécurité plus protectrices des clients.

En s'inspirant de la directive européenne 2019/771[3] du 20 mai 2019 relative à certains aspects concernant les contrats de vente de biens, un **système numérique** peut être défini comme un ensemble d'éléments en interaction *« qui intègre un contenu numérique ou un service numérique ou est interconnecté avec un tel contenu ou un tel service, d'une manière telle que l'absence de ce contenu numérique ou de ce service numérique empêcherait ce système de bien remplir ses fonctions »*. Le contenu numérique est constitué de « *données produites et fournies sous forme numérique* », et le service numérique, tel que défini par la directive 2019/770 du 20 mai 2019 correspond à *« un service permettant au consommateur de créer, traiter, stocker ou partager des données sous forme numérique ou d'y accéder, ou un service permettant le partage ou toute autre interaction avec des données sous forme numérique qui sont téléversées ou créées par le consommateur ou d'autres utilisateurs de ce service* ».

Cette définition est très vaste puisqu'elle englobe aussi bien une montre connectée, un dispositif de surveillance dans une habitation constitué par un ensemble de capteurs et d'actionneurs, une baie de stockage dans un data center, un micro-ordinateur ou un smartphone, un robot spécialisé dans l'accueil des visiteurs, un logiciel de trading ou d'assistance chirurgicale, la fourniture de musique ou de vidéo en ligne, le stockage de photos dans le nuage, les services de partage de données (FaceBook, Youtube,…) que l'accès à son logiciel de comptabilité par un artisan.

Certains de ces systèmes peuvent être des dispositifs apprenants grâce à l'intelligence artificielle qu'ils embarquent. Leur fonctionnement n'est alors plus complètement déterminé par le fournisseur[4], ce qui suscite de nouvelles réflexions en matière de responsabilité. C'est aujourd'hui un sujet d'étude doctrinale que de déterminer si la responsabilité d'un dysfonctionnement doit être recherchée chez son concepteur, son propriétaire, son superviseur d'apprentissage ou chez l'utilisateur du système. Cette catégorie de systèmes, qui fait actuellement l'objet de recherches dans le domaine du droit, ne sera pas abordée par la mission.

Ces systèmes numériques relèvent, quant à la responsabilité de leur fournisseur en cas de dysfonctionnement, de différents régimes juridiques.

---

[3] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019L0771&from=EN

[4] On se souvient du chatbot Tay de Microsoft (mars 2016), conçu pour participer à des conversations sur les réseaux sociaux, mais qui, en moins de 24 heures, avait tenu des propos racistes ou sexistes car alimenté de cette façon par certains internautes.

La protection des données personnelles traitées par le service en ligne est assurée par le règlement général de protection des données (RGPD), texte réglementaire européen qui encadre le traitement des données personnelles de manière égalitaire sur tout le territoire de l'Union Européenne. Il est entré en application le 25 mai 2018 et s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978. Il vise notamment à renforcer les droits des personnes et à responsabiliser les acteurs traitant des données. En particulier, le fournisseur sous-traitant est tenu de respecter des obligations spécifiques en matière de sécurité ou de confidentialité, et doit mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données. La mission n'a pas jugé nécessaire d'investiguer plus avant ce champ.

Pour les biens matériels, qui peuvent inclure ou être connectés à un élément numérique (contenu ou service), plusieurs dispositifs juridiques éprouvés existent et permettent à un consommateur ou, pour certains régimes, à un professionnel, d'engager la responsabilité de son fournisseur. La mission ne s'intéresse pas à ces biens.

Les différents régimes applicables aux transactions impliquant un bien matériel

La garantie légale de conformité (Code de la Consommation[5])
Elle s'applique aux contrats de vente de biens meubles corporels (pas aux logiciels donc), entre un vendeur professionnel et un consommateur.
Le Code de la consommation et ses articles L. 217-1 et suivants obligent le vendeur à réparer ou à échanger tout bien neuf ou d'occasion qui ;
-Ne correspond pas à la description qui lui en a été faite par le vendeur
-Est impropre à l'usage habituellement attendu d'un produit semblable
-Ne correspond pas à l'usage recherché tel que porté à la connaissance du vendeur par l'acheteur
En cas de non-conformité, l'acheteur peut réclamer la réparation ou le remplacement du bien, voire la résolution de la vente ou une réduction de prix.
L'article 241-5 du Code consommation écarte la possibilité pour le vendeur de limiter ou de s'exonérer de cette garantie.

La garantie légale des vices cachés (Code civil)
Son fondement est l'article 1641 du Code civil :
« Le vendeur est tenu de la garantie à raison des défauts cachés de la chose vendue qui la rendent impropre à l'usage auquel on la destine, ou qui diminuent tellement cet usage que l'acheteur ne l'aurait pas acquise, ou n'en aurait donné qu'un moindre prix, s'il les avait connus. »
Le vice affectant le bien doit être grave ou rédhibitoire (c'est une différence avec la non-conformité), c'est-à-dire que l'acheteur n'aurait pas acheté le bien s'il en avait eu connaissance, ou il l'aurait acheté à un prix moins élevé. Le vice s'apprécie par rapport à la destination normale de la chose, alors que la non-conformité se mesure à l'aune des spécifications du contrat (c'est une différence par rapport à celles-ci).
En cas de vice caché, l'acheteur peut rendre la chose et s'en faire restituer le prix, ou se faire restituer une partie du prix, voire, réclamer des dommages et intérêts s'il peut établir un lien entre le vice caché et un dommage.
Si l'acheteur est un professionnel achetant dans son domaine de compétence, un défaut décelable par un examen normal par un professionnel n'est pas un vice caché. Un vendeur professionnel est censé connaître

[5] Directive UE 1999/44/CE du 25 mai 19999 "sur certains aspects de la vente et des garanties des biens de consommation", adaptée en droit français par l'ordonnance n° 2005-136 du 17 février 2005

tous les défauts de son produit. Un vendeur occasionnel peut se prévaloir de sa méconnaissance légitime du défaut.
Au titre des clauses abusives du Code de la Consommation, le vendeur professionnel ne peut limiter ou s'exonérer de cette garantie.

La responsabilité du fait des produits défectueux
Il s'agit d'un un régime de responsabilité extracontractuelle qui bénéficie à toute victime[6] (consommateur ou professionnel) d'un défaut de sécurité du produit, liée par un contrat ou pas avec le producteur.
Cette responsabilité pèse sur le producteur du produit[7].
Pour engager la responsabilité du producteur, la victime doit prouver le dommage subi, le défaut de sécurité du produit et un lien de causalité entre le défaut et le dommage.
C'est une responsabilité sans faute (cf. 3.2.2 ci-dessous) : la victime n'a pas à prouver une faute de la part du producteur.
Les clauses qui visent à écarter ou à limiter la responsabilité du fait des produits défectueux sont interdites et réputées non écrites[8]. Toutefois, pour les dommages causés aux biens qui ne sont pas utilisés par la victime principalement pour son usage ou sa consommation privée, les clauses stipulées entre professionnels sont valables.

Pour ce qui concerne les logiciels, la mission n'a pas, là aussi, jugé nécessaire de traiter des logiciels spécifiques construits à la demande d'un client (contrat de prestation de services) pas plus que de la maintenance de ces logiciels ou de leur exploitation (qui peut aller jusqu'à des prestations d'infogérance[9]). Relevant du droit classique des contrats avec, très largement, des obligations partagées entre le fournisseur (généralement obligation de résultat, obligation de conseil,…) et le client (obligation de collaboration, obligation de réception,…), et faisant l'objet d'une abondante jurisprudence, ce champ ne semble pas être le siège d'une relation déséquilibrée entre clients et fournisseurs.

S'agissant des progiciels[10], les éditeurs, confrontés à la stagnation de leurs ventes de licences compte tenu du large niveau de diffusion maintenant atteint (peu de perspective de croissance du parc d'utilisateurs) s'orientent vers des systèmes de type vente de services (software as a service) et tirent donc leurs marges non pas de la vente de biens dématérialisés, mais de services hébergés sur leurs propres infrastructures (applications hébergées). Ce modèle de diffusion permet en outre aux éditeurs

[6] Le dommage peut être constitué par une atteinte à la personne ou par la réparation d'un bien endommagé lorsque cette réparation dépasse 500 €.

[7] Article 1245 du Code civil

[8] Article 1245-14 du Code civil

[9] En infogérance, le client externalise auprès d'un prestataire informatique la gestion et l'exploitation de tout ou partie de son système d'information (SI).

[10] Un progiciel est un logiciel conçu par un éditeur, destiné à l'usage d'une large clientèle ayant un ensemble commun de besoins. Par exemple, un progiciel comptable destiné à automatiser la tenue de la comptabilité d'une gamme d'entreprises (PME ou grande entreprise). A titre d'illustration, SAP ou SalesForce sont des fournisseurs de progiciel. Le fournisseur place dans le développement de son progiciel toute son expérience métier acquise auprès de ses clients qui, par le recours au progiciel, peuvent espérer profiter d'un système qui a déjà fait ses preuves et qui embarque dans ses fonctionnalités les processus standards d'un métier.

de faire l'économie d'un circuit de distribution et de maîtriser l'éventail des versions[11] en cours d'utilisation (avec à la clé des économies en matière de maintenance et de support client). Les clients de ces éditeurs trouvent également des avantages à ce modèle de commercialisation qui leur permet, grâce à la mutualisation des ressources chez les éditeurs, de réduire leurs coûts[12], d'accéder rapidement[13] à des progiciels hébergés chez l'éditeur avec une tarification basée sur l'usage[14] ou de déployer rapidement[15] leurs propres applications grâce à l'élasticité de l'offre.

Du fait de ses avantages tant pour les fournisseurs que pour les clients, ce mode d'accès à des logiciels, à de la puissance de traitement, à des capacités de stockage,… qu'est le cloud computing est aujourd'hui en constante progression.

L'utilisation du cloud par les entreprises dans l'UE[16]

Plus d'une entreprise sur 4 de plus de 10 salariés a utilisé des services de cloud computing en 2018 dans l'UE. Cette proportion s'élevait à 21% en 2016 et à 19% en 2014.
Les grandes entreprises l'utilisent plus (56% parmi celles employant au moins 250 salariés) que les petites (23% des entreprises entre 10 et 49 salariés).

Le courrier électronique est le principal usage du cloud computing (69% des entreprises), suivi par le stockage des fichiers dans le cloud (68%). Les logiciels de bureautique et l'hébergement de bases de données (53% et 48%) sont également en bonne position. Dans une moindre mesure, les entreprises ont acheté des services de gestion d'informations sur la clientèle (GRC, 29%) ou ont acheté de la puissance de calcul (23%).

Ces services en ligne, comme tout dispositif technique, peuvent faire l'objet de dysfonctionnements et donner lieu à des actions en justice pour dédommagement du préjudice subi. Mais, même si la mission reconnaît ne pas disposer d'éléments chiffrés faute de données disponibles, le cadre contractuel, qui apparaît déséquilibré en faveur des fournisseurs, freine le règlement judiciaire des différends.

---

[11] Revers de la médaille, la mission n'est pas tout à fait convaincue que le renouvellement imposé des versions se fait au bénéfice des consommateurs et clients.

[12] Selon une étude de la Commission européenne de 2012 citée dans « L'informatique en nuage – Une vue d'ensemble des enjeux économiques et politiques », mai 2016 (http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_FR.pdf), quatre entreprises sur cinq qui adoptent l'informatique en nuage ont pu réduire leurs coûts informatiques de 10 à 20%.

[13] Pas de machine à acheter, pas de logiciel à installer, pas de personnel d'exploitation supplémentaire à recruter, pas de data center à entretenir ou, pire, à étendre. Le client dispose sur ses postes de travail, une fois la configuration initiale effectuée, d'un accès aux fonctionnalités du progiciel.

[14] Le prix dépend de l'activité du client. Il n'y a pas d'investissement initial important, ce qui permet au client de tester rapidement de nouvelles offres sans courir un risque du fait de la nécessité d'investir au préalable dans un nouveau système d'information.

[15] Le client peut paramétrer, par une simple interface, les caractéristiques des machines dont il va avoir besoin. Il n'est plus nécessaire de commander des matériels, de les installer, de surveiller leur bon fonctionnement et de passer des contrats de maintenance.

[16] Selon une étude Eurostat de décembre 2018 (https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises)

Compte tenu de l'essor des services en ligne (cloud computing) et de la nouveauté de ce type de relation entre clients et fournisseurs, le régime juridique de ces services fera l'objet des principales recommandations de la mission.

En outre, les systèmes numériques, quels qu'ils soient (montre connectée, micro-ordinateur, smartphone, robot, service de partage de données, logiciel de comptabilité en ligne,…), peuvent subir des attaques (virus, ransomware, attaque par déni de service,…) qui menacent leur fonctionnement et conduisent dans les cas extrêmes à paralyser l'activité de l'organisation utilisatrice. En cas d'attaque couronnée de succès, l'utilisateur du système numérique se retrouve seul[17] face aux conséquences de l'attaque. Certes, le fournisseur risque aussi quelques dommages en voyant sa réputation écornée[18] si de trop nombreuses attaques réussissent, mais force est de constater qu'il n'est pas la principale victime dans l'attaque.

La mission proposera des recommandations pour concrétiser plus encore l'implication des fournisseurs auprès de leurs clients, dans la prise en compte de la sécurité des systèmes numériques pris dans leur acceptation la plus large, de la montre connectée au service en ligne de comptabilité, en passant par le robot d'assistance chirurgicale.

[17] L'appel à l'expertise du fournisseur pour remettre en route le système est généralement payante, qui plus est chère puisque l'expertise sollicitée est de niveau élevé.

[18] Mais encore faut-il que ces attaques deviennent publiques

2 LE CADRE JURIDIQUE EXISTANT

2.1 Des contrats à l'avantage des fournisseurs

2.1.1 Notre lecture de contrats et autres CGU/CGV

Le parlement européen, dans une étude de 2016[19], s'est livré à l'examen de quelques contrats cloud destinés au grand public.

Il en ressort que les fournisseurs « *déclinent toute responsabilité en matière de disponibilité ou de fonctionnalité du service, et qu'ils se prémunissent contre les éventuels dommages causés aux consommateurs. Les fournisseurs ont en outre un grand pouvoir d'appréciation en ce qui concerne les contenus ou la conduite des utilisateurs, ils peuvent changer les modalités et les conditions sans notification explicite, et ils peuvent résilier ou suspendre les services sans préavis* ».

Le même type de constat a pu être fait par la mission pour les contrats cloud destinés aux professionnels. La mission a en effet procédé à l'examen de quelques contrats et autres CGU[20] ou CGV[21] (cf. *Annexe 3 : Les contrats et CGU/CGV examinés par la mission*).

Dans ces contrats de service en ligne, l'obligation convenue entre le débiteur (fournisseur) et le client (créancier) est principalement la fourniture soit d'une infrastructure (Iaas[22]), soit d'une plate-forme d'exécution (PaaS[23]) soit d'un service (SaaS[24]). L'accès à un service de support client (par mail, par forum, par téléphone,…) est aussi généralement convenu.

Lorsqu'il s'agit de fourniture de service en mode SaaS, le contrat prévoit également la fourniture d'une maintenance corrective et évolutive du logiciel par laquelle le client bénéficie des dernières évolutions du produit.

---

[19] « L'informatique en nuage – Une vue d'ensemble des enjeux économiques et politiques », Mai 2016, http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_FR.pdf

[20] Conditions générales d'utilisation

[21] Conditions générales de vente

[22] Le fournisseur d'IaaS (Infrastructure as a Service) met à la disposition de son client une infrastructure informatique et gère les matériels serveurs, le stockage et les réseaux.

[23] Le fournisseur de PaaS (Platform as a Service) fournit à son client une plate-forme matérielle équipée des logiciels de base (système d'exploitation, base de données) que le client pourra utiliser pour y déployer et exploiter ses propres applications.

[24] Le fournisseur de SaaS (Service as a Service) donne accès à ses clients aux fonctionnalités d'un logiciel qu'il exploite sur ses propres serveurs.

Exemples de clauses rencontrées parmi les contrats examinés[25]

- [le fournisseur s'engage à] fournir des efforts commercialement raisonnables pour maintenir les Services en ligne disponibles 24 heures sur 24, 7 jours par semaine
- LES OFFRES DE SERVICES SONT FOURNIES « TELLES QUELLES»
- Aucune garantie QUE LE CONTENU QUEL QU'IL SOIT SERA CONSERVÉ DE MANIÈRE SÉCURISÉE ET NE SERA NI PERDU NI ENDOMMAGÉ
- SAUF SI LA LOI L'INTERDIT OU DANS LA MESURE OÙ DES DROITS LÉGAUX S'APPLIQUENT ET NE PEUVENT ÊTRE EXCLUS, LIMITÉS OU ÉCARTÉS…
- LES LIMITATIONS STIPULÉES DANS LA PRÉSENTE SECTION 11 S'APPLIQUENT UNIQUEMENT DANS LA MESURE OU CELA EST AUTORISÉ PAR LA LE DROIT APPLICABLE
- NOTRE RESPONSABILITÉ CONJOINTE AVEC CELLE DE NOS SOCIÉTÉS AFFILIÉES ET CONCÉDANTS DE LICENCE N'EXCÉDERA PAS LE MONTANT QUE VOUS NOUS VERSEZ EN VERTU DU PRÉSENT CONTRAT AU TITRE DU SERVICE QUI A DONNÉ LIEU A LA DEMANDE AU COURS DES 12 MOIS PRÉCÉDANT LA NAISSANCE DE L'OBLIGATION
- Nous pouvons modifier le présent Contrat (y compris toutes les Politiques) à tout moment en publiant une version révisée de celui-ci sur le Site […] ou en vous le notifiant de toute autre manière conformément à la Clause 13.10

Quelques traits caractéristiques de ces contrats peuvent être dégagés.

Il s'agit, dans tous les cas, d'engagement de moyens. Parfois, le fournisseur s'engage sur la disponibilité de son service au travers d'un SLA (Service Level Agreement) qui prévoit, par exemple, une disponibilité du service à hauteur de 99,5% pour chaque période mensuelle. En cas de non-respect de cet engagement, le client peut espérer récupérer une partie de son abonnement (généralement mensuel) mais le fournisseur exclut toujours dans le contrat de réparer un quelconque préjudice causé par l'indisponibilité du service.

Obligation de moyens et obligation de résultat

L'obligation du débiteur (le fournisseur) dans un contrat peut présenter différents degrés : on distingue généralement l'obligation de moyens et l'obligation de résultat.

Dans une obligation de moyens, le débiteur promet de mettre en œuvre tous les moyens dont il dispose pour exécuter le contrat. Il s'engage à « faire de son mieux ». L'obligation du débiteur est de fournir un effort constant. Certes, sa prestation s'oriente vers une fin ultérieure, mais la réalisation de cette dernière n'est pas promise. Un médecin ou un avocat ont une obligation de moyens : ils doivent mobiliser leurs connaissances pour guérir le patient ou gagner un procès, mais ni la guérison ni le gain du procès ne sont promis.

Une obligation de résultat oblige le débiteur à parvenir au résultat convenu. C'est le cas, notamment, du transporteur ou de l'entrepreneur qui s'engagent à livrer la chose confiée ou à effectuer les travaux convenus.

[25] Les clauses présentées ici sont extraites d'un des contrats examinés. Mais on retrouve le même type de clause dans chacun des contrats, dans une formulation différente mais identique dans l'esprit. Les clauses en majuscule apparaissent ainsi dans les contrats.

Il s'agit généralement de contrats d'adhésion que le client doit accepter en l'état. Seuls quelques grands clients que la mission a pu rencontrer peuvent tenter de négocier certaines clauses avec leur fournisseur qui leur dédie un contact commercial. Mais même dans ce cas de figure, peu de clauses semblent ouvertes à la négociation. Lorsque négociation il y a, elle est très fortement dirigée depuis le siège social du fournisseur et non par sa filiale française.

Qu'est-ce qu'un contrat d'adhésion ?

Le contrat d'adhésion est défini par l'article 1110 du Code civil : « Le contrat d'adhésion est celui qui comporte un ensemble de clauses non négociables, déterminées à l'avance par l'une des parties. »

Les contrats de licence ou d'hébergement peuvent très probablement[26] recevoir cette qualification de contrat d'adhésion : l'absence de négociation n'est-elle pas caractérisée dès lors que le client d'un service en ligne coche une case aux fins de bénéficier du service ?

Les contrats comportent de nombreuses clauses de non-responsabilité ou limitant l'indemnisation en cas de préjudice au montant payé par le client pour son abonnement.

La formulation de certaines clauses est peu compréhensible : elles sont écrites en majuscules[27], en employant des formulations commençant par « Sous réserve du droit applicable… » ce qui les rend particulièrement absconses pour le non-juriste qu'est le consommateur ou le « petit » professionnel qui ne dispose pas de service juridique.

2.1.2 Nos rencontres avec les acteurs du monde professionnel

Elles confortent nos constatations ci-dessus. Même s'ils nous ont peu parlé de différends en cours avec leurs fournisseurs, beaucoup ont fait part, même parmi les plus grands clients, de leur difficulté à négocier les contrats, signe d'un pouvoir économique de marché largement à l'avantage des fournisseurs.

2.2 Des dispositifs juridiques existent pour contenir le déséquilibre

Pour ce qui concerne le niveau européen, de nombreuses directives affectent le droit des obligations dans le cadre contractuel (comme celles sur la protection du consommateur) ou dans le cadre extra-contractuel (comme celle sur les produits défectueux). Mais à ce jour, malgré des tentatives d'harmonisation européenne[28], il n'existe pas de droit européen unifié des contrats.

[26] La qualification sera faite par le juge.

[27] L'écriture en majuscule permet de montrer devant un tribunal que l'attention du contractant a été spécialement attirée sur ladite clause

[28] L'idée de créer un droit européen des contrats remonte à 2001. Des travaux ont eu lieu dans le cadre des institutions européennes ainsi que dans le milieu universitaire, sans toutefois permettre, à ce jour, de créer ce nouveau droit européen unifié des contrats. Voir par exemple https://www.senat.fr/rap/l17-022/l17-0223.html

C'est donc dans la législation française qu'il faut rechercher les dispositifs pour tenter de contenir ce déséquilibre des contrats.

2.2.1 Code civil

L'article 1170 du Code civil (« *Toute clause qui prive de sa substance l'obligation essentielle du débiteur est réputée non écrite* ») vise ainsi à ce que le dispositif contractuel soit en accord avec l'engagement promis par le fournisseur. Sont ainsi visées les clauses limitatives de responsabilité par lesquelles le débiteur est peu incité à exécuter une obligation essentielle pour le créancier. Par exemple, dans un contrat d'hébergement, la limitation importante des pénalités dues en cas de non-respect de la qualité de service.

L'article 1171 du Code civil *(« Dans un contrat d'adhésion[29], toute clause non négociable, déterminée à l'avance par l'une des parties, qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite* »), introduit[30] le déséquilibre significatif dans le droit commun des contrats. Les clauses limitatives ou exclusives de responsabilité, les clauses excluant les garanties légales ou encore les clauses restreignant le droit d'agir de l'adhérent (clauses de compétence, de conciliation, abréviatives de prescription...) sont ainsi, par exemple, sans aucun doute visées par cet article. Encore faut-il montrer le déséquilibre significatif pour bénéficier de cette disposition. Les juristes peuvent argumenter sur le fait qu'une clause prise isolément peut paraître déséquilibrée mais que, en considérant l'ensemble des clauses du contrat, l'équilibre est rétabli entre les deux parties au contrat.

2.2.2 Code de la Consommation

Le Code de la Consommation protège le consommateur en tant que « partie faible » d'une relation contractuelle.

La notion de clause abusive de l'article L212-1 du Code de la consommation (« *Dans les contrats conclus entre professionnels et consommateurs, sont abusives les clauses qui ont pour objet ou pour effet de créer, au détriment du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat* ») est un instrument important de protection du consommateur. Lorsqu'un consommateur est en jeu, le bénéfice de cet article est souvent préféré à celui de l'article 1171 du Code civil sur les contrats d'adhésion, car une bonne partie des clauses abusives sont déjà listées par le Code de la Consommation[31], réduisant ainsi la marge d'interprétation possible par les tribunaux.

Les associations de consommateurs peuvent aussi agir afin de pouvoir faire masse d'une série de dommages peu importants pris individuellement et ne pas offrir l'impunité à un fournisseur indélicat.

Elles peuvent ainsi agir pour un intérêt collectif sur la base :

---

[29] Cf. 2.1.1 pour la définition du contrat d'adhésion.

[30] Cet article 1171 est issu de la réforme du droit des contrats de 2016.

[31] Article R212-1 pour les clauses abusives de manière irréfragable (le fournisseur n'est pas admis à apporter une preuve contraire) et article R212-2 pour les clauses présumées abusives (le fournisseur doit montrer que la clause n'est pas abusive).

- de l'article L621-1 du Code de la Consommation pour « *… exercer les droits reconnus à la partie civile relativement aux faits portant un préjudice direct ou indirect à l'intérêt collectif des consommateurs* **».**
- de l'article L621-9 du Code de la Consommation, en s'associant aux côtés d'un consommateur.

Elles peuvent également agir pour la réparation de préjudices patrimoniaux résultant des dommages matériels subis par des consommateurs en intentant une action de groupe (article L623-2 du Code de la Consommation). Il s'agit alors de régler l'ensemble des différends d'un groupe de consommateurs bien identifiés, de manière unifiée compte tenu de la proximité entre les diverses demandes des victimes, et de faire masse d'un ensemble de dommages individuels peu importants unitairement.

2.2.3 Code de Commerce

Pour les relations entre professionnels, la notion de pratique restrictive de concurrence du Code de Commerce joue un rôle analogue à celui tenu par la notion de clause abusive du Code de la Consommation : il s'agit de restaurer un équilibre contractuel dans les relations commerciales[32].

L'article L442-1-I[33] du Code de Commerce énumère ainsi parmi les pratiques restrictives de concurrence le fait de « soumettre ou de tenter de soumettre l'autre partie à des obligations créant un déséquilibre significatif dans les droits et obligations des parties ». La jurisprudence actuelle sur la sanction du déséquilibre significatif retient entre autres critères la possibilité ou non de négocier le contrat.

Le ministre de l'économie, par l'article L442-4-I du Code de Commerce, peut également intervenir pour sanctionner des pratiques restrictives de concurrence.

2.3 Peu d'actions en justice

Malgré ces dispositifs juridiques existants, peu d'actions sont intentées en justice.

S'agissant des acteurs professionnels, lorsque des différends ont été évoqués, nos interlocuteurs nous ont précisé que leur règlement s'était fait ou se faisait par une transaction, sans recours aux tribunaux. Parmi les raisons évoquées pour ne pas avoir recours à la voie judiciaire :

- L'assignation en justice entre entreprises est peu courante. Elle n'intervient que comme « dernière chance » de régler un litige, lorsque les relations sont rompues.
- Une action en justice est coûteuse (frais d'avocat, expertises) et longue.
- L'issue d'une action en justice est de plus incertaine, notamment dans un domaine très technique et relativement nouveau comme le numérique.
- Pour les « petits » professionnels, le sentiment d'avoir à faire à un fournisseur plus aguerri au plan juridique décourage toute initiative en la matière.

[32] Notamment entre les fournisseurs et la grande distribution

[33] L'ancien article L442-6-I du Code de Commerce énumérait 13 pratiques restrictives de concurrence. Le nouvel article L442-1-I n'en liste plus que deux à la suite de l'ordonnance n°2019-359 du 24 avril 2019 portant refonte du titre IV du livre IV du Code de commerce, car cette liste de 13 pratiques restrictives n'était pas pleinement exploitée par les acteurs économiques.

- Les informations techniques pour prouver la faute du fournisseur ne sont généralement pas accessibles car, même lorsqu'elles ne sont pas détenues par le seul fournisseur, leur interprétation est hors de portée du professionnel.

Quant aux particuliers, compte tenu du préjudice insuffisamment élevé pour justifier une action devant les tribunaux, leurs actions individuelles sont trop rares pour impressionner les auteurs des abus.

Les actions engagées en justice sont donc le fait d'associations de consommateurs ou de la DGCCRF[34].

C'est ainsi que Twitter (août 2018), Google+ (février 2019), Facebook (avril 2019) ont été condamnés pour clauses abusives dans des actions intentées par UFC Que Choisir…après environ 5 ans de procédure, pour une condamnation dérisoire à 30 K€ pour Twitter et Facebook.
En juin 2019, une action de groupe à l'encontre de Google a également été lancée par UFC Que Choisir qui reproche à Google de « noyer les consommateurs dans des règles de confidentialité interminables » et de « maintenir un véritable parcours du combattant pour agir sur la géolocalisation ».

Plusieurs actions en justice sont le fait de la DGCCRF, notamment :

- en mai 2014, assignation de Booking auquel Bercy reproche d'imposer des conditions drastiques aux hôteliers qui souhaitent mettre leurs offres en ligne.
- en juin 2017, condamnation[35] d'EXPEDIA à faire disparaître 2 clauses litigieuses[36] au titre d'une pratique restrictive de concurrence. Lors de cette procédure, il convient de remarquer que les victimes étaient absentes, seulement représentées par l'intermédiaire de leur syndicat, et qu'aucun hôtelier n'a osé demander réparation.
- en mars 2018, assignation de Apple et Google pour déséquilibre significatif dans le contrat-type de leur magasin d'applications (par exemple : la fixation unilatérale d'une fourchette de prix au sein de laquelle développeurs doivent fixer le tarif de leurs applications pour les consommateurs ou la possibilité pour Google/Apple de modifier ou suspendre unilatéralement le contrat).
- en septembre 2019, condamnation[37] d'Amazon à 4M€ d'amende pour déséquilibre significatif dans les relations commerciales sur sa marketplace.

Sans oublier la condamnation de Google à 150M€ d'amende par l'autorité de la concurrence, le 20/12/19, pour des règles de fonctionnement de Google Ads[38] établies et appliquées dans des conditions « non objectives, non transparentes et discriminatoires ».

[34] Direction générale de la concurrence, de la consommation et de la répression des fraudes

[35] Arrêt du 21 juin 2017 de la cour d'appel de Paris

[36] Clause de parité (l'hôtelier devait faire profiter EXPEDIA de son tarif le plus avantageux) et clause de la dernière chambre disponible (l'hôtelier devait accorder à EXPEDIA la réservation de sa dernière chambre)

[37] Jugement du 2/09/19 du tribunal de commerce de Paris. Une dizaine de clauses des conditions générales d'utilisation imposées par Amazon à ses partenaires commerciaux étaient particulièrement déséquilibrées et ne respectaient donc pas les règles fixées par le code de commerce.

[38] Le service de Google offert aux annonceurs pour la diffusion de publicité sur les résultats de recherche

3 DES PISTES D'EVOLUTION POUR REEQUILIBRER LES RAPPORTS CONTRACTUELS

Nos recommandations ont pour but principal de rééquilibrer les relations contractuelles en proposant quelques dispositifs destinés à l'usage par la partie la plus faible pour renforcer sa protection ou faciliter son action en justice.

3.1 Recueillir des cas concrets de dysfonctionnement/litige

En-dehors des quelques cas d'action en justice cités ci-dessus, la mission n'a pas pu disposer d'informations précises et étayées sur des cas concrets de différend entre les fournisseurs de service en ligne et leurs clients.

Il convient donc, dans un premier temps de…

Recommandation n° 1.	Mettre en place une task force pour recueillir pendant 6 mois des cas concrets de différends entre les fournisseurs de service en ligne et leurs clients

Ce recueil est indispensable pour vérifier si la conviction d'une relation déséquilibrée entre clients et fournisseurs qu'a la mission, résiste à l'épreuve des faits.

Ce recensement pourra en outre servir de base à la constitution d'un dossier de fact-checking pour porter devant la Commission Européenne la nécessité de faire évoluer la réglementation.

La task-force pourrait par exemple être placée auprès de la DGCCRF[39], du médiateur inter-entreprises de Bercy ou de l'Autorité de la concurrence. Une large publicité de la création de cette task-force auprès des entreprises par l'intermédiaire de leurs organisations professionnelles (CGPME, MEDEF,…) permettra de solliciter les contributions. Le fonctionnement ponctuel (6 mois) de cette task-force pourrait reposer sur quelques stagiaires ou être l'objet d'un appel à la sous-traitance.

Dans l'hypothèse, fort probable, où le recueil de faits par la task-force révèlera au grand jour, de façon précise, le déséquilibre existant entre fournisseurs de service en ligne et clients, la mission formule ici quelques recommandations pour rééquilibrer ces relations.

[39] Le site https://signal.conso.gouv.fr/ qu'elle anime pourrait ainsi recueillir les témoignages des consommateurs. Son élargissement aux relations entre professionnels serait nécessaire.

3.2 Instaurer une responsabilité sans faute pour les contrats de service en ligne

La responsabilité pour faute est le principe général de la responsabilité civile[40].

La responsabilité contractuelle[41], qui nous importe ici, est la variété de responsabilité civile qui s'applique lorsque le dommage a été causé par la mauvaise exécution d'un contrat liant un débiteur (le fournisseur) et son créancier (le client).

Cette responsabilité contractuelle suppose la réunion de trois éléments : un manquement contractuel (non-respect d'une obligation du contrat), un préjudice et un lien de causalité entre ceux-ci. Si le manquement contractuel constaté conduit à un dommage direct[42] pour le créancier, celui-ci devra, pour engager la responsabilité de son débiteur et obtenir réparation de son préjudice, prouver la faute du débiteur et le lien de causalité entre le manquement contractuel et le dommage subi.

En cas de mauvaise exécution du contrat, la distinction entre obligation de moyens et obligation de résultat [43]est importante pour la charge de la preuve : est-ce au créancier de prouver que son débiteur a commis une faute ou est-ce au débiteur qui n'a pas rempli son obligation de prouver qu'il en a été empêché ?

Dans une obligation de moyens, le fait que le résultat espéré ne soit pas obtenu ne suffit pas à établir la faute du débiteur puisque ce résultat n'a pas été promis. Seul l'engagement du débiteur à mobiliser ses moyens pour atteindre ce résultat a été convenu. Le créancier doit donc prouver que l'exécution défectueuse du contrat tient au fait que le débiteur ne s'est pas comporté avec toute la diligence nécessaire[44].

Dans une obligation de résultat, le seul fait que le résultat espéré ne soit pas atteint laisse présumer la défaillance du débiteur puisque celui-ci, normalement diligent, aurait dû atteindre le résultat sur lequel il s'était engagé. La preuve de la faute du débiteur se confond en pratique avec la preuve de la mauvaise exécution. C'est alors au débiteur de s'exonérer de cette faute en prouvant que la mauvaise exécution est due à un cas de force majeure.

Dans un contrat de services en ligne, l'obligation convenue peut bien entendu souffrir d'une inexécution ou d'exécution défectueuse ou tardive.

---

[40] Article 1240 (anciennement 1382) du Code civil : « Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer. » Rappelons ici que la responsabilité civile est une branche du droit qui régit la réparation du préjudice causé à autrui.

[41] Article 1147 Code civil : « Le débiteur est condamné, s'il y a lieu, au paiement de dommages et intérêts, soit à raison de l'inexécution de l'obligation, soit à raison du retard dans l'exécution, toutes les fois qu'il ne justifie pas que l'inexécution provient d'une cause étrangère qui ne peut lui être imputée, encore qu'il n'y ait aucune mauvaise foi de sa part. »

[42] Il doit exister un lien de causalité assez étroit pour être certain entre le manquement contractuel et le dommage exposé.

[43] Cf. 2.1.1 ci-dessus

[44] Toutefois, en cas d'inexécution totale, cette défaillance est si considérable que la faute du débiteur est présumée.

A titre d'illustration, cette mauvaise exécution[45] peut prendre différentes formes :

- Indisponibilité récurrente ou préjudiciable à une utilisation normale (mais restant dans les limites du SLA convenu)
- Temps de réponse/réaction anormalement long
- Disparition ou modification importante d'une fonctionnalité essentielle pour le client, sans respecter de délai de prévenance
- Régression lors d'une mise à jour
- Erreur de calcul
- Documentation erronée du logiciel ayant conduit à une utilisation inappropriée
- Archivage de données demandé mais non exécuté
- Archivage de données exécuté mais incomplet, donc impossible à réutiliser
- Perte d'un archivage antérieur
- Exécution trop tardive d'un service demandé
- Présence de virus dans les documents PDF émis par l'application
- Mélange avec des informations issues d'un autre client de la plate-forme
- Fuite de données du client (y compris des données non personnelles) à la suite d'une intrusion chez le fournisseur
- Etc…

Dans un contrat avec obligation de moyens, où l'engagement du débiteur est de fournir un effort constant et persévérant sans que la réalisation de la fin ultérieure de la prestation soit promise, le créancier doit observer le comportement de son débiteur pour montrer qu'il a commis une faute en ne se comportant pas avec toute la diligence requise.

Dans un contrat de service en ligne[46], il est impossible au créancier (le client) de prouver ce type de faute de la part de son débiteur (le fournisseur) :

- Pour des prestations exécutées à distance, il est impossible au client de scruter le comportement des agents du fournisseur pour s'assurer de leur diligence et de leur compétence
- Les traces techniques pouvant aider à prouver la faute du fournisseur ne sont pas accessibles au client. Quand bien même elles le seraient, la technicité requise pour les expertiser est hors de portée du client.
- Il n'existe pas, dans le secteur informatique, de référentiels de bonnes pratiques à l'instar des DTU[47] du BTP permettant de définir des comportements professionnels-types.

Face à cette situation, dans un souci de ré-équilibrage des relations entre clients (particuliers ou professionnels) et fournisseurs de services en ligne et pour une réparation plus facile des dommages rencontrés dans l'usage de ces services, deux pistes peuvent être envisagées :

- Instaurer par la loi des obligations accessoires aux contrats de service en ligne

[45] Le créancier devra bien entendu mettre en évidence, apporter la preuve de cette mauvaise exécution, ce qui peut déjà présenter une première difficulté.

[46] Qui est un contrat avec obligation de moyens

[47] Les DTU (Document Technique Unifié) sont des normes de mise en œuvre. En cas de litige avec un professionnel du bâtiment, concernant la qualité des travaux réalisés, les DTU servent de support aux experts des tribunaux, ainsi qu'aux assurances, afin de vérifier le respect des normes de la construction.

- Instaurer une responsabilité sans faute des fournisseurs de service en ligne

3.2.1 Instaurer par la loi des obligations accessoires aux contrats de service en ligne

Dans le cas des services en ligne, le principe de contractualisation est celui du "take it or leave it", en cohérence avec la standardisation des services fournis. Il s'agit donc sans hésiter de contrats d'adhésion[48] qui (cf. ci-dessus) sont souvent le reflet de relations déséquilibrées entre parties d'inégale puissance ou aux connaissances techniques et juridiques inégales.

Pour ré-équilibrer les relations entre parties, le droit pourrait intervenir pour ajouter aux obligations principales des contrats des obligations accessoires à ces dernières.

L'obligation de sécurité et l'obligation d'information sont, par exemple, deux constructions de la jurisprudence qui, en quelque sorte, ont introduit des clauses supplémentaires dans les contrats.

Obligation de sécurité et obligation d'information : deux exemples de « forçage contractuel »

L'obligation de sécurité, introduite par la Cour de cassation en 1911 en matière de transport de personnes, a depuis connu un certain succès dans les contrats de transport, l'utilisation des remontées mécaniques en montagne, les manèges de fête foraine,… Elle s'ajoute à une obligation principale du débiteur professionnel en lui imposant de ne pas créer de danger pour la santé des personnes. Cette obligation est cependant progressivement remplacée par des mécanismes juridiques tels que des régimes spéciaux d'indemnisation au profit de toutes les victimes ou encore la mention de cette obligation dans le Code de la Consommation ou le Code des Transports par exemple.

Par l'obligation d'information (ou de renseignement), le contractant est tenu de prévenir son cocontractant des risques et avantages de telle mesure ou de tel acte envisagés. Le médecin doit ainsi obtenir le consentement de son patient à l'opération projetée. Le gérant de portefeuille doit informer son client des risques encourus dans les opérations envisagées.

La loi intervient également dans les rapports contractuels entre professionnels et consommateurs d'un secteur. Ce fut le cas par l'arrêté du 14 juin 1982[49] qui régit les contrats entre agents de voyage et leurs clients. Aujourd'hui, le Code de la consommation, dans son chapitre IV « Règles spécifiques à des contrats ayant un objet particulier » du Titre II du Livre II, réglemente 18 types de contrat différents (de la fourniture d'électricité à la réparation automobile en passant par l'achat de métaux précieux). Cela reste très rare dans les contrats B-to-B.

[48] L'absence de négociation n'est-elle pas caractérisée dès lors que le client d'un service de Cloud coche une case aux fins de bénéficier du service ?

[49] Parmi les dispositions de ce texte (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000859991) :

- [L'agent de voyage] est garant de l'organisation du voyage ou du séjour et responsable de sa bonne exécution, […]
- Les défaillances de l'agent de voyages résultant de son fait ou de celui des prestataires de services […] sont couvertes par une assurance de responsabilité civile professionnelle
- Toute vente de prestations de séjour ou de voyage donne lieu à la remise d'un document approprié.

Recommandation n° 2. Pour un ré-équilibrage des relations contractuelles, instaurer par la loi des obligations accessoires aux contrats de service en ligne

Ces obligations accessoires pourraient par exemple poser les principes suivants :

- La fourniture du service est une obligation de résultat
- Le contrat doit comporter un accord sur les niveaux de service (SLA) pour :
  - La disponibilité du service
  - Le délai maximum de réponse à une sollicitation du support client
- La modification substantielle d'une fonctionnalité ou sa disparition doivent être annoncées avec un délai suffisant pour permettre au client la mise en place d'une solution de contournement économiquement acceptable

3.2.2 Instaurer une responsabilité sans faute des fournisseurs de service en ligne

Dans de nombreux domaines, la fonction réparatrice de la responsabilité civile a pris le pas sur toute autre considération et a conduit à une évolution vers une responsabilité sans faute : la faute n'est plus toujours requise pour justifier la responsabilité.

Les nombreux exemples de responsabilité sans faute[50]

La **responsabilité du fait personnel**[51]**,** qui est la « responsabilité de base » du Code civil, est une responsabilité pour faute, établie dès l'origine en 1804. Il existait à l'époque également 2 régimes particuliers : la responsabilité du fait des animaux et la responsabilité du fait des bâtiments en ruine. Il s'agissait de deux sources majeures d'accident dues à des choses non mues par l'homme. Pour tous les autres cas, la chose à l'origine d'un dommage était considérée comme un instrument dirigé par l'homme : il convenait alors de rechercher si la personne à l'origine de l'action dommageable avait ou non commis une faute.

Mais avec le développement des machines et des accidents liés à leur usage, il était souvent difficile de déterminer la part de l'homme dans la cause du dommage et donc sa faute difficile à prouver. Dans le souci de protéger les victimes, il a alors été établi un régime de **responsabilité du fait des choses**[52] où la responsabilité du « gardien de la chose », c'est-à-dire de celui qui en a l'usage, la direction et le contrôle[53], est présumée sans qu'il soit nécessaire de prouver sa faute.

Plus tard, toujours dans le souci de mieux protéger les victimes face à un dommage causé par un mineur ou un employé, une **responsabilité du fait d'autrui**[54] a vu le jour pour donner un répondant à la victime d'un dommage causé par une personne sur laquelle une autre exerce des pouvoirs ou une autorité. La responsabilité de cette dernière, sans qu'il soit besoin de prouver sa faute, est engagée dans le comportement fautif de la première.

Plus récemment[55], face à l'accroissement des nuisances causées par les installations industrielles, la jurisprudence va reconnaître que la théorie des **troubles anormaux de voisinage** est indépendante de l'existence d'une faute.

De nombreux textes spéciaux ont également rayé la faute des conditions de la responsabilité.

La **loi pour l'indemnisation des victimes d'accidents de la circulation** de 1985[56] où ce n'est pas la faute du conducteur (responsable) qui est à démontrer, mais l'implication de son véhicule dans l'accident.

« Considérant que seule la responsabilité sans faute du producteur permet de résoudre de façon adéquate le problème, propre à notre époque de technicité croissante, d'une attribution juste des risques inhérents à la production technique moderne [57]», la **responsabilité légale du fait des produits défectueux**[58] établit la responsabilité du producteur, sans qu'il soit nécessaire de prouver sa faute, dans le dommage causé par un défaut de sécurité de son produit provoquant une atteinte à la personne ou un dommage matériel dont la réparation est supérieure à 500 €.

La convention de Bruxelles du 29 novembre 1969 et la loi du 26 mai 1977[59] sur la responsabilité des dommages résultant de **fuites ou de rejets d'hydrocarbures** stipule que « Tout propriétaire d'un navire transportant une cargaison d'hydrocarbures en vrac est responsable des dommages par pollution résultant d'une fuite ou de rejets d'hydrocarbures de ce navire […] ».

La convention de Paris du 29 juillet 1960 et la loi du 30 septembre 1968 pour les **dommages causés par l'énergie nucléaire**, prévoit que « L'exploitant d'une installation nucléaire est responsable conformément à la présente Convention de tout dommage aux personnes et de tout dommage aux biens […] »

[50] D'après « Droit des obligations », 16ème édition, par Alain Bénabent, LGDJ, et « Droit de la responsabilité et des contrats. Régimes d'indemnisation », sous la direction de Philippe Le Tourneau, édition 2018-2019, DALLOZ

La responsabilité sans faute peut ainsi « apparaître comme la contrepartie du pouvoir, de l'autorité ou de la maîtrise dont dispose le responsable sur d'autres personnes ou sur des choses[60] ».

S'agissant des contrats de service en ligne, on peut s'étonner que l'engagement des fournisseurs ne soit que de moyens dans la mesure où d'une part ils ont la maîtrise de tous les éléments[61] pour rendre parfaitement leur prestation, sans aléa qui caractérise généralement l'engagement de moyens, et d'autre part le client n'a qu'un rôle passif[62] dans la prestation.

Aussi, s'inspirant de l'évolution tracée ci-dessus de la responsabilité civile, nous proposons :

Recommandation n° 3.	Pour une réparation plus facile du préjudice, instaurer une responsabilité sans faute du fournisseur dans les contrats de service en ligne

Tous les contrats de service en ligne sont visés, qu'ils concernent des consommateurs ou des professionnels.

Cette piste d'évolution est certainement celle à privilégier par rapport à l'instauration par la loi d'obligations contractuelles, compte tenu, d'une part, de sa portée plus générale (le client peut être un consommateur ou un professionnel) et, d'autre part, de l'évolution retracée ci-dessus de la notion de responsabilité sans faute qui a déjà été introduite dans de nombreux domaines du droit, alors que l'imposition par la loi[63] d'obligations contractuelles a essentiellement concerné les relations entre professionnels et consommateurs.

Cette proposition peut être aménagée pour faciliter son acceptation et sa mise en oeuvre :

- Elle peut n'être applicable qu'à des fournisseurs présentant une surface financière suffisante (à définir)

---

[51] Article 1240 Code civil, cf. ci-dessus

[52] Article 1242 Code civil : « On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde […] »

[53] Ayant la maîtrise de la chose, il a la possibilité d'empêcher qu'elle ne cause un dommage

[54] Cf. Article 1242 Code Civil ci-dessus

[55] En 1971

[56] Loi Badinter, n° 85-677, 5 juill. 1985, tendant à l'amélioration de la situation des victimes d'accidents de la circulation et à l'accélération des procédures d'indemnisation

[57] Considérant n°2 de la directive 85/374/CEE du 25 juillet 1985 (https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31985L0374&from=EN)

[58] Directive européenne 85/374/CEE du 25 juillet 1985 transposée par la loi du 19 mai 1998

[59] Loi n°77-530 du 26 mai 1977 relative à la responsabilité civile et à l'obligation d'assurance des propriétaires de navires pour les dommages résultant de la pollution par les hydrocarbures

[60] In « Les principes de la responsabilité civile », par Patrice Jourdain, 8ème édition, DALLOZ

[61] Matériels, logiciels, personnels, locaux, organisation, procédé technique mis en oeuvre

[62] Il n'est que consommateur de la prestation, sans intervention partagée avec le fournisseur

[63] L'obligation de sécurité et l'obligation d'information sont des créations de la jurisprudence.

- Pour faciliter l'assurabilité du risque, un délai de prescription (6 mois par exemple) peut être défini au-delà duquel la recherche de responsabilité du fournisseur n'est plus possible

3.3 Etendre la protection du Code de la Consommation aux « petits professionnels profanes »

Deux textes récents de la législation européenne viennent renforcer la protection des petits acteurs économiques.

D'une part, le règlement européen P2B[64] (Platform to Business) du 20 juin 2019 a fait un pas vers une protection accrue de la partie faible dans les relations avec les grands fournisseurs de place de marché (Amazon MarketPlace, eBay, Cdiscount,…). Il prévoit en particulier d'encadrer plus précisément les décisions de restreindre, suspendre ou déréférencer des vendeurs, de conditionner la modification des CGU à une notification des entreprises utilisatrices de la place de marché au moins 15 jours à l'avance et une obligation de clarté concernant les termes des relations contractuelles.

D'autre part, la directive 2018/1972[65] du 11 décembre 2018 établissant le code des communications électroniques européen, étend aux microentreprises, aux petites entreprises et aux organisations à but non lucratif le bénéfice de certaines dispositions prévues pour les consommateurs (sur les modalités de l'information contractuelle, sur la durée maximale des contrats et sur les offres groupées). Ces entités sont en effet considérées comme étant dans une situation comparable à celle des consommateurs en termes de pouvoir de négociation.

Dans le même esprit, pour renforcer la protection des petites entreprises dans leurs relations avec les fournisseurs de service en ligne, il est proposé :

Recommandation n° 4.	Etendre la protection de l'article L212-1 du Code de la consommation sur les clauses abusives aux « petits professionnels profanes »

Le Code de la consommation régit les relations entre un professionnel et un consommateur. Mais certaines dispositions de ce code régissent également les relations entre deux professionnels : il s'agit des dispositions concernant les « contrats conclus hors établissement[66] entre deux professionnels dès lors que l'objet de ces contrats n'entre pas dans le champ de l'activité principale du professionnel sollicité et que le nombre de salariés employés par celui-ci est inférieur ou égal à cinq » (article L 221-3 du code de la consommation). Le professionnel profane au sens de la recommandation ci-dessus est celui pour lequel le contrat n'entre pas dans le champ de son activité principale[67].

---

[64] Ce texte du 20 juin 2019 a été publié au Journal officiel de l'UE le 11 juillet 2019. Il entrera donc en vigueur le 12 juillet 2020. Cf. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R1150&from=EN

[65] Cette directive doit être transposée avant le 21 décembre 2020. Le code européen vise principalement à créer un cadre harmonisé au sein de l'UE pour la réglementation des réseaux et des services de communications électroniques Cf. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018L1972

[66] Un contrat est hors établissement lorsqu'il est conclu en-dehors des locaux du vendeur. C'est le cas, par exemple, des contrats obtenus par démarchage à domicile.

[67] C'est le cas du bijoutier qui achète un service de gestion de sa comptabilité en ligne.

Justifiée par le fait qu'un « petit professionnel » n'a pas nécessairement les connaissances juridiques suffisantes pour bien appréhender les conséquences d'un contrat et que l'achat d'un service en ligne[68] est désormais indispensable à l'exercice d'une activité professionnelle, la proposition ci-dessus consiste à étendre le champ des professionnels couverts par l'article L212-1 du Code de la consommation à une tranche supplémentaire d'entreprises que sont celles de moins de 20 salariés[69].

La protection par les clauses abusives de l'article L212-1 du Code de la consommation

L'article L212-1 du Code de la consommation stipule que « Dans les contrats conclus entre professionnels et consommateurs, sont abusives les clauses qui ont pour objet ou pour effet de créer, au détriment du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat. […] Un décret en Conseil d'Etat, pris après avis de la commission des clauses abusives, détermine des types de clauses qui, eu égard à la gravité des atteintes qu'elles portent à l'équilibre du contrat, doivent être regardées, de manière irréfragable, comme abusives […] »

L'article R212-1 du même code liste les clauses abusives de manière irréfragable, parmi lesquelles :

- Limite de responsabilité : « 2° Restreindre l'obligation pour le professionnel de respecter les engagements pris par ses préposés ou ses mandataires ; »
- Limite à l'indemnisation : « 6° Supprimer ou réduire le droit à réparation du préjudice subi par le consommateur en cas de manquement par le professionnel à l'une quelconque de ses obligations »

L'intérêt de ces articles L212-1 et R212-1 est d'établir, sans même que le défenseur soit admis à apporter une preuve contraire, une liste de clauses abusives, ce qui limite l'interprétation par les tribunaux.

L'intérêt de cette *Recommandation n° 4* est d'offrir une protection « automatique » au petit professionnel. Certes, celui-ci pourrait aussi se prévaloir du bénéfice de l'article 1171 du Code civil («Dans un contrat d'adhésion, toute clause non négociable, déterminée à l'avance par l'une des parties, qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite. […] »), mais alors il devrait prouver le caractère abusif de la clause litigieuse, ce qu'il n'a pas à faire en invoquant l'article R212-1 du Code de la consommation.

Cette proposition peut être aménagée pour faciliter son acceptation en restreignant son champ d'application aux seuls contrats de service en ligne.

[68] Site web, messagerie, logiciel comptable en ligne,…

[69] La proposition est un seuil de 20 salariés. Signalons ici que, pour la commission européenne, selon la recommandation du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises « Dans la catégorie des PME, une petite entreprise est définie comme une entreprise qui occupe moins de 50 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 10 millions d'euros (Cf. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32003H0361&from=FR).

3.4 Tenir compte du droit local dans l'expression des clauses d'exonération/limitation de responsabilité/indemnisation dans les contrats destinés aux particuliers et aux petits professionnels

L'article L211-1[70] du Code de la consommation stipule que « Les clauses des contrats proposés par les professionnels aux consommateurs doivent être présentées et rédigées de façon claire et compréhensible. […] ».

Cet article gagnerait à être complété, d'une part, en précisant que toutes les clauses doivent être exprimées en tenant compte du droit local du consommateur, d'autre part, en étendant son champ d'application aux petits professionnels de moins de 20 salariés.

Recommandation n° 5.	Compléter l'article L211-1 du Code de la consommation par une disposition exigeant l'expression en droit local de toutes les clauses du contrat et étendre son champ d'application aux petits professionnels

L'expression « en droit local » d'une clause signifie que la clause ne doit pas commencer par une forme du type « Sous réserve du droit applicable… » car ce type d'expression permet alors au rédacteur d'introduire toute une série d'exclusions limitant sa responsabilité ou le droit à indemnisation du cocontractant, même lorsque le droit français, par exemple, interdit une telle exclusion, sans que cette rédaction soit pour autant contestable devant un tribunal.

L'effet recherché par le rédacteur d'une telle formulation excessive et compliquée, est sans doute un effet dissuasif en pensant que le consommateur ou petit professionnel hésitera ou renoncera à agir en justice. Ce ne peut pas être par ignorance des fournisseurs, souvent dotés d'importants services juridiques, que de telles clauses sont ainsi rédigées.

L'extension du champ de cet article aux petits professionnels, profanes[71] ou non, tient au fait que le petit professionnel, pas plus que le consommateur, n'a de connaissances juridiques suffisantes pour « décoder » des formulations juridiques compliquées.

La recommandation proposée pourrait faciliter des actions en justice de la part de particuliers et petits professionnels, auxquelles pourraient se joindre les associations (cf. 2.2.2).

3.5 Spécialiser une juridiction sur les litiges relatifs à la responsabilité des fournisseurs de systèmes numériques

Les actions en justice de la part des entreprises sont rares (cf. 2.3).

[70] https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006069565&idArticle=LEGIARTI000032227013

[71] Rappel : nous appelons « professionnel profane » le professionnel pour lequel le contrat n'entre pas dans le champ de son activité (cf. 3.3)

Une des causes évoquées est l'incertitude quant à l'issue de ces actions, tout particulièrement dans un domaine nouveau où la jurisprudence se forme et où la compétence des tribunaux dans la prise en compte de cette nouvelle problématique est inégalement répartie.

Recommandation n° 6.	Spécialiser une ou des juridictions territoriales des tribunaux judiciaires sur les litiges relatifs à la responsabilité des fournisseurs de systèmes numériques

Par cette recommandation, grâce à la spécialisation progressivement acquise par ces juridictions, il s'agit de réduire la variabilité de la jurisprudence et de donner ainsi plus de visibilité aux justiciables sur l'issue probable d'une action en justice. Cette spécialisation permettrait également de ne pas démultiplier la compétence technique en la matière qui reste une ressource rare du secteur.

Ce principe de spécialisation existe aujourd'hui en matière, notamment, de protection de la propriété intellectuelle :

- « Le tribunal judiciaire ayant compétence exclusive pour connaître des actions en matière de brevets d'invention, de certificats d'utilité, de certificats complémentaires de protection et de topographies de produits semi-conducteurs, dans les cas et conditions prévus par le code de la propriété intellectuelle, est celui de Paris. » (art.D. 211-6[72] du code de l'organisation judiciaire).
- « […]Toutefois, la cour d'appel de Paris est seule compétente pour connaître directement des recours formés contre les décisions du directeur de l'Institut national de la propriété industrielle en matière de délivrance, rejet ou maintien de brevets d'invention, de certificats d'utilité, de certificats complémentaires de protection et de topographies de produits semi-conducteurs » (art.D. 411-19-1[73] du code de la propriété intellectuelle)

4 DES PISTES D'EVOLUTION POUR UNE MEILLEURE PRISE EN COMPTE DE LA SECURITE

Les produits et services de certains fournisseurs tiennent une place importante dans le bon fonctionnement de la société, qu'il s'agisse de son activité économique (AWS, Microsoft, Google Cloud Platform, OVH, SalesForce, SAP,…) ou des libertés individuelles (FaceBook, Twitter, Whatsapp,…).

A tel point que ces produits et services peuvent être considérés comme une infrastructure, à l'instar des réseaux de télécommunication, de distribution d'électricité, de distribution d'eau et d'assainissement.

Ceci emporte quelques exigences vis-à-vis des fournisseurs opérateurs de cette nouvelle infrastructure, quant à leur façon d'appréhender la sécurité de leurs produits et services.

Si les recommandations formulées jusqu'à présent (cf. 3. *Des pistes d'évolution pour rééquilibrer les rapports contractuels*) concernaient les services en ligne, les propositions ci-dessous, s'appliquent,

[72]https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000039066848&cidTexte=LEGITEXT000006071164&dateTexte=20200101

[73]https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000021144703&cidTexte=LEGITEXT000006069414

elles, à tous les systèmes numériques, de la montre connectée au service en ligne de comptabilité, en passant par le robot d'assistance chirurgicale.

Le coût des cyber-attaques

Il est difficile d'appréhender le coût des cyber-attaques : les organisations victimes de celles-ci communiquent peu sur ces coûts et la vérification du coût annoncé est impossible. Si Saint-Gobain, victime d'une attaque de type NotPeya[74] en 2017 avait défrayé la chronique en annonçant une perte de 80 M€ de résultats liée à cette attaque, la moyenne des coûts est difficile à connaître.

C'est néanmoins ce que tente de faire Accenture Security, en collaboration avec le Ponemon Institute, dans son étude de mars 2019[75] « The cost of cybercrime ».

Dans cette enquête menée fin 2018 par interview (2 600 interviews) auprès d'un panel de 355 sociétés de plus de 5000 personnes dans 11 pays, il a été demandé aux entreprises rencontrées d'estimer le coût des cyber-attaques subies en prenant en considération les coûts liés à la perte de données (secrets commerciaux, données clients, secrets industriels,…), à l'interruption d'activité (perte d'exploitation notamment) et à la remise en route des équipements.

En France, le coût moyen d'une cyber-attaque en 2018 était de 8,8M€, en augmentation de 23% par rapport à 2017.

4.1 Une prise de conscience grandissante de la nécessité d'une meilleure prise en compte de la sécurité

La sécurité de fonctionnement des dispositifs numériques est une préoccupation grandissante des organisations utilisatrices bien sûr, mais aussi, progressivement, des fournisseurs et des Etats.

Le Charter of Trust[76] (février 2018), à l'initiative de Siemens, est une démarche d'entreprises du numérique (Siemens, AES, Airbus, Allianz, Atos, Cisco, Daimler, Dell Technologies, Deutsche Telekom, Enel, IBM, MSC, NXP, SGS, Total et TÜV Süd) qui constitue une charte de bonne conduite dans la sécurisation des systèmes numériques et énonce 10 principes pour un monde digital plus sûr, parmi lesquels :

- Les données doivent être protégées contre les accès non autorisés tout au long du cycle de vie des données.
- Un niveau approprié de contrôle et de surveillance de l'identité et de l'accès, y compris des tiers, doit être appliqué et mis en œuvre.
- Un processus doit être en mis en place pour garantir que les produits et services sont authentiques et identifiables.
- Un niveau minimum d'éducation et de formation à la sécurité doit être déployé régulièrement auprès des employés.
- Certification, sur l'aspect sécurité, des dispositifs critiques (infrastructure et objets connectés)

[74] Cette attaque avait paralysé 25 000 PC sur 117 000. La reprise d'activité s'est faite en 10 jours. Elle a coûté, selon les déclarations de Saint-Gobain, 220 M€ de chiffre d'affaires et 80 M€ de résultats.

[75] https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

[76] https://new.siemens.com/global/en/company/stories/research-technologies/cybersecurity/cybersecurity-charter-of-trust.html

La Revue stratégique de cyberdéfense[77] (mars 2018) recommande de poser au niveau international un principe de responsabilité de sécurité des acteurs privés systémiques dans la conception et la maintenance de leurs produits et services numériques.

En novembre 2018, à l'occasion de la réunion à l'UNESCO du Forum de gouvernance de l'internet (FGI), le Président de la République a lancé l'Appel de Paris[78] pour la confiance et la sécurité dans le cyberespace (Trust and Security in Cyberspace). Les soutiens[79] de l'Appel de Paris s'engagent notamment à accroître la prévention et la résilience face aux activités malicieuses en ligne ou encore à accroître la sécurité des produits et services numériques ainsi que la "cyber-hygiène" de tous.

La Commission européenne exprime, dans deux directives récentes, sa préoccupation d'une meilleure prise en compte de la sécurité informatique dans les ventes faites aux consommateurs :

- La directive 2019/771 du 20 mai 2019 concernant les contrats de vente de biens, s'inscrit dans la continuité de la directive 1999/44[80] sur nombre de points, tout en se distinguant par son extension aux biens comportant des éléments numériques (contenu embarqué ou service interconnecté) puisque la conformité de ces biens au contrat de vente intègre désormais des exigences relatives à la diffusion de mises à jour y compris les mises à jour de sécurité.
- La directive 2019/770 du 20 mai 2019 relative aux contrats de fourniture de contenus numériques et de services numériques (musique ou vidéo en ligne, stockage d'informations dans le nuage, services de partage de données,…) oblige également le professionnel à procéder aux mises à jour, y compris de sécurité, qui sont nécessaires au maintien de la conformité du contenu ou du service numérique.

4.2 Nos recommandations

Dans le sillage de ces initiatives, la mission préconise quelques recommandations pour matérialiser certains des engagements pris ou proposer une évolution des dispositions législatives de la Commission européenne.

Avant de trouver à être concrétisées dans des schémas législatifs ou réglementaires, ces recommandations gagneront à faire l'objet de bonnes pratiques élaborées avec toutes les parties prenantes au sein d'organismes internationaux tels que l'OCDE ou à être précisées dans des normes ISO.

Certaines de ces recommandations peuvent paraître excessives, mais elles ne sont probablement qu'une anticipation de ce qui deviendra indispensable pour les véhicules autonomes.

---

[77] Cette revue, véritable livre blanc de la cyberdéfense, est le premier grand exercice de synthèse stratégique dans ce domaine (http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/)

[78] https://ue.delegfrance.org/cybersecurite-appel-de-paris-2018

[79] Parmi les signataires de cet appel, on trouve Google, IBM, Oracle, Microsoft, FaceBook, INTEL, SAP, SalesForce. Mais ni Apple ni AWS.

[80] Cette directive a été transposée par l'ordonnance du 17 février 2005 qui a instauré en droit français la garantie légale de conformité.

4.2.1 Imposer une sécurité par défaut

La mise en œuvre d'un niveau suffisant de sécurité pour déjouer les cyber-attaques connues ne doit pas nécessiter d'action explicite de l'utilisateur du produit ou service. Il est en effet illusoire d'attendre de l'utilisateur un choix éclairé dans la mise en œuvre des différentes options proposées compte tenu de la complexité des dispositifs de sécurité et de la technicité nécessaires à leur bonne compréhension.

Ce qui est nécessaire pour une protection efficace et actualisée doit être fait automatiquement, dès la mise en marche du produit ou à la première connexion au service. C'est, par exemple, le chiffrage du disque dur ou des communications, l'activation avec le bon paramétrage d'un pare-feu, la mise en place d'un login et d'un mot de passe non standards pour l'accès aux menus de configuration, le paramétrage d'une activation de l'installation automatique des mises à jour de sécurité.

Il devrait rester possible à l'utilisateur, de faire d'autres choix (pour des raisons de performance ou d'interopérabilité par exemple, à titre transitoire ou permanent), en l'informant auparavant des conséquences de ceux-ci sur la sécurité du produit ou service.

Recommandation n° 7.	Imposer une sécurité par défaut dans la mise en œuvre des produits et services numériques

4.2.2 Instaurer la gratuité des mises à jour de sécurité

L'utilisateur ne devrait pas avoir à faire d'arbitrage prix versus sécurité qui, lorsqu'il est fait, tourne souvent en défaveur de la sécurité.

Même en l'absence d'abonnement à des mises à jour fonctionnelles pour enrichir les fonctionnalités du produit ou du service, l'obtention des mises à jour de sécurité par l'utilisateur doit être possible et gratuite pour la version du produit ou du service qu'il utilise.

Recommandation n° 8.	Instaurer la gratuité des mises à jour de sécurité, même en l'absence d'abonnement aux évolutions fonctionnelles du produit ou du service numérique

La mise à jour de sécurité doit concerner tous les composants présents dans le produit ou le service, même s'ils correspondent à l'activation d'une option payante à laquelle l'utilisateur n'a pas souscrit. Ces composants, même « dormants », peuvent en effet être des cibles ou des vecteurs d'attaque.

4.2.3 Obliger à la fourniture des mises à jour de sécurité bien après la fin de commercialisation du produit

La durée de fonctionnement en sécurité d'un produit ou service numérique était, jusqu'il y a peu, librement fixée par le fournisseur et très largement inconnue du client avant l'achat.

La loi n°2020-105 du 10 février 2020[81] relative à la lutte contre le gaspillage et à l'économie circulaire remédie à cette situation en prévoyant, en son article 27, que « *le vendeur veille à ce que le consommateur reçoive les mises à jour[82] nécessaires au maintien de la conformité des biens au cours d'une période à laquelle le consommateur peut raisonnablement s'attendre. Cette période ne peut être inférieure à deux ans. Un décret fixe dans quelles conditions cette période peut être supérieure à deux ans et varier selon les catégories de produits eu égard au type et à la finalité des biens et éléments numériques et compte tenu des circonstances et de la nature du contrat*.»

L'obligation faite au fabricant du bien numérique de fournir les mises à jour de sécurité est justifiée par le maintien en conformité du bien. C'est assurément un progrès puisque la durée de fonctionnement en sécurité du bien est alors connue du consommateur et imposée par la loi.

Mais la période d'usage d'un produit numérique va bien au-delà de la période de deux années (période minimum certes) au cours de laquelle la conformité du produit doit être maintenue par le vendeur : un produit peut être utilisé même bien après la fin de sa commercialisation[83]. C'est bien durant toute cette période d'usage qu'il convient de maintenir le fonctionnement en sécurité du produit.

Recommandation n° 9. Instaurer l'obligation de fournir pendant [5, 10] ans après la fin de commercialisation du produit numérique, les mises à jour de sécurité

Le respect de cette obligation représentera un coût pour les fabricants de biens numériques, qui devrait obérer le gain escompté de l'arrêt de la commercialisation d'un produit et combattre ainsi la tentation d'une obsolescence programmée parfois prêtée par certaines associations environnementales ou de consommateurs aux fabricants.

Le respect de cette obligation permettra aux utilisateurs du bien de se préparer sereinement, avec une visibilité suffisante, à la migration vers un nouveau produit.

La durée de fourniture des mises à jour de sécurité, entre 5 et 10 ans, devra être débattue avec les parties prenantes. Trop courte, son intérêt est fortement amoindri, trop longue, elle peut être un frein à l'innovation technologique par les acteurs en place[84].

Pour les services numériques, accessibles par abonnement, la notion de fin de commercialisation se confond avec la rupture de l'abonnement à l'initiative du consommateur, qui prive celui-ci de l'accès au service. Notre recommandation ne trouve donc pas à s'appliquer.

---

[81] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041553759&categorieLien=id

[82] Ces mises à jour incluent les mises à jour de sécurité puisque cet article 27 indique également, dans un autre alinéa, que « Pour les biens comportant des éléments numériques, le vendeur veille à ce que le consommateur soit informé des mises à jour, y compris des mises à jour de sécurité, qui sont nécessaires au maintien de la conformité de ces biens»

[83] L'exemple de Windows 7 est, en ce sens, édifiant : Microsoft a dû prolonger la maintenance de son système d'exploitation du 9 avril 2013 (fin de maintenance initialement annoncée) au 14 janvier 2020 compte tenu de la réticence des utilisateurs, notamment en entreprise, à passer à la version supérieure du système d'exploitation de Microsoft.

[84] Un nouvel entrant n'aura pas cette contrainte de fourniture des mises à jour de sécurité.

5 QUELS IMPACTS POUR CES PISTES D'EVOLUTION ?

5.1 Vers une augmentation du prix des produits/services numériques ?

La mise en œuvre des nouvelles exigences présentées ci-dessus, destinées à renforcer la sécurité des produits/services numériques, va représenter un coût supplémentaire pour les fournisseurs. Pour couvrir cette augmentation, ceux-ci peuvent être tentés d'augmenter le prix de leur produit ou service.

Le risque accru d'une mise en cause de leur responsabilité civile, par le rééquilibrage des relations contractuelles présenté ci-dessus, peut également amener ces fournisseurs à augmenter leurs prix pour se constituer une « réserve » en cas de condamnation par les tribunaux.

Cette augmentation n'est cependant pas certaine compte tenu de la concurrence entre fournisseurs et de la force du signal prix dans la captation de nouveaux clients (les offres à prix réduit voire nul les premiers mois sont fréquentes).

D'ailleurs, l'entrée en vigueur d'une récente évolution réglementaire n'a pas conduit à une augmentation des prix. Il s'agissait de l'instauration, le 18 mars 2016, de l'extension à 2 ans (au lieu de 6 mois) de la durée de présomption de conformité dans le cadre de la Garantie légale de conformité due au consommateur. L'effet inflationniste[85] avancé par les opposants à cette mesure ne s'est pas produit. C'est ce qu'a observé l'association UFC Que Choisir dans une étude[86] de mai 2016.

Même si une augmentation de prix devait avoir lieu, elle pourrait ne pas être perçue négativement par le consommateur, conscient des enjeux, puisqu'en contrepartie le fonctionnement en sécurité du produit/service serait assuré pour une plus longue période qu'actuellement et par ailleurs s'inscrirait dans un cadre contractuel plus équilibré.

5.2 Un frein à l'innovation ?

Le rééquilibrage des relations contractuelles par la mise en œuvre des recommandations ci-dessus accroît le risque, pour les fournisseurs du numérique, d'une mise en cause plus fréquente de leur responsabilité civile. La mise sur le marché d'une nouvelle fonctionnalité, au fonctionnement et aux usages encore mal connus, peut alors être freinée par l'appréhension du fournisseur de voir sa responsabilité mise en cause dans un dommage.

Ce type de risque pourrait être couvert par une assurance, dont l'offre reste à construire.

---

[85] Selon les détracteurs de la mesure, une prise en charge accrue de la réparation ou du remplacement des équipements en panne se répercuterait sur les prix affichés.

[86] https://pyreneesorientales.ufcquechoisir.fr/wp-content/uploads/sites/46/2016/05/Etude-Garantie.pdf

L'existence de ce mécanisme assurantiel permettrait notamment que l'ensemble des coûts générés par des défaillances de systèmes numériques ne soit pas internalisé par les seuls clients, laissant l'essentiel de la marge aux fournisseurs.

Une telle assurance ferait certainement l'objet d'une limite de garantie compte tenu de l'incertitude des coûts engendrés à l'occasion d'un dommage.
Plusieurs facteurs concourent à cette incertitude :

- le manque d'historique : pour une offre d'assurance naissante, les données de sinistralité font défaut. L'assureur doit être prudent dans la couverture qu'il accorde puisqu'il lui est difficile d'estimer la probabilité, l'impact et le coût des sinistres.
- l'effet « boule de neige » peut rendre difficile l'évaluation précise des dommages consécutifs à un événement cyber[87].
- un même défaut ou une même vulnérabilité peuvent engendrer une multitude de sinistres pour un produit/service largement répandu.
- une action de groupe peut transformer un ensemble de petits incidents en un sinistre unitaire important.

Le risque pourrait être contrôlé par les assureurs en conditionnant, par exemple, la couverture assurantielle à l'application de normes ou contrôles, ou encore au résultat de tests.

*
* *

A l'heure où les systèmes numériques sont devenus incontournables dans la vie économique et sociale, l'évolution de leur usage doit être accompagnée par une évolution du droit et de leur sécurité de fonctionnement : c'est le sens des recommandations formulées ici.

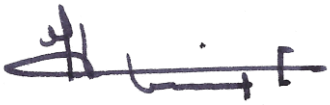
L'ingénieur général des Mines

Mario CASTELLAZZI

La contrôleur général économique et financier

Claudine DUCHESNE-JEANNENEY

L'ingénieur général des Mines



Ivan FAUCHEUX

[87] L'attaque en octobre 2016 du fournisseur américain de service DNS Dyn, a rendu difficilement accessibles les services de fournisseurs importants (AirBnb, Twitter, Github,…) pendant plusieurs heures

ANNEXES

Annexe 1 : Lettre de mission

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Paris, le 05 OCT. 2018

CONSEIL GÉNÉRAL DE L'ÉCONOMIE
DE L'INDUSTRIE, DE L'ÉNERGIE ET DES TECHNOLOGIES
TELEDOC 792
BATIMENT NECKER
120, RUE DE BERCY
75572 PARIS CEDEX 12

Affaire suivie par : Marie-Solange TISSIER
Téléphone : 01 53 18 54 66
Télécopie : 01 53 18 57 15
Mél. : marie-solange.tissier@finances.gouv.fr
Dossier N° 457

Le Vice-président

à

Mario Castellazzi
Ivan Faucheux
Françoise Trassoudaine

Objet : Responsabilité des fournisseurs de systèmes numériques

Les systèmes numériques, qu'ils soient utilisés à titre professionnel ou personnel, présentent fréquemment des insuffisances de conception et des failles de sécurité. Les conséquences vont d'un fonctionnement insatisfaisant ou dégradé à des vulnérabilités importantes permettant le vol de données sensibles ou personnelles vendues sur le marché de l'exploitation malveillante, ou une paralysie du terminal concerné voire du système d'information.

Ainsi, le 27 juin 2017, une cyber-attaque massive s'attaquant à certains systèmes d'exploitation Windows paralyse l'ensemble des infrastructures de certains grands groupes industriels. Les pertes financières correspondantes sont considérables. Début janvier 2018, une faille de sécurité majeure est détectée dans tous les processeurs Intel de la dernière décennie. Les corrections indispensables engendrent une baisse des performances des ordinateurs concernés estimée entre 5 % et 30 %.

Les dommages, parfois très élevés, sont à ce stade essentiellement financiers. Cependant, la sécurité physique de procédés industriels, de services urbains ou d'infrastructures de transport pourrait aussi être menacée avec des conséquences plus graves encore. En outre, l'omniprésence du numérique, la fréquence croissante des attaques et l'obsolescence rapide de certains systèmes numériques, dont les logiciels, provoquent une augmentation forte des coûts de sécurité au détriment des gains liés à la numérisation.

Enfin, certains acteurs en situation de quasi-monopole imposent à leurs clients des clauses qui pourraient être qualifiées d'abusives. Des interrogations apparaissent dans tous les pays, y compris aux Etats-Unis, quant aux façons les plus efficaces de réguler l'industrie du numérique et de protéger ses utilisateurs tout en préservant le dynamisme de développements technologiques créateurs de valeur économique.

S'agissant des logiciels, une première analyse juridique montre que, dans le Code de la propriété intellectuelle, ceux-ci figurent dans la liste des œuvres de l'esprit au même titre que les œuvres d'art. Ils ne semblent donc pas soumis, en tant que services ou biens, aux garanties qui s'appliquent habituellement aux biens corporels et incorporels. Ils ne semblent pas non plus couverts par le Code de la consommation puisque la cession porte sur un droit d'usage et non

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

sur le logiciel lui-même dont la propriété n'est jamais transférée. Le droit ad-hoc dépendrait alors uniquement des clauses de la licence d'utilisation que le client ne peut qu'accepter.

S'agissant de systèmes numériques de types particuliers, il conviendrait d'analyser dans quelle mesure le Code de commerce, en particulier ses dispositions relatives aux pratiques restrictives de concurrence, pourrait trouver à s'appliquer et permettre aux utilisateurs professionnels de disposer de leviers pour rééquilibrer la relation commerciale ou obtenir du juge qu'il sanctionne les clauses contractuelles et/ou les pratiques dont ils s'estimeraient victimes.

C'est pourquoi je vous demande de bien vouloir :

- étudier les règlementations et régimes de responsabilité qui s'appliquent tant aux logiciels qu'aux autres systèmes numériques, dans différents pays, notamment des États membres de l'Union européenne et les États-Unis ;

- analyser des contrats de licences logicielles ou d'utilisation de systèmes numériques en identifiant d'éventuelles clauses qui pourraient être qualifiées d'abusives ainsi que leur fréquence ;

- puis surtout envisager des mesures (nationales, européennes, internationales) qui pourraient conduire à une responsabilité des éditeurs de logiciels et offreurs de systèmes numériques, proportionnée à l'impact potentiel de leurs défaillances sur leurs clients. Vous étudierez spécifiquement la possibilité de profiter de la révision des directives communautaires en matière de protection du consommateur.

Vous examinerez les conséquences que pourraient avoir les mesures proposées sur les éditeurs et offreurs de systèmes numériques de logiciels de taille intermédiaire, notamment français, ainsi que sur le développement du secteur en France et en Europe.

Vous solliciterez en tant que de besoin les services et établissements publics compétents du ministère de l'économie et des finances, ainsi que du secrétariat d'Etat au numérique.

Vous me remettrez un rapport d'étape assorti des projets de recommandation pour le 15 février 2019 et votre rapport final au plus tard le 1er juin 2019.

Luc ROUSSEAU

Annexe 2 : Liste des personnes rencontrées ou interrogées

Organismes publics et parapublics

Ministère de l'intérieur : direction des systèmes d'information et de communication (DSIC)

Pascal DE LOS RIOS : chef du bureau de l'Achat, du contrôle de gestion et de l'optimisation des Moyens
Thierry MARKVITZ : sous-directeur des infrastructures
Vincent NIEBEL : Directeur
Emmanuelle RACINET : Adjointe au sous-directeur de l'administration générale et de l'achat
Sahondra RAKOTOZAFY: chef de bureau des affaires juridiques

Agence Nationale de la sécurité des systèmes d'information (ANSSI)

Vincent STRUBEL: sous-directeur expertise

Autorité de la Concurrence

Nicolas DEFFIEUX : Rapporteur général adjoint
Julien MICHEL : Rapporteur permanent

Ministère de l'Europe et des affaires étrangères

Florian ESCDUIE : Sous-directeur des affaires stratégiques et de la cyber sécurité
Jean HEILBRONN : sous direction des affaires stratégiques et de la cybersécurité

Direction des Achats de l'Etat (DAE)

Michel GREVOUL : directeur des achats de l'Etat
Hippolyte LE MEUR : Acheteur leader de logiciels
Maxence WAERNIERS : Adjointe au chef de bureau des achats informatiques, télécoms et postes de travail

Direction des Affaires Juridiques (DAJ)

Steeve ABITBOL : Adjoint au chef du bureau du droit des entreprises et de l'immatériel (4B)
Antoine de Château-Thierry : Sous-directeur du droit des régulations économiques (4ème sous-direction)
Claire IFFLI : Bureau 4B

Direction interministérielle du numérique et du système d'information et de communication (DINSIC)

Côme BERBAIN : Directeur des technologies numériques de l'Etat

Agence pour l'informatique financière de l'état (AIFE)

Marc GAUTIER : secrétaire général
Laurent ROBILLARD : Adjoint de la directrice

Secrétariat général aux affaires européennes

Loic AGNES : Chef du secteur Industrie-Télécoms-numérique-Environnement-Energie-Climat (ITEC) du SGAE
Christine CABUZEL DU VALLON : Adjointe au chef des secteurs ITEC
Jean Luc DANIEL: Adjoint au chef de secteur, Secteur Marché intérieur, consommateurs, concurrence, aides d'État, mieux légiférer (MICA).
Lucile GERNOT : Adjointe au chef de secteur Espace judiciaire européen coopération judiciaire en matière civile
Renaud HALEM : Chef du secteur Espace judiciaire européen, conseiller justice

DGCCRF :

Geneviève CAVAZZI, Adjointe Bureau 5A (Produits industriels)
Pierre CHAMBU : Chef de service de la protection des consommateurs et de la régulation des marchés
Raphaël CHAUVELOT-RATTIER, Bureau 3A (Politique de protection des consommateurs et loyauté)
Mary-Audrey COURTOIS, Adjointe Bureau 3C (Commerce et relations commerciales)
Philippe GUILLERMIN : Chef du Bureau Politique de protection des consommateurs et loyauté
Nadine MOUY, Sous-directeur Services, réseaux et numérique
Paul-Emmanuel PIEL : Chef du bureau médias, télécommunications, biens et services culturels
Pierre REBEYROL, Chef du bureau 3C (Commerce et relations commerciales)
Axel THONIER : chargé de mission

France TV :

Philippe Rouaud : Directeur des systèmes d'Information et Innovations-Développements

GIE Cartes bancaires :

Philippe LAULANIE : Administrateur directeur général

Union des groupements publics d'achat (UGAP) (échange par écrit) :

Jean-Marc BORNE : Directeur des achats techniques

Organismes privés

AXA :

Pierre Yves LAFFARGUE : Directeur souscription IARD Entreprises, directeur régional entreprises IARD IDF
Laurence LEMERLE : Axa particuliers et IARD Entreprises, Directrice Risques Techniques et Cyber
Hubert MARCK: Secrétariat Général d'AXA France, Directeur déontologie, Affaires Publiques et Conformité
Emmanuelle RIVÉ : Secrétariat Général d'AXA France, Responsable Affaires Publiques et Règlementaires, Assurance de personnes et opérations transverses

Alain Bensoussan Avocats lexing

Eric LE QUELLENEC : Avocat, Directeur du département informatique conseil

EIFFAGE :

Julien COMPAGNON : Département Contractual and Process Management

GEODIS :

Henri LINIERE : Global CIO

MAIF:

Guillaume RINCE : Chief technical officer

RATP :

Michel CORDIVAL: Directeur des systèmes d'information et de la télécommunication

Salesforce :

Amélie MERVANT : Corporate Counsel, EMEA Privacy
Sébastien LALOUE : Senior director, Legal EMEA (France & Iberia)

EDF :

Robert STRANGRET: Directeur Achats domaines IT, domaine Achats informatiques et Télécommunication

CIGREF

Henri d'AGRAIN : Délégué Général
Vanessa DEWAELE : chargée de mission

UFC QUE CHOISIR

Raphaël BARTLOME : responsable service juridique

LA POSTE

Bruno ECHARDOUR : Directeur des systèmes d'information du groupe
Cyrille TESSER : Adjoint au Directeur de la Cyber sécurité du Groupe

SAP :

Amal TALEB, Directrice Affaires Publiques, SAP France

SYNTEC Numérique (échange par écrit) :

Philippine Lefèvre-Rottmann, Déléguée aux relations institutionnelles

TECHN IN France :

Jean Sébastien MARIEZ : Avocat, Associé au cabinet De Gaulle Fleurance & Associés et conseiller de Tech in France
Loic RIVIERE : Délégué général
Marjorie VOLLAND : Marjorie Volland

Annexe 3 : Les contrats et CGU/CGV examinés par la mission

Les contrats et CGU/CGV examinés par la mission à titre d'observatoire des relations entre professionnels ont été les suivants. Ils sont relatifs à des acteurs tant étrangers que français, de taille mondiale ou internationale, et distribuent des services d'infrastructure (IaaS), de plate-forme (PaaS) ou de service (SaaS).

Par ordre alphabétique :

AWS
AWS (Amazon Web Services) est le leader mondial dans la fourniture de services cloud IaaS
Contrat de client AWS : https://aws.amazon.com/fr/agreement/
Engagement de niveaux de service de S3 (service de stockage de fichiers) :
https://aws.amazon.com/fr/s3/sla/
Engagement de niveaux de service de EC2 (fourniture d'instances de serveurs) :
https://aws.amazon.com/fr/compute/sla/

EBP
EBP est un fournisseur français de progiciels de gestion administrative, comptable et financière conçu pour les besoins les plus courants des petites et moyennes entreprises établies en France
CGV : https://www.ebp.com/wp-content/uploads/2019/10/ebp-cgs-2019.pdf

Google Cloud Platform (GCP)
GCP est le service de fourniture de services en ligne (IaaS et PaaS) de Google
Conditions d'utilisation de GCP : https://cloud.google.com/terms/?hl=fr
Engagement de niveaux de service : https://cloud.google.com/terms/sla/?hl=fr
Engagement de niveaux de service pour le stockage de fichiers (Google Cloud Storage) :
https://cloud.google.com/storage/sla?hl=fr

HEROKU
HEROKU est une filiale de SalesForce qui commercialise des services en mode PaaS
Terms of service : https://www.heroku.com/policy/salesforce-heroku-msa
Acceptable use policy : https://www.heroku.com/policy/aup

Microsoft
On line service terms : https://www.microsoft.com/en-us/licensing/product-licensing/products#OST
Contrat de niveaux de service :
http://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=OSCS&lang=French
Conditions relatives aux produits :
http://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=PT&lang=French

SAGE
SAGE est un acteur français qui fournit un progiciel d'automatisation des processus comptables des entreprises
CGU : https://media.sage.fr/cg/expert-comptable/CGU-SaaS-Sage-Experts-Comptables.pdf

SalesForce

SalesForce est un acteur US spécialisé dans la fourniture de logiciels en mode SaaS pour la gestion de la relation clients

Contrat cadre de souscription – SaaS :
https://c1.sfdcstatic.com/content/dam/web/en_us/www/documents/legal/salesforce_MSA.pdf

SAP

SAP est un fournisseur allemand de solutions logicielles pour la gestion d'une entreprise

Conditions générales du SaaS : https://www.sap.com/docs/download/agreements/general-terms-and-conditions/cls/general-terms-and-conditions-for-sap-cloud-services-direct-france-french-v12-2018.pdf

Engagement de niveaux de service : https://www.sap.com/docs/download/agreements/product-use-and-support-terms/cls/frfr/service-level-agreement-for-sap-cloud-services-french-v4-2019.pdf

OVH

OVH est un opérateur français de service en ligne

Conditions générales :
https://www.ovh.com/fr/support/documents_legaux/conditions%20generales%20de%20service.pdf

PaaS (hébergement partagé) :
https://www.ovh.com/fr/support/documents_legaux/conditions_particulieres_hebergement_web.pdf

IaaS (Serveurs dédiés) :
https://www.ovh.com/fr/support/documents_legaux/conditions%20particulieres%20serveur%20dedie.pdf

Annexe 4 : Glossaire

CGE	Conseil général de l'Economie
IaaS	Infrastructure as a Service
Magasin d'applications	Plate-forme en ligne pour la distribution d'applications aux utilisateurs
Marketplace	Place de marché
PaaS	Platform as a Service
SaaS	Service as a Service
SLA	Service Level Agreement ou Accord de niveau de service, par lequel un fournisseur s'engage sur le respect d'indicateurs (niveaux de service) dans l'exécution de sa prestation